NAPT Feature

bintec Dm735-I

Legal Notice

Warranty

This publication is subject to change.

bintec offers no warranty whatsoever for information contained in this manual.

bintec is not liable for any direct, indirect, collateral, consequential or any other damage connected to the delivery, supply or use of this manual.

Table of Contents

I Related Documents

bintec Dm702-I TCP-IP

Chapter 1 Introduction

1.1 Introduction to the NAPT feature

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 from external realms with globally 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:

- Transparent address assignment.
- Transparent routing through address translation (routing here refers to forwarding packets and not exchanging routing information RIP, OSPF, etc).
- ICMP error packet payload translation.

A typical NAT scenario is described below. In this example, we have a router performing NAT that is connected to an Internet Service Provider through another router belonging to the supplier's WAN (Wide Area Network).

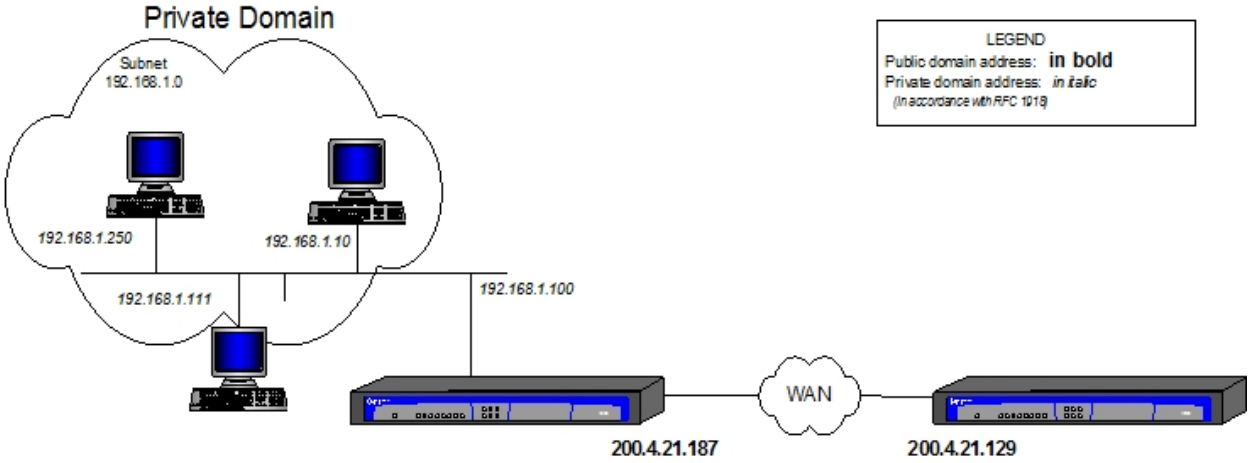

Fig. 1: **NAT scenario**

NAPT (Network Address Port Translation) extends the notion of translation by also translating the transport identifier (TCP and UDP ports or ICMP identifiers). This allows 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 basic NAT (Network Address Translation).

For outbound packets from a private network, NAPT translates the source IP address and source transport identifier and updates the fields corresponding to the different checksums of the implicated packets (IP, UDP, TCP or ICMP). The transport identifiers can be UDP/TCP ports or ICMP petition identifiers. For inbound packets 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 RFC 1361 (IP Network Address Translator).

1.2 NAPT exceptions

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

1.2.1 Visible ports

Imagine that the private domain wishes to allow access to an FTP server 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, establish the following association:

(Internal Address, Internal port) <---> External Port

which in the case of an FTP server is:

(192.168.1.21, 21) <---> 6400

Thus, all connections to the router's public address on destination port 6400 (the advertised port providing access to the FTP server) are translated, through NAPT, to the server's address on destination port 21 (standard FTP port) making an FTP connection to the server possible.

Proceed in a similar fashion if you want to make the Telnet ports of different devices in the private network public, or other services where the packets bound for standard ports are captured by the access router.

Note

You can advertise standard ports already captured by the access router (e.g., FTP or TELNET) provided that the captured port has been previously moved, i.e., if you do not want connections to 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 lose access to the router server for the connection through NAPT.

1.2.2 Visible subnets

The other exception to NAPT is where there is a group of addresses available in the public domain and you want them to be accessible through the access router performing NAPT.

Chapter 2 NAPT Feature Configuration

2.1 NAPT feature configuration

Access the NAPT feature configuration menu via 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, please see associated manual bintec Dm702-I TCP-IP. The rest of the configuration is carried out from the NAPT configuration menu.

A description of how to configure the various options offered by NAPT is given below.

The commands are defined according to the following nomenclature:

RULE Mandatory part.

<rule id> Mandatory part to be determined by the user.

[NO] Optional part.

2.1.1 Creating a visible port

The purpose of configuring a visible port is to allow incoming packets from the external domain bound for a specific port (external port) and redirect them to an internal domain IP address on a specific port (internal port).

Commands to configure a visible port:

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

This can also be summarized in a single command:

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

```
NAPT config>VISIBLE-PORT <external port> RULE <rule id> default
```

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

Rule Identifier: Identifier of the rule for which you want to make a specific port visible.

Internal Port: Internal host destination port.

IP Host address: Internal domain host IP address.

Note

If you set value 0 as external port and internal port, the router will redirect incoming traffic (through the connection flavored by NAPT) to the indicated address and by default discard packets. The IP address therefore becomes the destination for all traffic bound for ports unknown to the router.

The default option establishes the default values for a visible port, i.e., internal port 0 to generic internal address 0.0.0.0

Examples:

Redirect external port 80 (HTTP) for the connection flavored by NAPT rule 1 to internal address 192.168.1.5 on port 80: through this configuration, HTTP connections to the router (through the connection flavored by NAPT rule 1 on 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's HTTP server).

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

Redirect external port 8021 belonging to the router connection flavored by NAPT rule 1 to internal address 192.168.1.5 on port 21: through this configuration, the connection to the router (through the connection flavored by NAPT rule 1 on port 8021) will really constitute an FTP connection to the internal server 192.168.1.5.

```
NAPT config>VISIBLE-PORT 8021 RULE 1 IP 192.168.1.5 PORT 21
```

2.1.2 Modifying a visible port

Commands to modify a visible port:

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

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

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

Example:

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

Or like this:

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

2.1.3 Deleting a visible port

Command to delete a visible port:

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

Example:

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

2.1.4 Creating a range of visible ports

You can configure a range of visible ports so you don't have to create an individual input for each. Creating a range of visible ports is very useful when you require a large number of them.

The range of visible ports cannot contain any reserved ports, i.e., the ports related to the NAPT inputs are considered reserved and cannot be made visible. Likewise, if you already have a visible port included in the range, it cannot be created. You can create visible ports that coincide with a router service (FTP, DNS, HTTP, Telnet, etc.).

Command to create a range of visible ports:

```
NAPT config>  <first port> <last port> RULE <rule id> IP <IP host address>
```

First port: First port in the range visible from the external domain to access the service provided by the internal host.

Last port: Last port in the range visible from the external domain.

Rule ID: Identifier of the rule for which you want to make a specific port visible.

IP Host address: Internal domain host IP address.

Note

When configuring a range of visible ports, you cannot associate them independently with internal ports, as is the case with configuring individual ports. Therefore, when configuring a range of visible ports, the associated internal ports will match the external ports.

Example:

Redirects external ports 20, 21 (both FTP) and 23 (Telnet) for the connection flavored by NAPT rule 1 to internal ports 20, 21 and 23 belonging to internal address 192.168.1.5. Through this configuration, the FTP and Telnet connections, executed with the router through the connection, are redirected to an internal server.

```
NAPT config>  20 23 RULE 1 IP 192.168.1.5
```

Redirects the external ports, from 40000 up to 65535 (maximum possible port), for the connection flavored by NAPT rule 2, to internal ports with the same internal address number 192.168.1.5. This is an example of how you can configure a large number of visible ports through a single command.

```
NAPT config>  65535 RULE 2 IP 192.168.1.5
```

2.1.5 Modifying a range of visible ports

You can only modify the internal host IP address in a range of visible ports. This is achieved as follows:

```
NAPT config>  <first port> <last port> RULE <rule id> IP <new IP host address>
```

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

Example:

Modifies the previously created range flavored by NAPT rule 2 and redirects it to 192.168.2.10. (internal address).

```
NAPT config>  65535 RULE 2 IP 192.168.2.10
```

2.1.6 Deleting a range of visible ports

Command to delete a range of visible ports:

```
NAPT config>NO VISIBLE-PORT RANGE <first port> <last port> RULE <rule id>
```

Example:

```
NAPT config>NO VISIBLE-PORT RANGE 20 23 RULE 1
```

2.1.7 Listing the configured visible ports

Command to list the configured visible ports:

```
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

 Rule  Internal Address
 ----  ----------------   --------------
    1   192.168.1.5           20 -    23
    2   192.168.1.5        40000 - 65535

NAPT config>
```

2.1.8 Creating a visible subnet

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

Command used to configure a visible subnet:

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

Visible subnet IP address: IP address of the subnet that will be made visible through the connection flavored by NAPT rule.

Visible subnet mask: Mask of the subnet that will be made visible through the connection flavored by NAPT rule.

Rule Identifier: Identifier for the rule. The configured rules are prelisted.

Default router (optional): When the visible subnet has to be directly connected to an access router through an interface that does not have an address in said subnet, you must configure a visible subnet address in this field (specifically the visible subnet hosts' default gateway) so the access router responds to ARP requests 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 assigned subnet, then this field must be left with the default value (0.0.0.0). This prevents a visible subnet address in the interface from being used so operations execute correctly.

Default establishes the default parameters (only *gateway* in this case, which is 0.0.0.0, i.e., equivalent to *no gateway*).

Example:

Makes the subnet not directly connected to 200.12.100.128/25, visible through the connection flavored by NAPT rule 1: through this configuration, traffic from or to said subnet passing through the router (via the connection flavored by NAPT rule 1) is transparent.

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

Makes the subnet directly connected to 200.12.100.128/25 with default router 200.12.100.129 visible through the connection flavored by NAPT rule 1. Said connection is assigned address 200.12.100.129. This scenario is typical in WAN accesses where the ISP provides a group of public addresses and the WAN interface has an address for said subnet: NAPT must be configured to allow 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 with 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>
```

2.1.9 Modifying a visible subnet

You can only modify the **gateway** parameter for a defined visible subnet. The command 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 a predefined visible subnet.

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

Note

Given that there is only one parameter that can be configured in the visible subnets (GATEWAY), the **default** or **no gateway** commands can be used interchangeably.

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>
```

2.1.10 Deleting a visible subnet

Command to delete a visible subnet:

```
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
```

2.1.11 Listing the configured visible subnets

Command to list the visible subnets:

```
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>
```

2.1.12 Enabling and disabling NAPT

You can globally **enable** or **disable** the NAPT feature 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>
```

2.1.13 Listing the NAPT state

Command to list the state of the NAPT feature:

```
NAPT config>LIST CONFIGURATION
```

Example:

```
NAPT config>LIST CONFIGURATION
 ========================
 =  NAPT CONFIGURATION  =
 ========================
  NAPT Disabled
                  : 32768
  NAPT Entries (number of ports): 1024

NAPT config>
```

2.1.14 Configuring the range of ports to be used

The router offers the possibility of defining the range of ports to be used by NAPT, through two configuration parameters: **first port** and **number of ports** to be used.

Commands to configure the port range:

```
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 in the external domain simultaneously. However, more device resources are used (memory, processing capacity, etc.).

Note

Since the maximum port that can be used is 65535 (OxFFFF), if the configuration of the **First Port** and the **Number of NAPT Ports** exceed the maximum port value, the number of NAPT entries is internally limited to the value between the First Port and 65535.

2.1.15 Listing the configured range of NAPT ports

Command to list the range of NAPT ports:

```
NAPT config>LIST CONFIGURATION
```

Example:

```
NAPT config>LIST CONFIGURATION
 ========================
 =  NAPT CONFIGURATION  =
 ========================
  NAPT Disabled
                  : 60000
  NAPT Entries (number of ports): 1024

NAPT config>
```

2.1.16 EXIT

Run **exit** to exit the NAPT feature configuration.

```
NAPT config>EXIT
```

Example:

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

2.2 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>

LIST ALL
     VISIBLE-PORT
     SUBNET
     CONFIGURATION

NO VISIBLE-PORT RANGE <first port> <last port> RULE <id>
   VISIBLE-PORT RANGE <first port> <last port> RULE <id> IP <IP address>


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

NUMBER-OF-PORTS <value>

FIRST-PORTS <value>
```

Chapter 3 NAPT Feature Monitoring

3.1 NAPT feature monitoring

Access the NAPT feature monitoring menu via the IP monitoring menu through the following commands:

```
*P 3
+PROTOCOL IP
IP+NAT PAT
NAPT+
```

The commands for the NAPT feature 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 various NATP feature monitoring parameters.
EXIT	Exits the NAPT feature monitoring prompt.

3.1.1 ? 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    Deletes NAPT parameters
  list      Displays NAPT monitorization parameters
  exit      Exit to parent menu
NAPT+
```

3.1.2 DELETE

Run **delete** to debug different parameters.

Syntax:

```
NAPT+DELETE ?
  address    Deletes the NAPT entries used by a specified IP address
  entries    Deletes all the used NAPT entries
  idents     Deletes all the used ICMP identifiers
```

3.1.2.1 DELETE ADDRESS

Deletes the NAPT entries used by a specific IP address.

Syntax:

```
NAPT+delete address <IP_address>
```

Example:

```
NAPT+delete address 172.24.0.1
```

3.1.2.2 DELETE ENTRIES

Deletes all used NAPT entries.

Example:

```
NAPT+delete entries
```

3.1.2.3 DELETE IDENTS

Deletes all used ICMP identifiers.

Example:

```
NAPT+delete idents
```

3.1.3 LIST

Run **list** to display the various associated monitoring parameters.

Syntax:

```
NAPT+LIST ?
  address       Displays the NAPT entries used for a specified IP address
  all           Displays all the NAPT monitoring information
  callids       Displays the NAPT inputs associated to PPTP sessions
  entries       Displays all the used NAPT entries
  idents        Displays all the ICMP identifiers translated through NAPT
  statistics    Displays the different NAPT statistics
```

3.1.3.1 LIST ADDRESS

Displays the NAPT entries for a specific IP address.

Syntax:

```
NAPT+list address <IP_ address >
```

Example:

```
NAPT+list address 172.24.77.54
172.24.77.54 NAPT Entries:
 src 172.24.77.54:123 => conn 80.36.189.123:33122, age 25, flags 0x1
 dst 18.145.0.30:123 => ndst 18.145.0.30:123, virt OFF , posid

 src 172.24.77.54:1234 => conn 80.36.189.123:32768, age 30, flags 0x1
 dst 80.26.96.183:1234 => ndst 80.26.96.183:1234, virt OFF , posid

172.24.77.54 uses 2 NAPT entries
NAPT+
```

3.1.3.2 LIST ALL

Displays all NAPT monitoring information.

Example:

```
NAPT+list all

 Internal Src Address     External Src Address   Age  Flags  Delta
 Internal Dst Address     External Dst Address   Virt POSId
 ---------------------    ---------------------  ---- ------ -----
 172.24.77.54   :123   => 200.36.189.123 :33122  16   0x0001 0 0
 18.145.0.30    :123   => 200.145.0.30   :123    OFF

 172.24.77.54   :1234  => 200.36.189.123 :32768  30   0x0001 0 0
 80.26.96.183   :1234  => 200.26.96.183  :1234   OFF
Printing Visible Ports...
 10.0.0.3       :range => 200.36.189.123 :range  0    0x0000 0 0
                [40000,                  [40000,
                 65535]                   65535]
 any            :any   => any            :any    n/a  n/a

 10.0.0.1       :2525  => 200.36.189.123 :25     0    0x0000 0 0
 any            :any   => any            :any    n/a  n/a
```

```
 Internal Ident            External Ident          Age
 ----------------------    ----------------------  ---
 172.24.75.4    [  463] => 200.36.189.123  [    8]    2
 172.24.77.54   [ 2407] => 200.36.189.123  [   10]    2

Memory:
Reserved port-address structures ---- 4096
Used port-address structures -------- 2
Reserved ident-address structures --- 16
Used ident-address structures ------- 2

Port information:
Number of used ports ---------------- 2
Number of free ports ---------------- 4094
Maximum used ports ------------------ 55

Ident information:
Number of used idents --------------- 2
Number of free idents --------------- 14
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 --------- 4306
Received idents out of range -------- 0
Wrong target IP address ------------- 31804

NAPT+
```

3.1.3.3 LIST CALLIDS

Displays NAPT inputs associated with PPTP sessions.

Example:

```
NAPT+list callids

 Local Address & CallID   Visible Address & CallID   Remote Address & CallID
 ----------------------   -------------------------   -----------------------
     192.168.1.5[23674] =>   210.10.43.105[ 1354]  =>    201.32.110.5[31524]

NAPT+
```

3.1.3.4 LIST ENTRIES

Displays all used NAPT entries.

Example:

```
NAPT+list entries

 Internal Src Address     External Src Address   Age  Flags  Delta
 Internal Dst Address     External Dst Address   Virt POSId
 ----------------------   ----------------------  ---- ------ -----
 172.24.77.54   :123   => 80.36.189.123  :33122  26   0x0001 0 0
 18.145.0.30    :123   => 18.145.0.30    :123    OFF

 172.24.77.54   :1234  => 80.36.189.123  :32768  30   0x0001 0 0
 80.26.96.183   :1234  => 80.26.96.183   :1234   OFF

NAPT+
```

3.1.3.5 LIST IDENTS

Displays all ICMP identifiers translated through NAPT.

Example:

```
NAPT+list idents

 Internal Ident            External Ident          Age
 ----------------------    ----------------------  ---
 172.24.75.4    [  463] => 80.36.189.123  [    8]    1
 172.24.77.54   [ 2407] => 80.36.189.123  [   10]    2

NAPT+
```

3.1.3.6 LIST STATISTICS

Displays the different NAPT statistics.

Example:

```
NAPT+list statistics

Memory:
Reserved port-address structures ---- 4096
Used port-address structures -------- 2
Reserved ident-address structures --- 16
Used ident-address structures ------- 2

Port information:
Number of used ports ---------------- 2
Number of free ports ---------------- 4094
Maximum used ports ------------------ 55

Ident information:
Number of used idents --------------- 2
Number of free idents --------------- 14
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 --------- 4338
Received idents out of range -------- 0
Wrong target IP address ------------- 34903

NAPT+
```

The meaning of the statistics is as follows:

Reserved port-address structures	NAPT structures reserved in memory (this must match the number of NAPT entries configured except 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 used.
Number of used idents	Used ICMP identifiers.
Number of free idents	Available ICMP identifiers.
Maximum used idents	Maximum number of ICMP identifiers 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 ports outside the allowed range.
Received idents out of range	Packets destined for ICMP identifiers outside the allowed range.
Wrong target IP address	Packets not addressed to the IP connection addresses.

3.1.4 EXIT

Run **exit** to exit NAPT feature monitoring.

Syntax:

```
NAPT+exit
```

Example:

```
NAPT+exit
IP+
```

Chapter 4 NAPT Feature Events

4.1 Viewing the NAPT feature events

As with other subsystems, you can view any produced events associated with the NAPT feature in real time.

Enable these from the events general configuration menu as follows:

```
*PROCESS 4
User Configuration
Config>EVENT

-- ELS Config --
ELS Config>ENABLE TRACE SUBSYSTEM NAPT ALL
ELS Config>EXIT
Config>SAVE
Save configuration [n]? Y

Saving configuration...OK
Config>
```

These can also be enabled from the monitoring menu. In this case, you do not need to reboot the device to view them. The process is as follows:

```
*PROCESS 3
Console Operator
+EVENT

-- ELS Monitor --
ELS+ENABLE TRACE SUBSYSTEM NAPT ALL
ELS+EXIT
+
```

The list of events available for NATP depends on the software release. Each software release distribution is accompanied by its own set of events.

4.2 Events example

The following is an example of a typical event trace in a series of translations in a router with the NATP feature configured.

```
*PROCESS 2
02/16/05 12:26:05  NAPT.014 In   445
02/16/05 12:26:05  NAPT.028 Drop in pkt (80.36.138.58:1443 -> 80.36.189.123:445)
 no napt dst port
02/16/05 12:26:08  NAPT.014 In   445
02/16/05 12:26:08  NAPT.028 Drop in pkt (80.36.138.58:1443 -> 80.36.189.123:445)
 no napt dst port
02/16/05 12:26:13  NAPT.002 In (80.36.189.123:33595 => 172.24.77.54:1026)
02/16/05 12:26:18  NAPT.028 No NAPT to in pkt (83.34.227.107:500 -> 80.36.189.12
3:500) no napt dst port
02/16/05 12:26:18  NAPT.020 Out pkt (80.36.189.123 -> 83.34.227.107) local orig,
 no NAPT
02/16/05 12:26:18  NAPT.008 No NAPT to IpSec protocols (AH, ESP) packet
02/16/05 12:26:18  NAPT.024 No NAPT to In pkt (172.24.100.131 -> 172.24.0.55) Un
known
02/16/05 12:26:18  NAPT.020 Out pkt (80.36.189.123 -> 83.34.227.107) local orig,
 no NAPT
02/16/05 12:26:18  NAPT.008 No NAPT to IpSec protocols (AH, ESP) packet
02/16/05 12:26:18  NAPT.024 No NAPT to In pkt (172.24.100.131 -> 172.24.0.55) Un
known
02/16/05 12:26:23  NAPT.003 Out (172.24.75.4[463] => 80.36.189.123[8])
02/16/05 12:26:23  NAPT.004 In (80.36.189.123[8] => 172.24.75.4[463])
02/16/05 12:26:31  NAPT.014 In   137
02/16/05 12:26:31  NAPT.028 Drop in pkt (80.116.236.171:1030 -> 80.36.189.123:13
```

```
7) no napt dst port
02/16/05 12:26:43  NAPT.002 In (80.36.189.123:33595 => 172.24.77.54:1026)
02/16/05 12:26:49  NAPT.014 In
02/16/05 12:26:49  NAPT.028 Drop in pkt (161.53.97.5:58893 -> 80.36.189.123:1258
8) no napt dst port
*
```

Chapter 5 Example of NAPT Feature Configuration

5.1 Description of the configuration example

Supposing you wish to configure a private domain so a router interconnects a central office with three branches and provides access to the public and private domains with two connections making use of the NAPT feature through a Point to Multipoint link. The characteristics of the different connections are described below.

The router providing communications between the public and private domains is located in the central office. Two NAPT connections are established with different characteristics. The public domain access address is IP 200.12.100.129. The mask 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 the device is capable of distinguishing what circuit is going to communicate with the rest of the network. Furthermore, they must belong to the same subnet. These addresses are 200.12.100.27 and 200.12.100.18.

5.1.1 Configuring the offices

5.1.1.1 Central office configuration

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

Said office is connected to the other 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) belonging to subnets 192.168.28.0, 192.168.29.0, and 192.168.30.0

5.1.1.2 Configuration of the NAPT links

To show the NAPT possibilities, the links interconnecting the private domain central office with the public domain are configured in a different way.

Thus, for connections through link (200.12.100.129, 200.12.100.27), you need to make an FTP server installed on host 192.168.27.224 accessible from port 6421 and the Telnet server on host 192.168.27.111 through port 6423. A Telnet server in Office 2 with IP address 192.168.29.121 also needs to be visible through port 5423. 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 inbound traffic through this link.

For connections through link (200.12.100.129, 200.12.100.18), public addresses that are in the private domain need to be accessible 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:

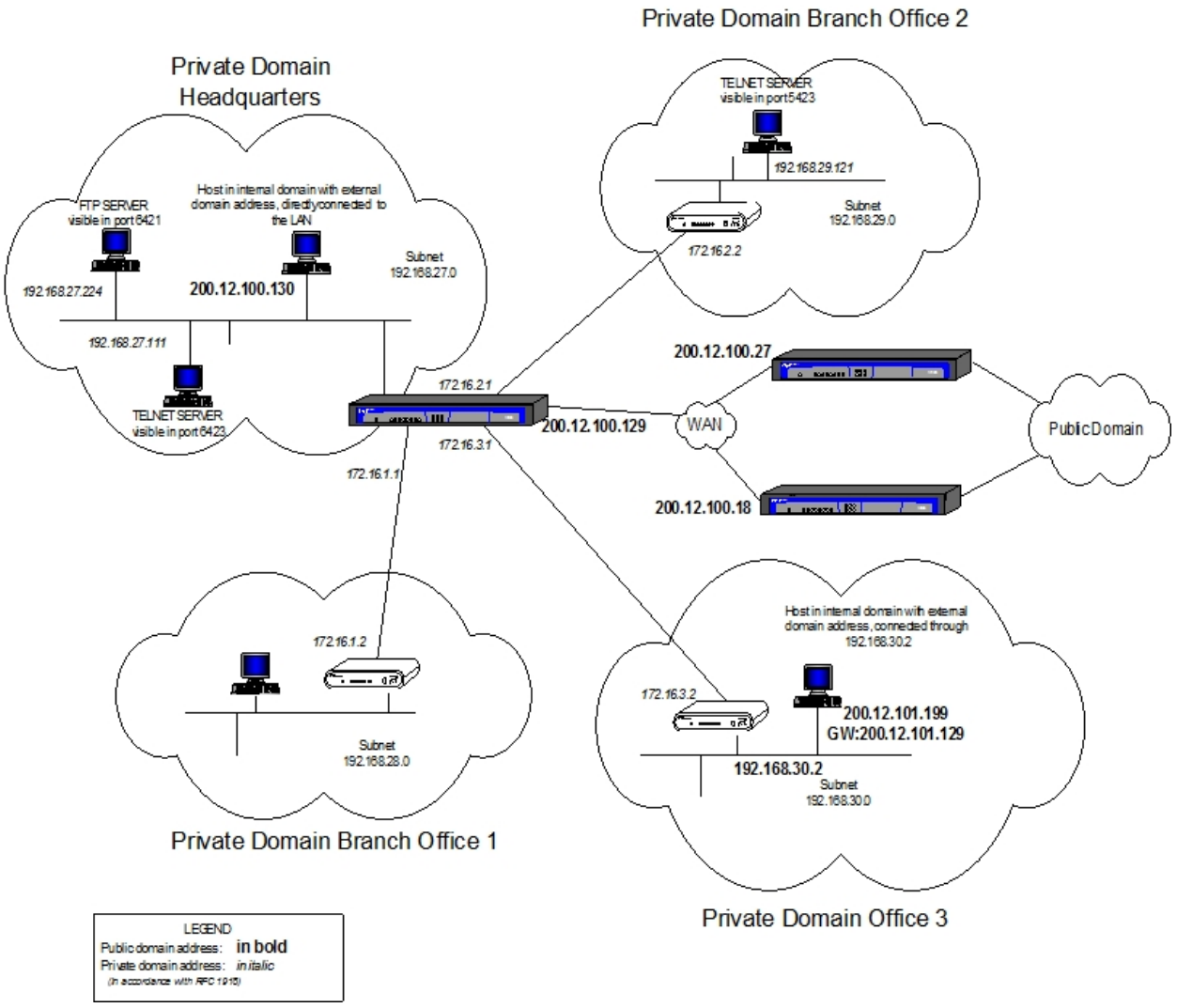

Fig. 2: **Configuration of the NAPT links**

The steps given below are to configure the NAPT feature in the access router so the previously described environment is operative.

5.1.2 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 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 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

To configure a NAPT rule, first enter the local and the remote IP. Once these addresses are configured, the options to configure NAPT parameters appear. For further information on this, please see the associated manual bintec Dm702-I TCP-IP.

Note

The first defined rule makes the access router act as a firewall, blocking access to its standard ports.

5.1.3 Configuration of link (200.12.100.129, 200.12.100.27)

To meet the requirements for link (200.12.100.129, 200.12.100.27), configure three visible ports to give access to both the Telnet ports 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 are 6423, 5423 and 6421 respectively.

When configuring the ports and visible subnets, enter 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 captured by the router due to services running on them, you need to do port mapping as shown in the example for the FTP and Telnet ports.

5.1.3.1 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. To configure the visible ports as the environment specifies, enter:

```
IP config>NAT PAT

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

5.1.3.2 Configuring the visible subnet

You do not need to enter 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 Office 3 router.

5.1.4 Configuration of link (200.12.100.129, 200.12.100.18)

To comply with the needs defined by the environment for this link, carry out the following.

5.1.4.1 Configuring the visible subnet

The rule identifier defining this link (200.12.100.129, 200.12.100.18) is 2. To configure the visible subnets, configure the gateway in the visible subnet (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 2 GATEWAY 200.12.100.129
NAPT config>
```

In the access router IP configuration menu, carry out the following:

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