Teldat Router

NAPT Facility

Doc. *DM735-I* Rev. *10.00*
December, 2002

INDEX

Chapter 1
Introduction

1. Introduction to the NAPT facility

Network Address Translation is a method by which IP addresses are mapped from one address realm to another, providing transparent routing to the various network stations. Traditionally, the NAT devices are used to isolate address realms with non-registered private addresses in external realms with unanimously assigned unique addresses.

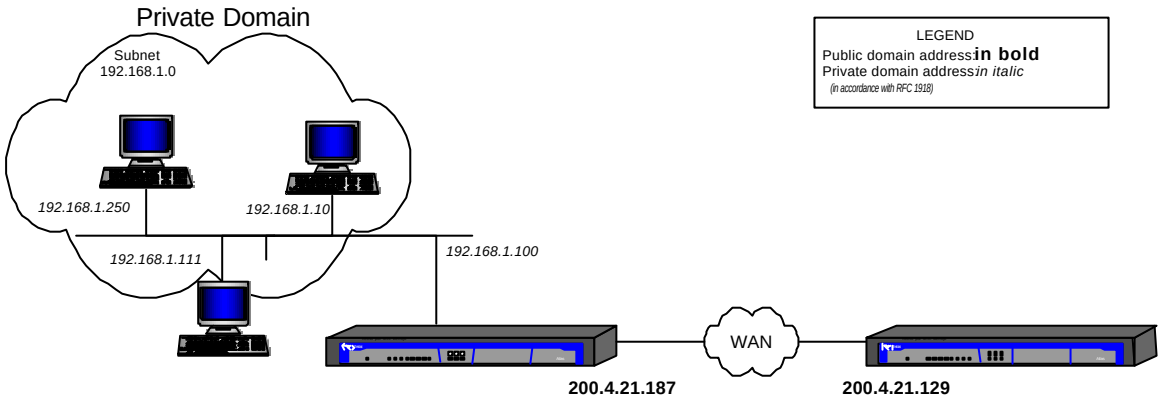
There are many variations of address translation that lend themselves to distinct applications. However all flavors of NAT devices should share the following characteristics:

a) Transparent Address assignment.

b) Transparent routing through address translation (routing here refers to forwarding packets and not exchanging routing information RIP, OSPF, etc).

c) ICMP error packet payload translation.

The typical NAT scenario is described below. In this example, you can see a router performing NAT that is connected to an Internet Service Provider through another router pertaining to the supplier's WAN (Wide Area Network).



NAPT (Network Address Port Translation) extends the notion of translation one step further by also translating transport identifier (TCP and UDP ports or the ICMP identifiers). This allows the transport identifiers of a number of private hosts to be multiplexed through other transport identifiers with a single address common to all. This can be combined with the basic NAT (Network Address Translation).

For packets outbound from the private network, NAPT translates the source IP address, source transport identifier and updates fields related to the distinct checksums of the implicated packets (IP, UDP, TCP or ICMP). The transport identifiers can be UDP/TCP ports or ICMP petition identifiers. For packets inbound to the private domain, the destination address and the transport identifiers are translated and the checksums for the implicated packets are recalculated.

Algorithms to recalculate the checksums in differential mode are taken from the RFC 1361 (IP Network Address Translator).

2. NAPT Exceptions

Two exceptions to NAPT occur when the private domain finds itself with determined needs.

2.1. Visible Ports

Imagine that the private domain wishes to facilitate access to an FTP server who is placed in the local network segment of the private domain itself. If the external or global domain tries to access the server's FTP port, the packets will be captured by the router providing access in such a way that the initial FTP server cannot be reached by the external domain.

To avoid this situation, what it does is "**advertise**" the server's FTP port (found in the private domain) in the access router with another port reserved for this server. To do this, you need to establish the following association:

(Internal Address, Internal port) ⟷ External Port

which in the case of an FTP server could be:

(192.168.1.21, 21) ⟷ 6400

In this way, the router's public address provides access to the destination port 6400 (the advertised port providing access to the FTP server). Through NAPT the destination address is translated to that of the server itself and to the destination port 21 (standard FTP port) making the FTP connection possible with the said server.

For analog, you proceed as if you wished to make the Telnet ports from various devices in the private network public or other services where packets destined to standard ports are captured by the access router.

You can "advertise" standard ports already captured by the access router (e.g. FTP or TELNET) provided that the port captured by the device has been previously moved i.e. if you do not wish the connections to the public address default TELNET port (23) to correspond to a connection to the router TELNET server but to a connection to a TELNET server for a private domain device, you must move the router service port (e.g. to port 8023) and advertise in the standard port.

If you do not move the router port, you will lose access to the router server for the connection carried out by NAPT.

2.2. Visible Subnets

The other exception to NATP is the case where there is a group of addresses pertaining to the public domain available and you wish them to be accessible from the domain through the access router carrying out NAPT.

Chapter 2
NAPT Facility Configuration

1. NAPT facility configuration

Access to the NAPT facility configuration menu is carried out through the IP configuration menu through the following commands:

```
*P 4
Config>PROTOCOL IP

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

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

The NAPT rules are directly added or deleted from the IP configuration menu. For further information on this, please see the associated manual Dm 702-I. The rest of the configuration for this facility is executed from the NAPT configuration menu.

A description of how to configure the distinct possibilities offered by NAPT is given below.

The commands are defined complying with the following nomenclature:

`RULE`	Mandatory part.
<rule id>	Mandatory part to be determined by the user.
`[NO]`	Optional part.

1.1. Creating a visible port

The purpose of configuring a visible port is to permit the entry of packets coming from the external domain destined to a determined port (external port) and redirect them to an internal domain IP address to a determined port (internal port).

The command used to configure a visible port is as follows:

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

External Port: This is the visible connection port from the external domain to access the service in the host specified by the address and internal port.

Rule Identifier: This is the identifier for the rule you wish to make visible in a determined port.

Internal Port: This is the internal host destination port.

IP Host address: This is the internal domain host IP address.

If you set the value 0 as external port and internal port, this is defined so the router will redirect, towards the indicated address, traffic entering through the connection affected by the NAPT which will by default discard; this IP address will be converted into the destination for all traffic destined to ports unknown to the router.

Additionally, there is the `DEFAULT` option which establishes the default values for the visible port, i.e. internal port 0 to the generic internal address 0.0.0.0

Examples:

Redirect external port 80 (HTTP) pertaining to the connection affected by the NAPT rule number 1 to the internal address 192.168.1.5 port 80: through this configuration the HTTP connections carried out with the router through the connection affected by the NAPT rule 1 to the HTTP default port are redirected to an internal HTTP server (if you have not changed the router HTTP server port, you will not be able to access the router HTTP server through the connection affected by the NAPT rule number 1).

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

Redirect external port 8021 pertaining to the router connection affected by the NAPT rule 1 to the internal address 192.168.1.5 port 21: through this configuration the connection carried out with the router through the connection affected by the NAPT rule number 1 to port 8021 will really constitute an FTP connection to the internal server 192.168.1.5.

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

1.2. Modifying a visible port

The command used to modify a visible port is as follows:

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

Internal new port: if this is different to the previously configured port, it is substituted for the indicated port.

New IP Host address: if this is different to the previously configured address, it is substituted for the indicated address.

Example:

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

1.3. Deleting a visible port

The command used to delete a visible port is as follows:

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

Example:

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

1.4. Listing the configured visible ports

The command used to list the configured visible ports is as follows:

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

Example:

```
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. Creating a visible subnet

The purpose of configuring a visible subnet is to provide total transparency towards and from determined internal domain addresses. For these addresses the router behaves as if NAPT is not configured.

The command used to configure a visible subnet is as follows:

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

Visible subnet IP address: This is the IP address of the subnet you are going to make visible through the connection defined by the NAPT rule.

Visible subnet mask: This is the mask for the subnet you are going to make visible through the connection defined by the NAPT rule.

Rule Identifier: This is the identifier for the rule. The configured rules appear previously listed.

Default router (optional): In cases where the visible subnet has to be directly connected to the access router through an interface that does not have an address in the said subnet, in this field you must configure a visible subnet address (specifically the visible subnet hosts default route) so the access router responds to the ARP petitions from the subnet hosts. If the subnet is not directly connected or the router has a visible subnet address in the interface directly connected to the said subnet assigned, then this field must be left with the default value (0.0.0.0) in order to avoid using a visible subnet address in the said interface and permit correct functionality in the environment.

The `DEFAULT` option establishes the default parameters (in this case, the only parameter is `GATEWAY` which is configured as 0.0.0.0, i.e. equivalent to `NO GATEWAY`).

Example:

Makes the subnet not directly connected 200.12.100.128/25 visible through the connection affected by the NAPT rule number 1: through this configuration traffic coming from or destined to the said subnet passing through the router via the connection affected by the NAPT rule number 1 is transparent.

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

Makes the subnet directly connected 200.12.100.128/25 with the default router 200.12.100.129 visible through the connection affected by the NAPT rule number 1, connection that specifically has address 200.12.100.129 assigned; this scenario is typical in WAN accesses where the ISP provides a group of public addresses: the WAN interface will have an address for the said subnet: NAPT must be configured in order to permit access to the exterior for those devices with private addressing located in the internal domain at the same time as having transparent access to devices associated to the assigned subnet addresses.

Example:

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

1.6. Modifying a visible subnet

You can only modify the "gateway" parameter for a defined visible subnet. The command used to modify the gateway is the same one used to define a visible subnet with the peculiarity that the subnet address and mask coincide with the values of an already defined visible subnet.

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

Given that there is only one parameter that can be configured in the visible subnets (`GATEWAY`), the commands `DEFAULT` o `NO GATEWAY` can be equally used.

Example:

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

or

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

1.7. Deleting a visible subnet

The command used to delete a visible subnet is as follows:

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

Example:

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

1.8. Listing the configured visible subnets

The command used to list the visible subnets is as follows:

```
NAPT config>LIST SUBNET
```

Example:

```
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. Enabling and disabling NAPT

You can globally enable or disable the NAPT facility through the following commands:

```
NAPT config>ENABLE
```

or

```
NAPT config>DISABLE
```

or

```
NAPT config>NO ENABLE
```

Example:

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

or

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

1.10. Listing the NAPT state

The command used to list the state of the NAPT facility is as follows:

```
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. Configuring the range of ports to be used

The router offers the possibility of defining the range of ports to be used by the NAPT through two configuration parameters: the first port and the number of ports to be used.
The commands used to configure the port range are as follows:

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

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

Example:
Here we are going to duplicate the number of ports available for NAPT and configure the first port as 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>
```

NOTE: The greater the number of NAPT entries, the more the internal domain host can access simultaneous the external domain. However more device resources will be needed to be used (memory, processing capacity, etc.).

NOTE: Due to the fact that the maximum port that can be used is 65535 (OxFFFF), if the configuration of the Initial Port and the Number of NAPT Entries exceed the maximum port value, the number of NAPT entries is internally limited to the value comprising of the Initial Port and 65535.

1.12. Listing the configured range of NAPT ports

The command used to list the range of NAPT ports is as follows:

```
NAPT config>LIST CONFIGURATION
```

Example:

```
NAPT config>LIST CONFIGURATION

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

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

NAPT config>
```

1.13. EXIT

The **EXIT** command permits you to exit the NAPT facility configuration environment.

```
NAPT config>EXIT
```

Example:

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

2. Commands summary

```
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>
```

Chapter 3
NAPT Facility Monitoring

1. NAPT Facility Monitoring

The NAPT facility monitoring menu is accessed via the IP monitoring menu through the following commands:

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

The commands available in the NAPT facility monitoring environment are as follows:

Command	Function
? (HELP)	Lists the available commands or their options.
DELETE	Carries out debugging for different parameters.
LIST	Displays the distinct NATP facility monitoring parameters.
EXIT	Exits the NAPT facility monitoring prompt.

As a general rule, if you do not introduce all the necessary parameters in the command line in order to complete a command, the device will prompt you for them.

1.1. ? HELP

This command displays the commands valid at the level where the router is programmed. You can also use this command after a specific command to list the available options.

Syntax:

```
NAPT>?
```

Example:

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

1.2. DELETE

The **DELETE** command found in the NAPT monitoring menu permits you to debug different parameters.

Syntax:

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

a) DELETE ADDRESS

Deletes the NAPT entries used by a determined IP address.

Example:

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

b) DELETE ENTRIES

Deletes all the used NAPT entries.

Example:

```
NAPT>DELETE ENTRIES
```

c) DELETE IDENTS

Deletes all the used ICMP identifiers.

Example:

```
NAPT>DELETE IDENTS
```

1.3. LIST

The **LIST** command found in the NAPT monitoring menu displays the distinct associated monitoring parameters.

Syntax:

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

a) LIST ADDRESS

Displays the NAPT entries used for a determined IP address.

Example:

```
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

Displays all the NAPT monitoring information.

Example:

```
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

Displays all the used NAPT entries.

Example:

```
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

Displays all the ICMP identifiers translated through NAPT.

Example:

```
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

Displays the distinct NAPT statistics.

Example:

```
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>
```

The meaning of the statistics is as follows:

Reserved port-address structures	NAPT structures reserved in memory (this must coincide with the number of NAPT entries configured except in cases where this exceeds the maximum permitted port).
Used port-address structures	Used NAPT structures.
Reserved ident-address structures	ICMP identifier structures reserved in memory.
Used ident-address structures	Used ICMP identifier structures.
Number of used ports	Used ports.
Number of free ports	Available ports.
Maximum used ports	Maximum number of ports that have been used.
Number of used idents	Used ICMP identifiers.
Number of free idents	Available ICMP identifiers.
Maximum used idents	Maximum number of ICMP identifiers that have been used.
Bad version	Packets with incorrect IP version.
Bad header length	Packets with incorrect IP header length.
Bad checksum	Packets with incorrect IP checksum.
Bad tcp checksum	Packets with incorrect TCP checksum.
Received ports out of range	Packets addressed to out of permitted range ports.
Received idents out of range	Packets destined to out of permitted range ICMP identifiers.
Wrong target IP address	Packets not addressed to the IP connection addresses.

1.4. EXIT

The **EXIT** command permits you to exit the NAPT facility monitoring environment.

Syntax:

```
NAPT>EXIT
```

Example:

```
NAPT>EXIT
IP>
```

Chapter 4
Example of NAPT Facility Configuration

1. Description of the configuration example

Supposing you wish to configure a private domain in such a way that a router interconnects a central office with three branches and permits access to both the public and private domain with two connections making use of the NAPT facility through a Point to Multipoint link. The characteristics of the distinct connections are described below.

The router permitting the communication between the public and private domains is located in the central office. Two NAPT connections are established with distinct characteristics. The access address to the public domain is the IP address 200.12.100.129. The mask for this address is class C (255.255.255.0). When dealing with a Point to Multipoint link, the remote addresses for both circuits should be specified so that the device is capable of distinguishing which circuit is going to communicate with the rest of the network. Furthermore they must pertain to the same subnet. These addresses are 200.12.100.27 and 200.12.100.18.

1.1. Configuration of the offices

a) Central office configuration

The central office's private domain network is a network defined with class C private addresses (RFC 1918) pertaining to the subnet.

This office is connected to the other three branches through the following links:

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

The local networks for Branches 1, 2 and 3 are also defined with class C private addresses (RFC 1918) pertaining to the subnets 192.168.28.0, 192.168.29.0, and 192.168.30.0

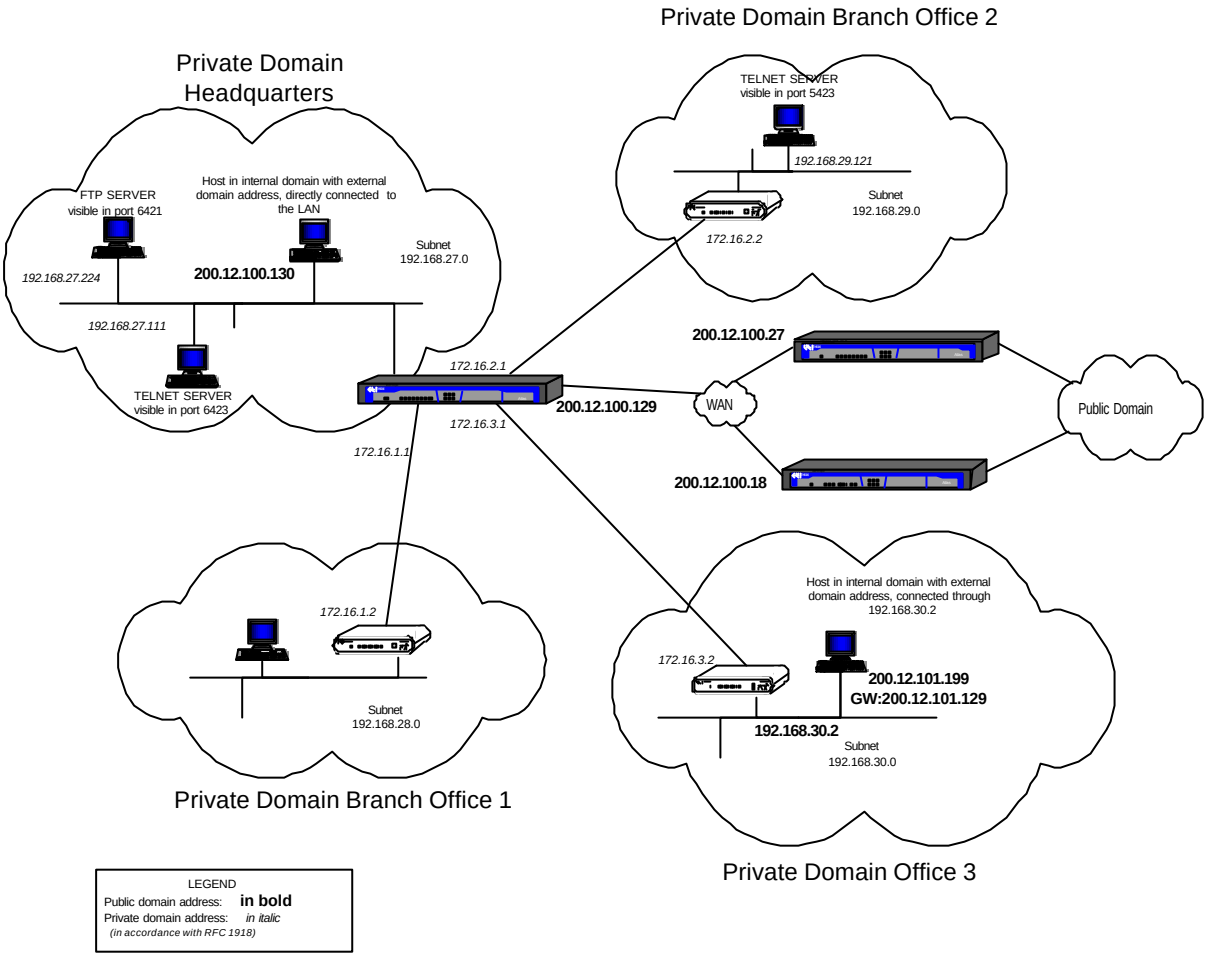
b) Configuration of the NAPT links

In order to display the NAPT possibilities, the links interconnection the private domain central office with the public domain are configured in a different way.

In this way, for connections through the link (200.12.100.129, 200.12.100.27), you wish to make accessible to an FTP server installed in the host (address 192.168.27.224) which is visible from port 6421 and host Telnet server 192.168.27.111 through port 6423. Also a Telnet service in Office 2 192.168.27.111 through port 6423 needs to be made visible. Lastly this NAPT connection provides access to a visible subnet accessible by Office 3 with subnet address 200.12.101.128 mask 255.255.255.128 and accessible from 192.168.30.2. The firewall capability is also enabled from this connection, i.e. the ports (Telnet, DNS, FTP etc.) are hidden from incoming traffic through this link.

For connections through link (200.12.100.129, 200.12.100.18) you wish to make accessible public addresses within the private domain in the form of a visible subnet, directly connected to the access router LAN with the subnet address 200.12.100.128 and mask 255.255.255.128.

The resulting network is as shown below:



The steps to take in order to configure the NAPT facility in the access router so that the previously described environment is operative are explained.

1.2. Configuration of the NAPT rules

In the NAPT configuration menu:

```
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
```

NOTE: The first defined rule makes the access router act as a firewall; these standard ports cannot be accessed

1.3. Configuration of link (200.12.100.129, 200.12.100.27)

In order to comply with the needs demanded by the link (200.12.100.129, 200.12.100.27) you must configure three visible ports in order to permit access to both the Telnet port with IP addresses 192.168.27.111 and 192.168.29.121 and the FTP port with IP address 192.168.27.224. The ports used for this are 6423, 5423 and 6421 respectively.

When configuring the ports and visible subnets, you must introduce the associated IP rule identifier previously created in the IP configuration menu. The available IP rules are displayed for this reason.

NOTE: With all the ports the router has captured in order to have services set up in them, you need to carry out port mapping as shown in the example for the FTP and Telnet ports.

a) Configuration of Visible Ports

In this example, the rule identifier defining the link (200.12.100.129, 200.12.100.27) you are configuring is 1. In order to configure the visible ports as the environment specifies you need to enter:

```
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) Configuring the Visible Subnet

You do not need to introduce the gateway, as the subnet is not directly connected.

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

In the ARP configuration menu for the office 3 router:

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

Where the MAC address is the same as the Office 3 router.

1.4. Configuration of link (200.12.100.129, 200.12.100.18)

In order to comply with the needs defined by the environment for this link, you need to carry out the following.

a) *Configuring the Visible Subnet*

The rule identifier defining this link (200.12.100.129, 200.12.100.18) is 2. In order to configure the visible subnets you need to configure the gateway in the visible subnet as this subnet is directly connected and the directly connected interface does not have an address in this subnet.

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

In the access router IP configuration menu, the following is carried out:

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