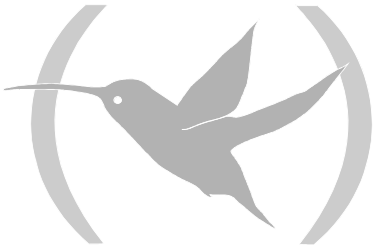
Router Teldat

Facilidad NAPT

Doc. *DM735* Rev.*10.00*
Diciembre, 2002

ÍNDICE

Capítulo 1
Introducción



1. Introducción a la facilidad NAPT

La Traducción de Direcciones de Red (Network Address Translation) es un método por el que las direcciones se mapean de una red a otra, con la intención de proporcionar un routing transparente a las distintas estaciones de la red. Tradicionalmente, los dispositivos de NAT se emplean para aislar dominios de direcciones con direcciones privadas no registradas de dominios externos con direcciones únicas asignadas de forma unívoca.

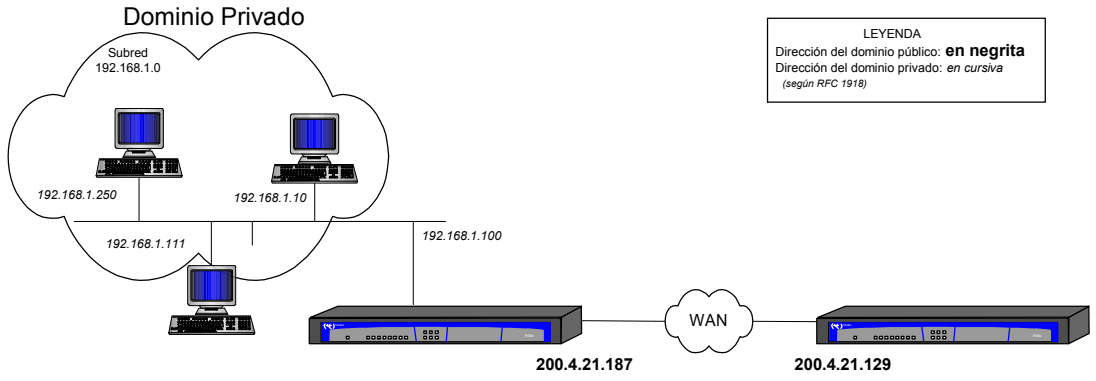
Hay una gran variedad de traducción de direcciones que se utiliza en distintas aplicaciones. Sin embargo, hay características comunes entre los dispositivos que hacen NAT:

a) Asignación transparente de direcciones.

b) Routing transparente a través de la traducción de direcciones (el rutado aquí se refiere al encaminamiento de los paquetes y no al intercambio de paquetes de información sobre el routing, RIP, OSPF, etc).

c) Traducción de la información útil de los paquetes ICMP de error.

El escenario típico de NAT es el que se describe a continuación. En él, se muestra un router que hace NAT y que está conectado a un Proveedor de Servicio de Internet (ISP) a través de otro router perteneciente a la WAN (Wide Area Network) del proveedor.



La facilidad NAPT (Network Address Port Translation) extiende la idea de traducción un paso más, realizando también la traducción del identificador de transporte (Puertos UDP o TCP, o los identificadores ICMP). Esto permite que los identificadores de transporte de un número de hosts privados se multiplexen a través de otros identificadores de transporte con una única dirección común para todos. Puede combinarse con la facilidad NAT básica (Traducción de direcciones).

Para paquetes destinados fuera de la red privada, NAPT traduce la dirección IP fuente, el identificador de transporte fuente y actualiza los campos correspondientes a los distintos checksums de los paquetes implicados (IP, UDP, TCP o ICMP). Los identificadores de transporte pueden ser puertos de UDP/TCP o bien los identificadores de petición ICMP. Para los paquetes que vayan a entrar en el dominio privado se traducen la dirección destino y los identificadores de transporte y además se recalculan los checksums de los paquetes implicados.

Algoritmos para recalcular los checksums de forma diferencial se proporcionan en la RFC 1361 (IP Network Address Translator).

2. Excepciones al NAPT

Surgen dos excepciones al NAPT cuando el dominio privado se encuentra con determinadas necesidades.

2.1. Puertos visibles

Imagínese que se desea facilitar acceso a un servidor FTP que está emplazado en el segmento de la red local del dominio privado. Si desde el dominio externo o global se intenta acceder al puerto FTP del servidor, los paquetes serán capturados por el router que da acceso, de tal modo que el servidor FTP inicial no podría ser alcanzado por el dominio externo.

Para evitar esta situación puede "publicar**"** el puerto FTP del servidor (que se encuentra en el dominio privado) en el router de acceso con otro puerto, que queda reservado para este servidor. Para ello habría que establecer la siguiente asociación:

(Dirección Interna, Puerto Interno) ⟷ Puerto Externo

En el caso del servidor FTP podría ser:

(192.168.1.21, 21) ⟷ 6400

Así, las conexiones a la dirección pública del router al puerto destino 6400 (el publicado para hacer accesible el servidor FTP), se traducen , mediante NAPT, a la dirección del propio servidor y al puerto destino 21 (puerto estándar del FTP) haciendo posible la conexión FTP con dicho servidor.

De manera análoga se procede si se quisiera hacer públicos los puertos de Telnet de distintas máquinas de la red privada, u otros servicios en los que los paquetes destinados a puertos estándar sean capturados por el router de acceso.

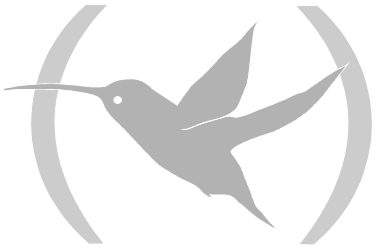
Se pueden "publicar" puertos estándar ya capturados por el router de acceso (por ejemplo, FTP o TELNET) si previamente se traslada el puerto que captura el equipo; es decir, si se desea que las conexiones al puerto TELNET por defecto (23) de la dirección pública no correspondan a una conexión al servidor TELNET del router sino a una conexión al servidor TELNET de un equipo del dominio privado, debe trasladar el puerto del servicio del router (por ejemplo, al puerto 8023) y publicar en el puerto estándar.

Si no traslada el puerto del router, perderá el acceso al servidor del router por la conexión que realiza NAPT.

2.2. Subredes visibles

La otra excepción de NAPT es el caso que se da cuando se dispone de un conjunto de direcciones del dominio público y se quiere que sean accesibles a través del router de acceso que está haciendo NAPT.

Capítulo 2
Configuración de la facilidad NAPT



1. Configuración de la facilidad NAPT

El acceso al menú de configuración de la facilidad de NAPT se realiza a través del menú de configuración de IP, mediante los siguientes comandos:

```
*P 4
Config>PROTOCOL IP

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

-- NAPT configuration --
NAPT config>
```

Las reglas NAPT se añaden o borran directamente desde el menú de configuración de IP. Para obtener más información, consultar el manual asociado Dm 702. El resto de la configuración de esta facilidad se realiza desde el menú de configuración de NAPT.

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

Los comandos se definen según la siguiente nomenclatura:

`RULE`	Parte obligatoria.
`<rule id>`	Parte obligatoria a determinar por el usuario.
`[NO]`	Parte opcional.

1.1. Creación de un puerto visible

La configuración de un puerto visible tiene el objeto de permitir la entrada de paquetes procedentes del dominio externo destinados a un puerto determinado (puerto externo) y redirigirlos a una dirección IP del dominio interno a un puerto determinado (puerto interno)

El comando para configurar un puerto visible es el siguiente:

```
NAPT config>VISIBLE-PORT <external port> RULE <rule id> PORT <internal port> IP <IP
host address>
```

External port (Puerto externo): Puerto de conexión visible desde el dominio externo para acceder al servicio que proporciona el host interno.

Rule ID (Identificador de regla): Es el identificador de la regla para la que queremos hacer visible un determinado puerto.

Internal port (Puerto interno): Es el puerto destino del host interno..

IP Host address (Dirección IP): Es la dirección IP del host del dominio interno.

Si configura como puerto externo y como puerto interno el valor 0, está definiendo que el router redirija, hacia la dirección indicada, el tráfico entrante por la conexión afectada por el NAPT que por defecto descartaría; dicha dirección IP se convierte en el destino de todo el tráfico destinado a puertos desconocidos por el router.

Adicionalmente dispone de la opción `DEFAULT` que establece los valores por defecto para el puerto visible, es decir, puerto interno 0 a dirección interna 0.0.0.0 de tipo genérico.

Ejemplos:

Redirigir el puerto externo 80 (HTTP) de la conexión afectada por la regla de NAPT número 1 al puerto 80 de la dirección interna 192.168.1.5: con esta configuración conseguiría que las conexiones HTTP realizadas contra el router por la conexión afectada por la regla de NAPT 1 al puerto por defecto HTTP se redirigieran a un servidor HTTP interno (Si no ha cambiado el puerto del servidor HTTP del router, no podrá acceder al servidor HTTP del router por la conexión afectada por la regla de NAPT número 1).

```
NAPT config>VISIBLE-PORT 80 RULE 1 PORT 80 IP 192.168.1.5
NAPT config>
```

Redirigir el puerto externo 8021 de la conexión del router afectada por la regla de NAPT 1 al puerto 21 de la dirección interna 192.168.1.5: con esta configuración conseguiría que las conexiones realizadas contra el router por la conexión afectada por la regla de NAPT número 1 al puerto 8021 constituyan realmente una conexión FTP al servidor interno 192.168.1.5.

```
NAPT config>visible-port 8021 rule 1 port 21 ip 192.168.1.5
NAPT config>
```

1.2. Modificación de un puerto visible

El comando para modificar un puerto visible es el siguiente:

```
NAPT config>VISIBLE-PORT <external port> RULE <rule id> PORT <internal new port> IP
<new IP host address>
```

Internal new port (Nuevo puerto interno): si es distinto al puerto anteriormente configurado, se sustituye por el indicado.

New IP Host address (Nueva dirección IP): si es distinta a la dirección anteriormente configurada, se sustituye por la dirección indicada

Ejemplo:

```
NAPT config>VISIBLE-PORT 8021 RULE 1 PORT 6021 IP 192.168.1.6
NAPT config>
```

1.3. Borrado de un puerto visible

El comando para borrar un puerto visible es el siguiente.:

```
NAPT config>NO VISIBLE-PORT <external port> RULE <rule id>
```

Ejemplo:

```
NAPT config>NO VISIBLE-PORT 80 RULE 1
  Port deleted
```

1.4. Listado de los puertos visibles configurados

El comando para listar los puertos visibles configurados es el siguiente:

```
NAPT config>LIST VISIBLE-PORT
```

Ejemplo:

```
NAPT config>LIST VISIBLE-PORT

 ========================
 =  NAPT VISIBLE PORTS  =
 ========================

 Rule  Internal Address   Int.Port --> Ext.Port
 ----  ----------------   --------     --------
    1   192.168.1.5           80   -->     80
    1   192.168.4.5           21   -->   8021

NAPT config>
```

1.5. Creación de una subred visible

La configuración de una subred visible tiene el objetivo de proporcionar total transparencia hacia y desde determinadas direcciones del dominio interno, actuando el router para dichas direcciones como si no tuviera NAPT configurado.

El comando para configurar una subred visible es el siguiente:

```
NAPT config>SUBNET <IP Network address> <IP Network mask> RULE <rule id> < DEFAULT |
GATEWAY <IP address>]
```

Dirección IP de la subred visible: Es la dirección IP de la subred que se va a hacer visible a través de la conexión definida por la regla de NAPT.

Máscara de la subred visible: Es la máscara de la subred que se va a hacer visible a través de la conexión definida por la regla de NAPT.

Identificador de regla: Es el identificador de la regla. Las reglas configuradas aparecen listadas previamente.

Router por defecto (opcional): En el caso de que la subred visible esté directamente conectada al router de acceso por un interfaz que no tiene dirección en dicha subred, en este campo hay que configurar una dirección de la subred visible, concretamente la pasarela de la ruta por defecto de los hosts de la subred visible, para que el router de acceso responda a las peticiones ARP de los hosts de la subred. Si no es así, es decir, si la subred no está directamente conectada o el router tiene asignada una dirección de la subred visible en el interfaz directamente conectado a dicha subred, se dejará este campo con valor por defecto (0.0.0.0) para no utilizar una dirección de la subred visible en dicho interfaz y permitir un correcto funcionamiento del entorno.

La opción `DEFAULT` establece los parámetros por defecto (en este caso, el único parámetro es `GATEWAY` que configura a 0.0.0.0, es decir, equivalente a `NO GATEWAY`).

Ejemplo:

Hacer visible la subred no directamente conectada 200.12.100.128/25 a través de la conexión afectada por la regla NAPT número 1; con esta configuración consigue que el tráfico procedente o destinado a dicha subred que atraviese el router por la conexión afectada por la regla de NAPT número 1 lo haga de forma transparente.

```
NAPT config>SUBNET 200.12.100.128 255.255.255.128 RULE 1 DEFAULT
NAPT config>
```

Hacer visible la subred directamente conectada 200.12.100.128/25 con router por defecto 200.12.100.129 a través de la conexión afectada por la regla NAPT número 1, conexión que tiene asignada precisamente la dirección 200.12.100.129; este escenario es típico en accesos WAN en los que su ISP le proporciona un conjunto de direcciones públicas: su interfaz WAN tendrá una dirección de dicha subred: deberá configurar NAPT para permitir el acceso al exterior a los equipos con direccionamiento privado situados en el dominio interno a la vez que tiene acceso transparente a los equipos asociados a las direcciones de la subred asignada.

Ejemplo:

```
NAPT config>SUBNET 200.12.100.128 255.255.255.128 RULE 1 GATEWAY 200.12.100.129
NAPT config>
```

1.6. Modificación de una subred visible

Solo se puede modificar el parámetro "gateway" de una subred visible definida.El comando para modificar el gateway es el mismo que el utilizado para definir una subred visible, con la particularidad de que la dirección y máscara de la subred coinciden con los valores de una subred visible ya definida.

```
NAPT config>SUBNET <IP network address> <IP network mask> RULE <rule id>  < NO
GATEWAY | GATEWAY <IP address> >
```

Dado que actualmente solo hay un parámetro configurable en las subredes visibles (GATEWAY), puede utilizar indistintamente DEFAULT o NO GATEWAY.

Ejemplo:

```
NAPT config>SUBNET 200.12.100.128 255.255.255.128 RULE 1 NO GATEWAY
NAPT config>
```

o

```
NAPT config>SUBNET 200.12.100.128 255.255.255.128 RULE 1 DEFAULT
NAPT config>
```

1.7. Borrado de una subred visible

El comando para borrar una subred visible es el siguiente:

```
NAPT config>NO SUBNET <IP network address> <IP network mask> RULE <rule id>
```

Ejemplo:

```
NAPT config>NO SUBNET 200.12.100.128 255.255.255.128 RULE 1
  Subnet deleted
```

1.8. Listado de las subredes visibles configuradas

El comando para listar las subredes visibles es el siguiente:

```
NAPT config>LIST SUBNET
```

Ejemplo:

```
NAPT config>LIST SUBNET

 ========================
 = NAPT VISIBLE SUBNETS =
 ========================

 Rule     Net Address        Net Mask       Default Gateway
 ----   --------------    ---------------   ---------------
    1   200.12.100.128    255.255.255.128   200.12.100.129

NAPT config>
```

1.9. Habilitar y deshabilitar NAPT

Puede habilitar o deshabilitar de modo global la funcionalidad de NAPT mediante los siguientes comandos:

```
NAPT config>ENABLE
```

o

```
NAPT config>DISABLE
```

o

```
NAPT config>NO ENABLE
```

Ejemplo:

```
NAPT config>ENABLE
  NAPT enabled
NAPT config>
```

o

```
NAPT config>DISABLE
  NAPT disabled
NAPT config>
```

1.10. Listado del estado del NAPT

El comando para listar el estado de la facilidad NAPT es el siguiente:

```
NAPT config>LIST CONFIGURATION
```

Ejemplo:

```
NAPT config>LIST CONFIGURATION

 ========================
 =  NAPT CONFIGURATION  =
 ========================

  NAPT Disabled
  NAPT First Port               : 32768
  NAPT Entries (number of ports): 1024

NAPT config>
```

1.11. Configuración del rango de puertos a utilizar

El router ofrece la posibilidad de definir el rango de puertos a utilizar por el NAPT mediante dos parámetros de configuración: el puerto inicial y el número de puertos a utilizar.
Los comandos para configurar el rango de puertos son los siguientes:

```
NAPT config>NUMBER-OF-PORTS <value>

NAPT config>FIRST-PORT <value>
```

Ejemplo:
Vamos a duplicar el número de puertos disponibles para NAPT y configurar como primer puerto el 60000.

```
NAPT config>NUMBER-OF-PORTS
  Number of NAPT entries [1024]? 2048
NAPT config>
```

```
NAPT config>FIRST-PORT
  First NAPT port (1024-65535) [32768]? 60000
NAPT config>
```

NOTA: A mayor número de entradas NAPT más host del dominio interno pueden acceder simultáneamente al dominio externo, pero requiere la utilización de más recursos del equipo (memoria, capacidad de procesamiento, etc).

NOTA: Debido a que el puerto máximo que se puede utilizar es el 65535 (0xFFFF), si la configuración de Puerto Inicial y Número de Entradas NAPT hace que se sobrepase el valor del puerto máximo, el número de entradas NAPT se limita internamente al valor comprendido entre el Puerto Inicial y 65535.

1.12. Listado del rango configurado de puertos NAPT

El comando para listar el rango de puertos NAPT es el siguiente:

```
NAPT config>LIST CONFIGURATION
```

Ejemplo:

```
NAPT config>LIST CONFIGURATION

 ========================
 =  NAPT CONFIGURATION  =
 ========================

  NAPT Disabled
  NAPT First Port               : 60000
  NAPT Entries (number of ports): 1024

NAPT config>
```

1.13. EXIT

El comando **EXIT** permite salir del entorno de configuración de la facilidad NAPT.

```
NAPT config>EXIT
```

Ejemplo:

```
NAPT config>EXIT
IP config>
```

2. Resumen de comandos

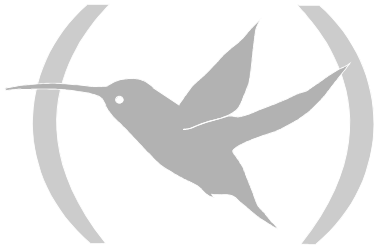
```
DISABLE
[NO] ENABLE

NO VISIBLE-PORT <external port> RULE <id>
   VISIBLE-PORT <external port> RULE <id> DEFAULT
                                          PORT <port number>
                                          IP <IP address>


NO SUBNET <IP address> <IP mask> RULE <id>
   SUBNET <IP address> <IP mask> RULE <id> DEFAULT
                                           GATEWAY <IP address>
                                           NO GATEWAY

NO VIRTUAL-IP <IP address> RULE <id>
   VIRTUAL-IP <IP address> RULE <id> DEFAULT
                                     FIRST-PORT <port number>
                                     MAXIMUM-NUMBER-OF-PORTS <number>
                                     REAL-IP <IP address>
                                     NO FIRST-PORT
                                     NO MAXIMUM-NUMBER-OF-PORTS
                                     NO REAL-IP <IP address>
```

Capítulo 3
Monitorización de la facilidad NAPT



1. Monitorización de la facilidad NAPT

El acceso al menú de monitorización de la facilidad de NAPT se realiza a través del menú de monitorización de IP, mediante los siguientes comandos:

```
*P 3
+PROTOCOL IP
IP>NAPT
NAPT>
```

Los comandos disponibles en el entorno de monitorización de la facilidad NAPT son lo siguientes:

Comando	Función
? (AYUDA)	Lista los comandos u opciones disponibles.
DELETE	Realiza el purgado de diferentes parámetros.
LIST	Muestra los distintos parámetros de monitorización de la facilidad NAPT.
EXIT	Sale del prompt de monitorización de la facilidad NAPT.

En general, si no se introducen en la línea de comandos todos los parámetros necesarios para completar un comando, el equipo los irá solicitando.

1.1. ? (AYUDA)

Este comando muestra 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:

```
NAPT>?
```

Ejemplo:

```
NAPT>?
DELETE
LIST
EXIT
NAPT>
```

1.2. DELETE

El comando **DELETE** del menú de monitorización de NAPT permite purgar diferentes parámetros.

Sintaxis:

```
NAPT>DELETE ?
ADDRESS
ENTRIES
IDENTS
NAPT>
```

a) DELETE ADDRESS

Borra las entradas NAPT utilizadas por una determinada dirección IP.

Ejemplo:

```
NAPT>DELETE ADDRESS
IP address [0.0.0.0]? 172.24.0.1
```

b) DELETE ENTRIES

Borra todas las entradas NAPT utilizadas.

Ejemplo:

```
NAPT>DELETE ENTRIES
```

c) DELETE IDENTS

Borra todos los identificadores ICMP utilizados.

Ejemplo:

```
NAPT>DELETE IDENTS
```

1.3. LIST

El comando **LIST** del menú de monitorización de NAPT muestra los distintos parámetros de monitorización asociados.

Sintaxis:

```
NAPT>LIST ?
ADDRESS
ALL
ENTRIES
IDENTS
STATISTICS
```

a) LIST ADDRESS

Muestra las entradas NAPT utilizadas por una determinada dirección IP.

Ejemplo:

```
NAPT>LIST ADDRESS
IP address [0.0.0.0]? 172.24.0.1

172.24.0.1 NAPT Entries:
 src 172.24.0.1:1291 => conn 200.200.200.1:32779, age 5, flags 0x1
 src 172.24.0.1:1290 => conn 200.200.200.1:32778, age 2, flags 0x7
 src 172.24.0.1:1289 => conn 200.200.200.1:32777, age 5, flags 0x1
 src 172.24.0.1:1288 => conn 200.200.200.1:32776, age 2, flags 0x7
 src 172.24.0.1:1287 => conn 200.200.200.1:32775, age 5, flags 0x1
 src 172.24.0.1:1286 => conn 200.200.200.1:32774, age 2, flags 0x7
 src 172.24.0.1:1285 => conn 200.200.200.1:32773, age 5, flags 0x1
 src 172.24.0.1:1284 => conn 200.200.200.1:32772, age 2, flags 0x7
 src 172.24.0.1:1283 => conn 200.200.200.1:32771, age 5, flags 0x1
 src 172.24.0.1:1282 => conn 200.200.200.1:32770, age 2, flags 0x7
 src 172.24.0.1:1281 => conn 200.200.200.1:32769, age 5, flags 0x1
 src 172.24.0.1:1280 => conn 200.200.200.1:32768, age 2, flags 0x7

172.24.0.1 uses 12 NAPT entries

NAPT>
```

b) LIST ALL

Muestra toda la información de monitorización de NAPT.

Ejemplo:

```
NAPT>LIST ALL

 Internal Address         External Address       Age  Flags  Delta
 ---------------------    ---------------------  ---- ------ -----
 172.24.5.197   :1305  => 200.200.200.1  :32793     5 0x0001 0 0
 172.24.5.197   :1304  => 200.200.200.1  :32792     2 0x0007 2 3
 172.24.5.197   :1303  => 200.200.200.1  :32791     5 0x0001 0 0
 172.24.5.197   :1302  => 200.200.200.1  :32790     2 0x0007 2 3
 172.24.5.197   :1301  => 200.200.200.1  :32789     5 0x0001 0 0
 172.24.5.197   :1300  => 200.200.200.1  :32788     2 0x0007 2 3
 172.24.5.197   :1299  => 200.200.200.1  :32787     5 0x0001 0 0
 172.24.5.197   :1298  => 200.200.200.1  :32786     2 0x0007 2 3
 172.24.5.197   :1297  => 200.200.200.1  :32785     5 0x0001 0 0
 172.24.5.197   :1296  => 200.200.200.1  :32784     2 0x0007 2 3
 172.24.5.197   :1292  => 200.200.200.1  :32780     2 0x0007 2 3
 172.24.0.1     :1291  => 200.200.200.1  :32779     1 0x0001 0 0
 172.24.0.1     :1289  => 200.200.200.1  :32777     1 0x0001 0 0
 172.24.0.1     :1287  => 200.200.200.1  :32775     1 0x0001 0 0
 172.24.0.1     :1285  => 200.200.200.1  :32773     1 0x0001 0 0
 172.24.0.1     :1283  => 200.200.200.1  :32771     1 0x0001 0 0
 172.24.0.1     :1281  => 200.200.200.1  :32769     1 0x0001 0 0


 Internal Ident            External Ident          Age
 ----------------------    ----------------------  ---
 172.24.5.197   [  256] => 200.200.200.1  [    2]    2
 172.24.0.117   [  256] => 200.200.200.1  [    3]    2


Memory:
Reserved port-address structures ---- 1024
Used port-address structures -------- 4
Reserved ident-address structures --- 16
Used ident-address structures ------- 1

Port information:
Number of used ports ---------------- 17
Number of free ports ---------------- 1007
Maximum used ports ------------------ 614

Ident information:
Number of used idents --------------- 1
Number of free idents --------------- 15
Maximum used idents ----------------- 3

Packets not processed because of:
Bad version ------------------------- 0
Bad header length ------------------- 0
Bad checksum ------------------------ 0
Bad tcp checksum -------------------- 0
Received ports out of range --------- 17
Received idents out of range -------- 0
Wrong target IP address ------------- 0

NAPT>
```

c) ***LIST ENTRIES***

Muestra todas las entradas NAPT utilizadas.

Ejemplo:

```
NAPT>LIST ENTRIES

 Internal Address         External Address       Age  Flags  Delta
 ---------------------    ---------------------  ---- ------ -----
 172.24.5.197   :1305  => 200.200.200.1  :32793     5 0x0001 0 0
 172.24.5.197   :1304  => 200.200.200.1  :32792     2 0x0007 2 3
 172.24.5.197   :1303  => 200.200.200.1  :32791     5 0x0001 0 0
```

```
 172.24.5.197   :1302  => 200.200.200.1  :32790     2 0x0007 2 3
 172.24.5.197   :1301  => 200.200.200.1  :32789     5 0x0001 0 0
 172.24.5.197   :1300  => 200.200.200.1  :32788     2 0x0007 2 3
 172.24.5.197   :1299  => 200.200.200.1  :32787     5 0x0001 0 0
 172.24.5.197   :1298  => 200.200.200.1  :32786     2 0x0007 2 3
 172.24.5.197   :1297  => 200.200.200.1  :32785     5 0x0001 0 0
 172.24.5.197   :1296  => 200.200.200.1  :32784     2 0x0007 2 3
 172.24.5.197   :1295  => 200.200.200.1  :32783     5 0x0001 0 0
 172.24.5.197   :1294  => 200.200.200.1  :32782     2 0x0007 2 3
 172.24.5.197   :1293  => 200.200.200.1  :32781     5 0x0001 0 0
 172.24.5.197   :1292  => 200.200.200.1  :32780     2 0x0007 2 3
 172.24.0.1     :1291  => 200.200.200.1  :32779     1 0x0001 0 0
 172.24.0.1     :1289  => 200.200.200.1  :32777     1 0x0001 0 0
 172.24.0.1     :1287  => 200.200.200.1  :32775     1 0x0001 0 0
 172.24.0.1     :1285  => 200.200.200.1  :32773     1 0x0001 0 0
 172.24.0.1     :1283  => 200.200.200.1  :32771     1 0x0001 0 0
 172.24.0.1     :1281  => 200.200.200.1  :32769     1 0x0001 0 0

NAPT>
```

d) LIST IDENTS

Muestra los identificadores ICMP traducidos mediante NAPT.

Ejemplo:

```
NAPT>LIST IDENTS

 Internal Ident            External Ident          Age
 ----------------------    ----------------------  ---
 172.24.5.197   [  256] => 200.200.200.1  [    2]    2
 172.24.0.117   [  256] => 200.200.200.1  [    3]    2

NAPT>
```

e) LIST STATISTICS

Muestra los distintos estadísticos de NAPT.

Ejemplo:

```
NAPT>LIST STATISTICS

Memory:
Reserved port-address structures ---- 1024
Used port-address structures -------- 4
Reserved ident-address structures --- 16
Used ident-address structures ------- 1

Port information:
Number of used ports ---------------- 4
Number of free ports ---------------- 1020
Maximum used ports ------------------ 614

Ident information:
Number of used idents --------------- 1
Number of free idents --------------- 15
Maximum used idents ----------------- 3

Packets not processed because of:
Bad version ------------------------- 0
Bad header length ------------------- 0
Bad checksum ------------------------ 0
Bad tcp checksum -------------------- 0
Received ports out of range --------- 15
Received idents out of range -------- 0
Wrong target IP address ------------- 0

NAPT>
```

El significado de los estadísticos es el siguiente:

Reserved port-address structures	Estructuras NAPT reservadas en memoria (debe coincidir con el número de entradas NAPT configuradas salvo en el caso de que se sobrepase el puerto máximo permitido).
Used port-address structures	Estructuras NAPT utilizadas.
Reserved ident-address structures	Estructuras de identificadores ICMP reservadas en memoria.
Used ident-address structures	Estructuras de identificadores ICMP utilizadas.
Number of used ports	Puertos utilizados.
Number of free ports	Puertos disponibles.
Maximum used ports	Número máximo de puertos que se han llegado a utilizar.
Number of used idents	Identificadores ICMP utilizados.
Number of free idents	Identificadores ICMP disponibles.
Maximum used idents	Número máximo de identificadores ICMP que se han llegado a utilizar.
Bad version	Paquetes con versión de IP incorrecta.
Bad header length	Paquetes con longitud de cabecera IP incorrecta.
Bad checksum	Paquetes con checksum de IP incorrecto.
Bad tcp checksum	Paquetes con checksum de TCP incorrecto.
Received ports out of range	Paquetes dirigidos a puertos fuera del rango permitido.
Received idents out of range	Paquetes destinados a identificadores ICMP fuera del rango permitido.
Wrong target IP address	Paquetes no dirigidos a direcciones de las conexiones IP.

1.4. EXIT

El comando **EXIT** permite salir del entorno de monitorización de la facilidad NAPT.

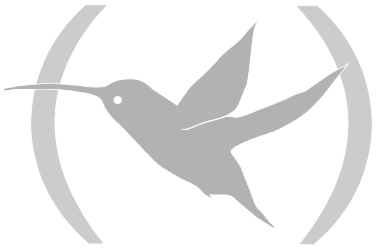
Sintaxis:

```
NAPT>EXIT
```

Ejemplo:

```
NAPT>EXIT
IP>
```

Capítulo 4
Ejemplo de configuración de la facilidad NAPT



1. Descripción del ejemplo de configuración

Supóngase que se desea configurar un dominio privado de forma que un router interconecte una oficina central con tres oficinas, y permita el acceso tanto al dominio público como al dominio privado, con dos conexiones que hagan uso de la facilidad NAPT, a través de un enlace Punto a Multipunto. A continuación se describen las características de las distintas conexiones.

En la oficina central está localizado el router que interconecta ambos dominios. Se establecen dos conexiones de NAPT con distintas características. La dirección de acceso al dominio público es la dirección IP 200.12.100.129 con máscara de clase C (255.255.255.0). Al tratarse de un enlace Punto a Multipunto las direcciones remotas de ambos circuitos deben estar especificadas para que el equipo sea capaz de distinguir por cuál de los circuitos va a comunicarse con el resto de la red. Además deben pertenecer a la misma subred. Estas direcciones son 200.12.100.27 y 200.12.100.18.

1.1. Configuración de las oficinas

a) Configuración de la oficina central

La red del dominio privado de la oficina central es una red definida con direcciones privadas (RFC 1918) de clase C, pertenecientes a la subred 192.168.27.0.

Esta oficina está conectada a las otras tres oficinas a través de los siguientes enlaces:

(Oficina Central, Oficina 1) === (172.16.1.1/24, 172.16.1.2/24)
(Oficina Central, Oficina 2) === (172.16.2.1/24, 172.16.2.2/24)
(Oficina Central, Oficina 3) === (172.16.3.1/24, 172.16.3.2/24)

Las redes locales de las Oficinas 1, 2, 3 también están definidas con direcciones privadas (RFC 1918) de clase C, pertenecientes a las subredes 192.168.28.0, 192.168.29.0, y 192.168.30.0.

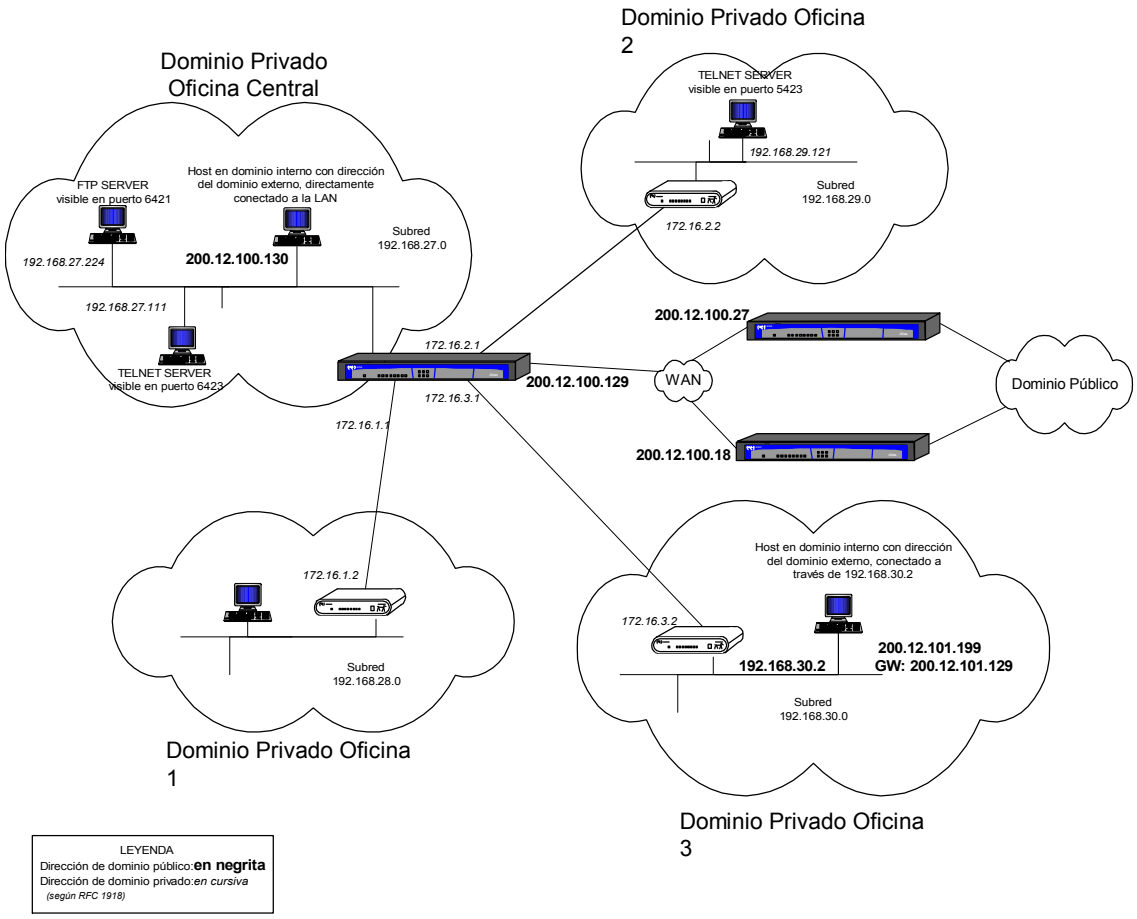
b) Configuración de los enlaces NAPT

Para mostrar las posibilidades de NAPT los enlaces que interconectan la oficina central del dominio privado con el dominio público, se configuran de distinta forma.

Así, para las conexiones por el enlace (200.12.100.129, 200.12.100.27), se hace accesible un servidor FTP instalado en el host 192.168.27.224 visible desde el puerto 6421 y además el servidor de Telnet del host 192.168.27.111 a través del puerto 6423. También se hace visible un servidor de Telnet de la Oficina 2, de dirección IP 192.168.29.121 a través del puerto 5423. Por último, esta conexión de NAPT da acceso a una subred visible accesible a través de la Oficina 3, con dirección de subred 200.12.101.128 máscara 255.255.255.128 y accesible desde 192.168.30.2. Además se habilita la capacidad de firewall para esta conexión, es decir que se ocultan los puertos de Telnet, DNS, FTP, etc para el tráfico entrante por este enlace.

Para las conexiones por el enlace (200.12.100.129, 200.12.100.18) se hacen accesibles direcciones públicas que están en el dominio privado en forma de subred visible, directamente conectada a la LAN del router de acceso con dirección de subred 200.12.100.128 y máscara 255.255.255.128.

La red resultante queda como se muestra en la figura:



Los pasos a seguir para configurar la facilidad NAPT en el router de acceso para que el entorno descrito anteriormente se encuentre operativo son los que se describen a continuación.

1.2. Configuración de las reglas de NAPT

En el menú de configuración de IP:

```
*P 4

Config>PROTOCOL IP

-- Internet protocol user configuration --
IP config>rule 1 local-ip 200.12.100.129
IP config>rule 1 remote ip 200.12.100.27
IP config>rule 1 napt translation
IP config>rule 1 napt firewall
IP config>rule 2 local-ip 200.12.100.129
IP config>rule 2 remote-ip 200.12.100.18
IP config>rule 2 napt translation
IP config>route 200.12.101.128 255.255.255.128 192.168.30.2 1
```

NOTA: La primera de las reglas definidas es la que hace que el router de acceso actúe de firewall, no dejando acceder a sus puertos estándar.

1.3. Configuración del enlace (200.12.100.129, 200.12.100.27)

Para cumplir los requisitos exigidos para el enlace (200.12.100.129, 200.12.100.27) es necesario configurar tres puertos visibles, para permitir el acceso a los puertos de Telnet de las direcciones IP 192.168.27.111 y 192.168.29.121 y al de FTP con dirección IP 192.168.27.224. Los puertos empleados para ello son respectivamente 6423, 5423 y 6421.

A la hora de configurar los puertos y las subredes visibles será necesario introducir el identificador de la regla IP asociada que se ha creado previamente en el menú de configuración de IP. Por ese motivo se muestran las reglas IP disponibles.

NOTA: Con todos los puertos que el router tenga capturados por tener servicios en dichos puertos es necesario hacer la asignación de puertos que se muestra en el ejemplo para los puertos FTP y Telnet.

a) Configuración de los Puertos Visibles

En este ejemplo, el identificador de la regla que define el enlace que se está configurando (200.12.100.129, 200.12.100.27) es el 1. Para configurar los puertos visibles como el entorno especifica hay que introducir:

```
IP config>NAT PAT

-- NAPT configuration --
NAPT config>VISIBLE-PORT 6423 RULE 1 PORT 23 IP 192.168.27.111
NAPT config>VISIBLE-PORT 6421 RULE 1 PORT 21 IP 192.168.27.224 FTP
NAPT config>VISIBLE-PORT 5423 RULE 1 PORT 23 IP 192.168.29.121
NAPT config>
```

b) Configuración de la Subred Visible

No hace falta introducir gateway porque la subred no está directamente conectada.

```
NAPT config>SUBNET 200.12.101.128 255.255.255.128 RULE 1 DEFAULT
NAPT config>
```

En el menú de configuración de ARP del router de la oficina 3:

```
*P 4
Config>PROTOCOL ARP
ARP config>entry ethernet0/0 200.12.101.129 00-A0-26-43-3C-7C public
ARP config>
```

donde la dirección MAC es la del router de la Oficina 3

1.4. Configuración del enlace (200.12.100.129, 200.12.100.18)

Para cumplir los requisitos que el entorno define para este enlace se debe realizar lo siguiente.

a) Configuración de la Subred Visible

El identificador de la regla que define el enlace (200.12.100.129, 200.12.100.18) es el 2. Por ello, para configurar las subredes visibles es necesario configurar el gateway en la subred visible porque dicha subred está directamente conectada y el interfaz directamente conectado no tiene dirección en dicha subred.

```
NAPT config>SUBNET 200.12.100.128 255.255.255.128 RULE 1 GATEWAY 200.12.100.129
NAPT config>
```

En el menú de configuración de IP del router de acceso se efectúa lo siguiente:

```
IP config>ROUTE 200.12.100.128 255.255.255.128 ethernet0/0 1
```