Teldat Router

NAT Feature

Doc. *DM520-I* Rev. *8.40*
October, 2000

INDEX

Chapter 1
Introduction

1. Introduction to NAT

Two of the key problems facing the Internet are depletion of IP address space and scaling in routing. Network Address Translation (NAT) is a feature that allows an organization's IP network to appear form the outside to use different IP address space than what it is actually using. Thus, NAT allows an organization with non-globally routable addresses to connect to the Internet by translating those addresses into globally routable address space. NAT also allows a more graceful renumbering strategy for organizations that are changing service providers or voluntarily renumbering into CIDR blocks. NAT is also described in RFC 1631.

NAT has several applications. Use it for the following purposes:

- If you want to connect to the Internet, but not all your hosts have globally unique IP addresses (allowed). NAT is configured on the router at the border of a stub domain (local network) and a public domain such as the Internet (outside network). The NAT translates the inside local addresses to globally unique IP addresses before sending packets to the outside network.
- If an organization requires IP connectivity between remote offices. The remote offices have inside IP networks which do not comply with the addressing plan as the routing tables through which connectivity is carried out between them are large or unmanageable. In this case it is sufficient to configure NAT in the border router of each office thus carrying out the translation between office inside networks and global networks as these now comply with the addressing plan.
- You must change your inside addresses. Instead of changing them, which can be a considerable amount of work, you can translate them by using NAT.

A significant advantage of NAT is that it can be configured without requiring changes to hosts or routers other than those few routers on which NAT will be configured. The disadvantages of NAT appears when large numbers of hosts require NAT simultaneously or when the network applications exchange source or destination IP address references. These applications do not work if the information is sent through a NAT router in transparent mode. In these cases the only solution is that the NAT router analyses the data packet of the application, ascertain and change the references to local IP addresses.

A router configured with NAT will have at least one local interface (an interface in contact with the local network) and one global (an interface in contact with the global network). In atypical environment, NAT is configured at the exit router between a stub domain and backbone. When a packet is leaving the domain, NAT translates the locally significant source address into a globally unique address. When the packet is entering the domain, NAT translates the globally unique address into a local address.

A router configured with NAT must not advertise the local networks to the outside. However, global routing can be advertised through the local interfaces.

As previously mentioned, the term 'local' refers to those networks that are owned by an organization and that must be translated. Inside the domain, hosts will have address in the one address space, while on the outside, they will appear to have addresses in another address space. The first address space is referred to as the "local" address space while the second is referred to as the "global" address space.

2. Types of NAT

Address translation can be:

- Static NAT: where the mapping of local and global addresses is unanimous.
- Dynamic NAT: establishes a mapping of local addresses in a pool of global addresses. This means that the mapping between global addresses and local addresses is not unanimous and depends of the execution conditions.
- NAPT (Address Port Translation): establishes a mapping between local addresses and a unique global address. In this case a translation of the transport protocols ports (UDP, TCP) is carried out.

In the following sections m and n mean:

m: number of local IP addresses.

n: number of global IP addresses.

2.1. Static NAT

m : n-Translation, m, n ≥ 1 and m = n (m, n ∈ N)

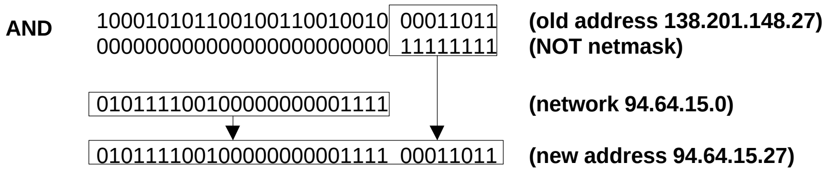
With static NAT we can translate between local networks and global networks of the same size (contain the same number of IP addresses). A special case is when both networks contain just one IP address, i.e. the netmask is 255.255.255.255). The NAT process can be described with the following translation:

global-address = global-network OR (local-address AND (NOT netmask))

local-address = local-network OR (global-address AND (NOT netmask))

Example:

- NAT rule: translate all the local network addresses 138.201.148.0 in the global network 94.64.15.0, netmask is 255.255.255.0 for both.



```
AND   100010101100100110010010  00011011   (old address 138.201.148.27)
      000000000000000000000000  11111111   (NOT netmask)

      010111100100000000001111             (network 94.64.15.0)

      010111100100000000001111  00011011   (new address 94.64.15.27)
```

2.2. Dynamic NAT

m: n-Translation, m ≥ 1 and m ≥ n (m, n ∈ N)

This type of NAT is necessary when the number of global addresses to translate does not equal the number of local ones, or they are equal but for some reason it is not desirable to have a static mapping. The number of hosts communicating is generally limited by the number of global addresses available. When all the global addresses are being used then subsequent connections must be rejected returning a "host unreachable". Dynamic NAT is more complex than static NAT, since you must keep track of the communicating hosts and their current mapping with global addresses.

Example:

- NAT rule: dynamically translates all the local network addresses 138.201.0.0 mask 255.255.0.0 into global network addresses 278.201.112.0 with mask 255.255.255.0.
- Each new connection from the local network towards the outside obtains a global address from the pool of global address available.
- if the local address already has a global address it uses this mapping.

2.3. NAPT (Masquerading)

m: n-Translation, $m \geq 1$ and $n = 1$ ($m, n \in N$)

This is a very special case of dynamic NAT and currently is the type of NAT most used. Here there exist many local addresses which are translated into the same global address. In contrast to the previous NAT more than 'x' connections are permitted. Now an arbitrary number of connections are multiplexed using port information (TCP, UDP). The number of simultaneous connections is limited only by the number of NAT ports available.

The main problem with this type of NAT is that many services only accept connections coming from privileged ports in order to ensure that it does not come from an ordinary user. To support NAT, you need to maintain handlers for each TCP, UDP connection.

Another limitation is that incoming connections are not permitted.

Example:

- NAT rule: masquerade the global network addresses 138.201.0.0 after the router's outside global interface address.
- For each outgoing packet the source address is replaced by the NAT router's outside interface address and the source port is exchanged for an unused NAT port.
- If the destination of the incoming packets is the NAT router's outside interface address and the destination port corresponds to an already assigned NAT port, the address and port is exchanged for the corresponding local address and local port.

3. Problems common to all NAT techniques

All connections through a router are identified by a five-tuple: protocol, source address and port, destination address and port. If the router has NAT enabled, three five-tuples appear representing the same connection, one for each section:

- The first or local section: from the source to the NAT router.
- The second or global section: from the NAT router to the destination.
- Third or inside section: the inside NAT router interface or local to the outside interface or global.

Only the NAT router has the information on what is going on in each section, but this also means that the NAT router has to store a lot of information on the established connection, something which routers without NAT do not have to do.

This is something that they have in common with firewalls: because both types of devices not only relay packets but also analyze and control the type of information which is exchanged between them and maintain the state information on each connection: a significant overhead in time compared to a router without NAT.

If NAT is being used, all packets must go through the NAT router i.e. there must not be any alternative routes a packet could take, circumventing the address translation.

3.1. State Information

Except for static NAT, the NAT router needs to store dynamic information on the current mapping between the local and global addresses. In addition this type of state information must have a timeout limit so that if a specific device stops transmitting information it can be cleared from the list.

3.2. Fragmentation

In NAT strategies where not only the addresses are translated but also the ports, another problem appears in the fragmentation. When a packet is fragmented the NAT router can only used the port information from the first fragment as the rest of the fragments have a port 0xFFFF. This is why you must keep state information about fragments.

3.3. Behavior depending on protocol

a) FTP

The FTP commands **PORT** and **PASV** contain IP address and port information. For FTP to work correctly you need to translate these addresses and ports. This gets complicated when this type of information travels in ASCII format as when you change the packet, the length can vary. Due to this you need to adjust the sequence number of the packet's TCP header and the subsequent packets from the same connection. Accordingly you need to store more information on hops (deltas) of the sequence numbers for FTP connections.

All protocols which exchange local addresses or ports in their control packets have the same problem as the FTP and do not work through NAT routers transparently thus making it necessary to store state information for each connection.

b) *ICMP*

Some ICMP messages, depending on the type of message, include a part of original IP packet that caused this message to be generated, including the IP header. If the packet has been translated, the header will contain information on the translated address and not on the real address. Depending on where and how this information is used, this can present a problem and in some cases it is necessary to translate it.

c) *DNS*

Obviously this service presents problems if the nameservice for the local network devices is provided in the global network. One solution would be to have two DNSs, one for inside address resolution and the other for outside addresses.

d) *BOOTP*

This should be no problem as in the majority of cases it is very unlikely that this protocol has to cross the NAT router.

e) *Dynamic Routing Protocols (RIP, EGP, ...)*

A NAT configured router should not announce the local networks through the global interfaces. However the global routes can be announced through the local interfaces. Depending on the type of routing protocol this should be fairly easy to implement. Static routing is recommended.

4. Implementation

There already exists NAPT implementation (or extended NAT) which can only be used for PPP interfaces. Additionally static NAT has been implemented for any interface.

Implemented static NAT permits the following applications:

- All those applications which do not have a local address specified in their data.
- FTP protocol: The data for this protocol has been analyzed in order to detect and change the local addresses specified in the control commands such as PORT and PASV. For this, the state information has been stored and can be viewed at any time through the connection monitoring commands.
- ICMP Protocol: analyzes the data of the types of messages where a part of the IP packet is located provoking these messages and where NAT has been carried out on this data.
- IP Fragmentation: where there is no change of port, there are no problems in IP fragments.
- RIP Dynamic routing protocol: a modification has been carried out on this protocol so that local addresses cannot be sent through global interfaces.

Chapter 2
Configuration

1. NAT Configuration

The steps required in order to configure the NAT facility are described in this chapter. Once the required options have been configured you must save the configuration and restart the router so these take effect. The following sections describe the configuration procedure in more detail.

- Access the NAT configuration environment.
- Activate or deactivate NAT.
- NAT rules configuration.
- Exit the NAT configuration procedure.
- Restart the router so the new configuration can take effect.

Accessing the NAT Configuration environment

In order to access the NAT configuration environment, you need to previously access the IP:

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

Here, you need to enter the following command:

```
IP config> NAT
NAT configuration
NAT config>
```

Activate or deactivate NAT

The NAT facility can be enabled or disabled. To activate or deactivate this you must enter the following commands:

```
NAT config> SET ENABLED
```

or

```
NAT config> SET DISABLED
```

Configure NAT rules

The NAT facility is based on an ordered global list of rules. If the NAT facility is enabled, each source, translated or received IP packet is inspected for the list of rules.

Each rule is made up of the following camps:

1.1. Position or identifier

Each rule possesses a unique identifier which specifies its position in the list (minor identifier → first rule in the list). The identifiers should be natural consecutive numbers (excluding zero). When adding a new rule you need to specify where you want to insert it. By default it will appear at the end of the list.

1.2. Local Interface

This is the inside NAT router interface or the interface it is in contact with or through which it reaches the local domain. You must enter an associated local interface for each rule. The way to specify the interface can be:

- A physical interface: for this you need to specify the physical interface number by using the same notation as when specifying the unnumbered addresses: (For example ETH/0 → 0.0.0.0).
- A logical IP interface: for this you need to specify the logical IP interface by entering the IP address (numbered) of the NAT router interface. (For example ETH/0 with two addresses configured to specify which logical interface you need to give the required numbered IP address).

1.3. Global Interface

This is the outside NAT router interface or the interface it is in contact with or through which it reaches the global domain. The means of specifying of interface can be:

- A physical interface: for this you need to specify the physical interface number by using the same notation as when specifying the unnumbered addresses: (For example ETH/0 → 0.0.0.0).
- A logical IP interface: for this you need to specify the logical IP interface by entering the IP address (numbered) of the NAT router interface. (For example ETH/0 with two addresses configured to specify which logical interface you need to give the required numbered IP address).

1.4. Local Network

This is specified by giving the address and mask for this. It is the set of local addresses over which you want the rule to act.

1.5. Global Network

This is specified by giving the address and mask for this. It is the set of global addresses over which you want the rule to act.

1.6. Type of translation

There are two types of translation and the meaning of them is as follows:

- Inside Source:

All packets which pass from the local domain to the global (provided that all the requisites for the rule have been complied with) the local source address is changed for the corresponding global address. And all the packets which pass from the global domain to the local (provided that all the requisites for the rule have been complied with), the global destination address is changed for the corresponding local address.

- Inside destination:

All packets which pass from the local domain to the global (provided that all the requisites for the rule have been complied with), the local destination address is changed for the corresponding global address. And all the packets which pass from the global domain to the local (provided that all the requisites for the rule have been complied with), the global source address is changed for the corresponding local address.

1.7. Translating direction

There are 5 translation directions which mean the following:

- Local to Global:

If the packet enters through the local interface and exits through the global interface and its address (source or destination) belongs to the local network, its address (source or destination) is changed for the corresponding global address.

- Global to Local:

If the packet enters through the global interface and its address (source or destination) belongs to the global network, then its global address is changed (source or destination) for the corresponding local address.

- Local to Global , Global to Local: the above two.
- Skip Local.

If the packet enters through the local interface and exits through the global interface and its address (source or destination) belongs to the local network, no change is carried out.

- Skip Global.

If the packet enters through the global interface and its address (source or destination) belongs to the global network, then no change is carried out.

NOTE: (source or destination) depends on the type of translation.

2. NAT Configuration Commands

This section summarizes and explains all the NAT facility configuration commands of the router. These commands permit you to configure the behavior of the NAT facility router and in this way permits you to enter the required operation specifications.

Enter the NAT configuration commands when you see the NAT config> prompt. In order to access this prompt you must enter the following:

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

Command	**Function**
?(HELP)	List of commands or options.
ADD	Adds information to the NAT configuration.
DELETE	Deletes the NAT configuration entered through the ADD command.
LIST	Lists the NAT elements configuration.
SET	Establishes the NAT facility configuration modes.
EXIT	Exits the NAT configuration.

The letters written in **bold** are the minimum number of characters you must enter to make the command effective.

2.1. ? (HELP)

Use the **?** (HELP) command in order to list the valid commands at the level where the router is programmed. You can also use this command after a specific command in order to list the available options.

Syntax:

```
NAT config> ?
```

Example:

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

2.2. ADD

Use the **ADD** command to add more NAT configurations to the current NAT configuration. This command permits you to add NAT rules.

Syntax:

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

a) ADD RULE

Adds a new entry in the list of NAT rules. This command places the entry at the end of the list by default if you do not specify a particular position. Each entry contains: Position or identifier, local Interface, global Interface, local Network, global Network, translation direction.

There are two types of translation: inside Source, inside Destination.

There are 5 translation directions: Local to Global, Global to Local, the two previous ones, skip local, skip global.

Syntax:

```
NAT config> ADD RULE <translating_type, translating_direction, local_interface,
global_interface, local-ip-addr, local_ip_mask, global_ip_addr, global_ip_mask,
position>
```

Example:

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

2.3. DELETE

Use this command to delete a NAT configuration parameter which was previously added through the **ADD** command. Generally you must specify which element you wish to delete in accordance with the **ADD** command.

Syntax:

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

a) DELETE RULE

Deletes one of the registers from the NAT rules list.

Syntax:

```
NAT config> DELETE RULE <position>
```

Example:

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

2.4. LIST

Use the **LIST** command in order to view the various NAT configuration parameters depending on the option chosen.

Syntax:

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

a) LIST ALL

Displays all the NAT configuration.

Syntax:

```
NAT config> LIST ALL
```

Example:

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

b) LIST RULES

Displays the list of configured NAT rules.

Each rule has a register number associated. This number is the rule's order or position number within the list.

The type and translation direction is specified in the following way:

- <-S-> Type: Inside source. Direction: Local to Global and Global to Local.
- <-D-> Type: Inside destination. Direction: Local to Global and Global to Local.
- >-S-> Type: Inside source. Direction: Local to Global.
- >-D-> Type: Inside destination. Direction: Local a Global.
- <-S-< Type: Inside source. Direction :Global to Local.
- <-D-< Type: Inside destination. Direction: Global to Local.
- >-S-! Type: Inside source. Direction: Skip Local.
- >-D-! Type: Inside destination. Direction: Skip Local.
- !-S-< Type: Inside source. Direction: Skip Global.
- !-D-< Type: Inside destination. Direction: Skip Global.

Syntax:

```
NAT config> LIST RULES
```

Example:

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

c) LIST STATE

This shows you if the NAT facility is active or not.

Syntax:

```
NAT config> LIST STATE
```

Example:

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

2.5. SET

Permits you to activate or deactivate the NAT facility.

Syntax:

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

a) SET DISABLED

Permits you to deactivate the NAT facility.

Example:

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

b) SET ENABLED

Permits you to activate the NAT facility.

Example:

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

2.6. EXIT

Use the **EXIT** command to return to the previous prompt level.

Syntax:

```
NAT config> EXIT
```

Example:

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

Chapter 3
Monitoring

1. NAT Monitoring

This section summarizes and explains all the NAT facility monitoring commands of the router. These commands permit you to configure the behavior of the NAT facility router and in this way permits you to enter the required operation specifications.

Enter the NAT monitoring commands when you see the NAT monit> prompt. In order to access this prompt you must enter the following:

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

Command	Function
?(HELP)	Lists the commands or options.
LIST	Lists the NAT parameters.
EXIT	Exit the NAT monitoring.

The letters written in **bold** are the minimum number of characters you must enter to make the command effective.

1.1. ? (HELP)

Use the **?** (HELP) command in order to list the valid commands at the level where the router is programmed. You can also use this command after a specific command in order to list the available options.

Syntax:

```
NAT monit> ?
```

Example:

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

1.2. LIST

Use this command to view the various NAT facility monitoring parameters.

Syntax:

```
NAT monit> LIST ?
CONNECTIONS
```

a) LIST CONNECTIONS

Displays the list of non transparent connections to the NAT. In cases of static NAT, only the FTP control connections which have clients in the local domain and the server in the global domain pertain to this category and that also have transmitted PORT commands where the packet length has changed.

The connection list fields represent the following:

- Type: the type of non transparent connection which is passing through the NAT router, in cases of static NAT these are FTP control non transparent connections only.
- Addr:Port Source and Addr:Port Destination represents the connection’s source address, source port, destination address and destination port. All in global format (as can been seen in the global domain).
- Age: timeout value between entering and before being deleted.
- Active: indicates if the connection is active or not (if the NAT router has detected whether the connection is active or not).

Syntax:

```
NAT monit> LIST CONNECTIONS
```

Example:

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

1.3. EXIT

Use the **EXIT** command to return to previous prompt level.

Syntax:

```
NAT monit> EXIT
```

Example:

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

Chapter 4
Examples

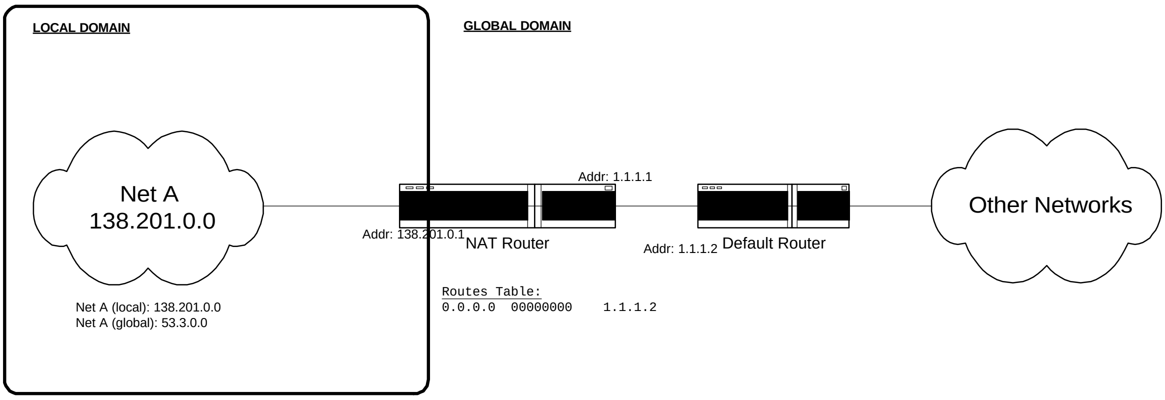
1. Static NAT

Over the previous chapters the static NAT application fields have been marked, now you will find a series of examples in order to learn how to use the current implementation.

1.1. Changing the source addresses of a whole network

This is a classic case of static NAT. In this example you have a large organization using a class A IP network (53.0.0.0). It happens that a small department within the organization for various reasons needs an IP address and believing that they would never have to connect to the rest of the company arbitrarily choose a net (138.201.0.0). The years pass and the moment arrives when they need total connectivity due to the development of new communication technologies. The first solution to appear is to change the local domain addresses for addresses belonging to the network assigned by the organization, but they immediately realize that this is impossible. This is because the department has a great many clients that have contracted continuous connectivity (24 hours per day and 7 days a week) with the local domain's addresses and they cannot of course accept any solution which would mean failure to comply with that contract.

The solution for the organization's department is to configure static NAT in the router carrying out the connection between the department and the rest of the corporate Intranet. Below you can see how to configure the NAT router:



- Monitoring the addresses:

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

- Monitoring the routes:

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

- Configure the NAT rule:

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

- Enable NAT:

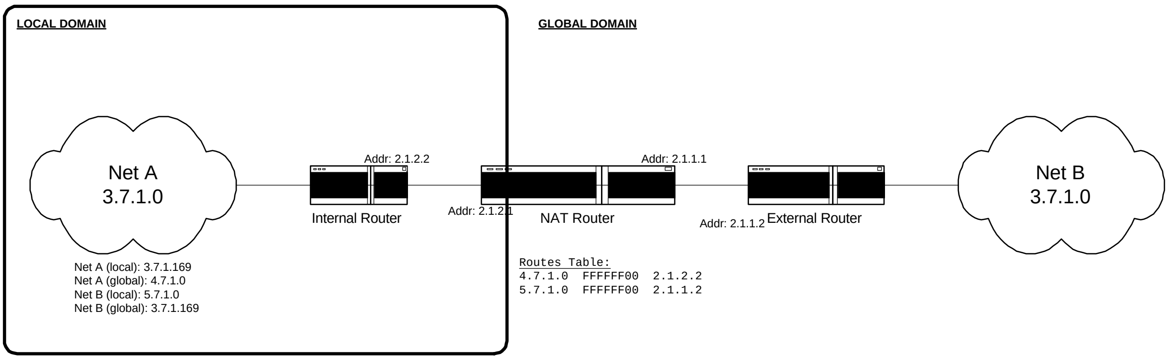
```
NAT config> SET ENABLED
```

- List the NAT configuration:

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

1.2. Connecting two networks using the same address space

The case where a private network which needs to connect to another public network, has IP addresses which officially belong to the public network is called overlapping. You can use NAT to connect these networks. You need that the local domain is seen as possessing another address(NAT type: change inside destination) as the public network (outside) already possesses a global address. At the same time that in the global domain the private network (inside) is seen with global addresses (NAT type: change inside source). With two bi-directional rules the problem can be solved.



- Monitoring the addresses:

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

- Monitoring the routes:

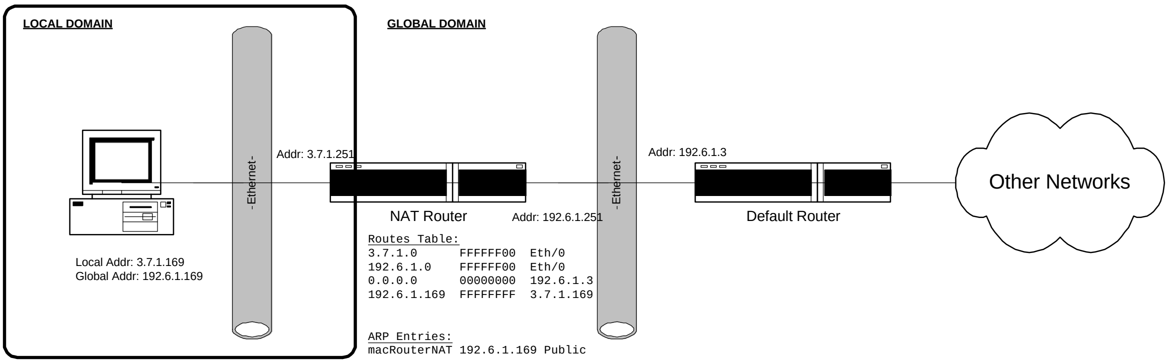
```
IP> DUMP
Type     Dest net       Mask      Cost  Age  Next hop (s)
------   --------       --------  ----  ---  ------------
Dir(1)   2.1.1.0        FFFFFF00  1     0    Eth/0
Dir(1)   2.1.2.0        FFFFFF00  1     0    Eth/0
Stat(1)  4.7.1.0        FFFFFF00  1     0    2.1.2.2
Stat(1)  5.7.1.0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

- List the NAT configuration:

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

1.3. Address overlapping (autoaliasing)

This case is know as “autoaliasing”. Many clients want to configure NAT in such as way that they can translate their local addresses to unused subnet global addresses directly connected to the NAT router. This means that the router must respond to ARP petitions for these global addresses so all packets are sent to one of these global addresses and are accepted and translated by the NAT router. In order for this to happen you need to configure permanent and public ARP entries in the router. The creation of these ARP entries is not automatic and must be carried out as one more step in the configuration procedure by the NAT router administrator. Below you can see a simple example of this.



```
Routes Table:
3.7.1.0      FFFFFF00  Eth/0
192.6.1.0    FFFFFF00  Eth/0
0.0.0.0      00000000  192.6.1.3
192.6.1.169  FFFFFFFF  3.7.1.169


ARP Entries:
macRouterNAT 192.6.1.169 Public
```

- Monitoring the addresses:

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

- Monitoring the routes:

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

- List ARP configuration:

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

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

- List NAT configuration:

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