NAT Feature

bintec Dm720-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

Chapter 1 Introduction

1.1 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 from the outside to use different IP address space. Thus, NAT allows an organization, which uses private addresses (local addresses) and therefore not accessible through the Internet routing tables, to connect to the Internet by translating those addresses into globally routable address spaces (public addresses) that are accessible from Internet. NAT also allows organizations to launch readdressing strategies where the changes in the local IP networks are minimum. NAT is described in RFC 1631.

NAT has several applications. Some possible scenarios are as follows:

- 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 (for connectivity) are large or unmanageable. In this case, NAT can be configured 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 involve a considerable amount of work, you can translate them by using NAT.

A major advantage of NAT is that changing the addresses of multiple local devices only requires making configuration changes in the NAT routers. The disadvantages of NAT appear 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. The only solution in these cases is for the NAT router to analyze the data packets of the application, and ascertain and modify 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 a typical 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 routes 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 local domain, hosts will have addresses in 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.

1.2 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 on 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 protocol 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.

1.2.1 Static NAT

m : n-Translation, m, n ⊠1 and m = n (m, n Î N)

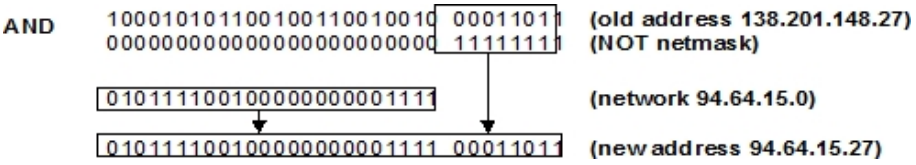
With static NAT, translation is performed between local and global networks of the same size (containing the same number of IP addresses). A special case is when both networks contain just one IP address, i.e., the netmask is 255.255.255.255). The NAT process can be described with the following transformation:

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.



This manual focuses on the configuration of static NAT. There are other manuals which describe and explain the rest of the NAT variations.

1.2.2 Dynamic NAT

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

This type of NAT is necessary when there are fewer global addresses available than local ones, or when there is the same number but for some reason static mapping is not desirable. The number of hosts simultaneously communicating with the outside network is generally limited by the number of global addresses available. If all the global addresses are being used, subsequent connections must be rejected by returning a “host unreachable” message.

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 available global addresses.
- If the local address already has a global address, the same mapping is reused.

1.2.3 NAPT/PAT (Masquerading)

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

This is a very special case of dynamic NAT and is the most common NAT system in use today. Here, multiple local addresses are translated into the same global address. Unlike the previous type of NAT, this one can have more than ‘n’ connections. Now an arbitrary number of connections are multiplexed using port information (TCP, UDP). The number of simultaneous connections is only limited by the number of NAT ports available.

The main problem with this type of NAT is that many services only accept connections from privileged ports to ensure they do not come from normal users. To support NAT, you need to maintain handlers for each TCP, UDP connection.

Another limitation is that incoming connections are not allowed (default).

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.

1.3 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.

The NAT router is the only device that has information on what is going on in each section, but this also means that it has to store a lot of information about each established connection, something which normal routers (without NAT) do not have to do.

This is something NAT routers have in common with firewalls: both types of devices not only relay packets, they also analyze and control the type of information that passes through them and maintain stateful information about each connection – which amounts to a significant overhead compared to a router without NAT.

If NAT is enabled, all packets traveling from the local domain to the global domain must go through the NAT router/routers.

1.3.1 Stateful information

Except for static NAT, NAT routers must keep dynamic information about the current mappings between local and global addresses. In addition, this type of stateful information must have a timeout limit so that if a specific device stops transmitting information, it can be cleared from the list.

1.3.2 Fragmentation

In NAT systems where not only the addresses are translated but also the ports, another problem appears in fragmentation. When a packet is fragmented, the NAT router can only use the port information from the first fragment (as the rest of the fragments have port 0xFFFF). Therefore, in this type of NAT, the NAT device needs to keep stateful information about fragments.

1.3.3 Behavior depending on protocol

1.3.3.1 “Poisonous” applications

The so-called “Poisonous” applications are those applications which include IP addressing information and/or TCP/UDP ports outside the corresponding header fields. Each application of this type requires specific treatment. Examples of these applications are FTP, ICMP, etc.

1.3.3.2 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. Static routing is recommended.

Chapter 2 Configuration

2.1 NAT Configuration

This chapter describes the steps required to configure the NAT feature. Once the required options have been configured, save the configuration and restart the router so the new configuration takes 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.
- If the new configuration is entered at the P4 process, save the configuration and restart the router to activate it.

Accessing the NAT Configuration environment

To access the NAT configuration environment, you need to preaccess the IP:

```
*config
Config>protocol IP
-- Internet protocol user configuration --
IP config>
```

Here, enter the following command:

```
IP config>nat static
-- Static NAT configuration --
SNAT config>
```

Activate or deactivate NAT

The NAT feature can be enabled or disabled. To activate or deactivate this, enter the following commands:

```
SNAT config>enable
```

```
SNAT config>disable
```

or

```
SNAT config>no enable
```

Configure NAT rules

The NAT feature is based on a global ordered list of rules. If the NAT feature is enabled, every originated, transferred or received IP packet is inspected for the list of rules.

Each rule is made up of the following fields:

2.1.1 Position or identifier

Each rule has a unique identifier that specifies its position in the list: the rules are analyzed in order according to their identifier. The identifiers should be natural consecutive numbers (excluding zero). When adding a new rule, you must specify where you want to insert it.

2.1.2 Local Interface

This is the interface that is in contact with the local network (local domain) or through which it is reached. Enter an associated local interface for each rule. 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: ethernet0/0 # 0.0.0.0)
    - Specify the interface identifier, for example: ethernet0/0, serial0/0, ...

- A logical IP interface: specify the logical IP interface by entering the IP address (numbered) for the NAT router interface. (For example: ethernet0/0 with two addresses configured to specify which logical interface you need to give the required numbered IP address.)
- If this is not specified (**unspecified** option), the local interface is not taken into consideration when deciding whether to apply the rule.

2.1.3 Global interface

This is the interface in contact with the global network (global domain) or through which it is reached. Enter an associated gobal interface for each rule.The global interface is specified in the same way as a local interface, except it cannot be left unspecified.

2.1.4 Local network

This is specified by giving its address and mask. It is the set of local addresses on which you want the rule to act. You can also configure the network connected to a device interface as the local network, giving the identifier for said interface. Given that static NAT carries out a one-to-one association between the local domain addresses and the global domain addresses, the mask for both networks must be the same (the router ensures both masks are the same).

Note

When you specify the local interface in the NAT rule, you must add a static IP route with a global network destination where the next hop is the local interface. This static route is not used in the routing process, but is used as a help route queried by NAT before executing global translation to identify the local interface (and consequently select the appropriate rule).

When the local interface isn't specified (**unspecified**) the help route isn't required.

2.1.5 Global network

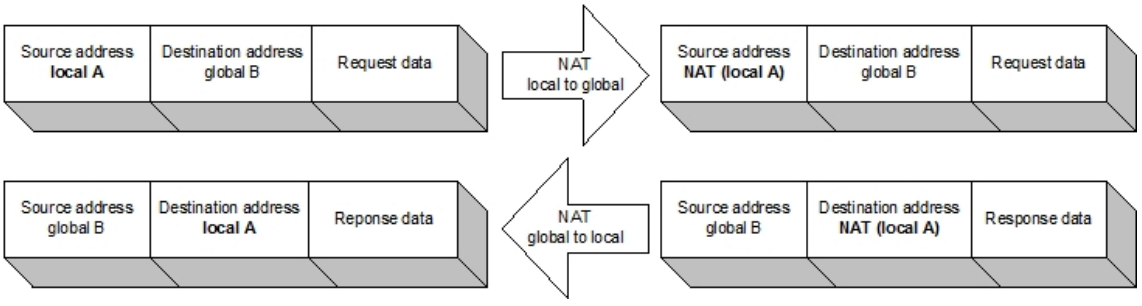
This is specified by giving its address and mask. You can also configure the network connected to a device interface as the local network, giving the identifier for said interface. It is the set of global addresses on which you want the rule to act.

2.1.6 Type of translation

There are two types of translation:

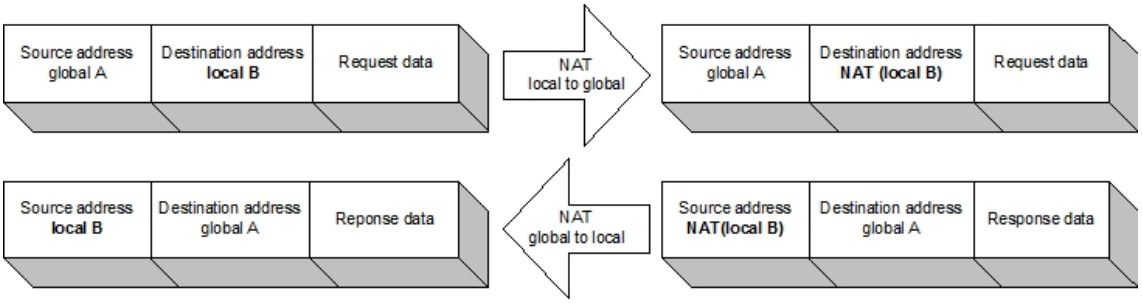
- Inside Source:

Any packet that goes from the local domain to the global one (provided that it meets the other requirements of the rule) will have the local source address changed to the corresponding global address. And every packet that passes from the global domain to the local one (as long as it meets the other requirements of the rule) will have the global destination address changed to the corresponding local address.



- Inside destination:

Any packet that passes from the local domain to the global one (provided that it meets the other requirements of the rule), will have the local destination address changed to the corresponding global one. And every packet that passes from the global domain to the local one (as long as it meets the other requirements of the rule) will have the global source address changed to the corresponding local address.



2.1.7 Translating direction

There are five translation directions:

- 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 to 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) to the corresponding local address.

- Local to Global and Global to Local: the above two simultaneously.
- 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. This type of rule is used to define exceptions and is avoided when other more generic rules are applied.

- 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. This type of rule is used to define exceptions and is avoided when other more generic rules are applied.

Note

(source or destination) determines the type of translation.

Note

In the input transformation (global # local), NAT inverts the IP header: the source address and source port become the destination address and destination port and vice versa. Consequently, if an access list controlling the traffic (when NAT is applied) is indicated, pay special attention when configuring the access list, as the header inverts prior to executing the consultation. For further information, please see the sub section on “Configuring access lists” in the section on “Configuring a NAT rule.”

2.2 NAT configuration commands

This section summarizes and explains all of the router's NAT feature configuration commands. These commands allow you to configure the behavior of the NAT feature on the router and thus reach the desired operating specifications.

To access the prompt, enter the following:

```
*config
Config>protocol IP
-- Internet protocol user configuration --
IP config>nat static
-- Static NAT configuration --
SNAT config>
```

We will now describe how to configure the various possibilities offered by NAT.

The commands are defined according to the following nomenclature:

RULE	Mandatory part
<rule id>	Mandatory part to be determined by the user.
<SOURCE | DESTINATION>	Mandatory part with various options.

2.2.1 Configuring a NAT rule

As previously indicated, the configuration of a NAT rule allows address translation between the STUB domain (local) and the BACKBONE domain (global). There are configuration commands to configure each one of the parameters making up a NAT rule.

To create a NAT rule, use the **default** option, which creates a rule with the default values. To modify a NAT rule parameter, enter the command related to the parameter, indicating the identifier of the rule you wish to modify.

To simplify the configuration/modification, configure various parameters in the same command.

The default values for NAT rule parameters are as follows:

- Type of translation: internal source (**translate source**).
- Translation direction: local to global and global to local (**direction both**).
- Local interface: ethernet0/0.
- Global interface: ethernet0/0.
- Local subnet: ethernet0/0.
- Global subnet: ethernet0/0.

2.2.1.1 Configuring the type of translation

RULE <rule id> TRANSLATE <SOURCE | DESTINATION>

SOURCE	# internal source.
DESTINATION	# internal destination.

```
SNAT config>rule 1 translate destination
```

2.2.1.2 Configuring the translation direction

RULE <rule id> DIRECTION <LOCAL-TO-GLOBAL | GLOBAL-TO-LOCAL | BOTH | SKIP-LOCAL | SKIP-GLOBAL>

```
SNAT config>rule 1 direction skip-local
```

Note

If you configure a rule as **skip-local**, then the range of global addresses configured for the rule will be ignored. Likewise, if you configure the rule as **skip-global**, then the range of local addresses configured for the rule will be ignored.

2.2.1.3 Configuring the range of addresses

On configuring a NAT rule, indicate the local addresses, which have to be translated to global addresses.

RULE <rule id> **local-network** {<IP network address> <IP address mask> | <*Interface ID*>}

RULE <rule id> **global-network** {<IP network address> <IP address mask> | <*Interface ID*>}

The local and global networks are specified through their addresses and masks or, if dealing with the network connected to a device interface, indicate this through the said interface identifier.

```
SNAT config>rule 1 local-network 192.6.2.0 255.255.255.0
SNAT config>rule 1 global-network 80.6.2.0 255.255.255.0
```

Note

If on configuring one of the subnets, the mask of the other subnet is not the same, this is automatically modified so they agree.

2.2.1.4 Configuring the local and global Interfaces

On configuring a NAT rule, indicate which interface will provide access to the local domain and which interface to the global domain.

RULE <*rule id*> **local-network** <*IP address* | *Interface ID* | UNSPECIFIED>

RULE <*rule id*> **global-network** <*IP address* | *Interface ID*>

As you can see, the interface can be specified in two ways:

- IP address corresponding to the interface, whether this is a standard address or an unnumbered address (i.e., 0.0.0.x, where x is the interface number).
- Interface identifier i.e., ethernet0/0, serial0/0, etc.

Additionally, when dealing with the interface providing local domain access, there is a third possibility that consists of not specifying the local interface (**unspecified** option). This means said interface is not taken into consideration when deciding whether to apply the rule.

```
SNAT config>rule 1 local-interface 0.0.0.1
SNAT config>rule 1 local-interface serial0/0
SNAT config>rule 1 local-interface 192.168.1.1
```

Note

When you specify the local interface in the NAT rule, add a destination static IP route with a global network destination where the next hop is the local interface. This static route is not used in the routing process, but is used as a help route queried by NAT before executing global translation, to identify the local interface and consequently select the appropriate rule.

When the local interface isn't specified (**unspecified**) the help route isn't required.

2.2.1.5 Configuring an access list

When configuring a NAT rule, you can indicate that a preconfigured access control list controls the traffic to which the NAT rule applies.

RULE <*rule id*> **access-list** <*access list ID*>

The access list to apply should be preconfigured in the specific menu for the **access-list** feature. When you list the configuration, a 0 (zero) value indicates that the rule is not associated with any access list.

```
SNAT config>rule 1 access-list 3
```

Note

You need to take the following aspects into consideration when organizing the access list:

Note

- The access list is checked both in output (local transformation # global) as well as in input (global transformation # local).
- This check is carried out before executing the corresponding transformation.
- In the input translation (global # local), NAT inverts the IP header before executing the query: the source address and source port convert to the destination address and the port address; the destination address and the port address pass to the source address and the source port.

Note

If, for example, you do NOT want to apply NAT to the TELNET input sessions, then configure an access list with a **deny** rule indicating port 23 is the source port and not the destination port (as this will invert the packet header and consequently achieve a "match" when consulting the access list).

2.2.2 Modifying a NAT rule

As previously said, to modify a NAT rule parameter, enter the command relative to the parameter and indicate the rule to modify.

Suppose we have the following NAT rules configured:

```
SNAT config>list all
Static NAT is: enabled
 Id    Local Ifc         Global Ifc     Local network            Global network
--- ---------------  ---------------  ------------------      ------------------
1   ethernet0/0      serial0/0        192.6.2.0/24      >-S-! ...
2   ethernet0/0      81.23.4.12       ...               !-S-< 81.23.5.0/24
3   10.15.67.3       serial0/0        192.6.2.0/24      <-S-> 80.23.4.0/24
 Id   Acces-List
---  ------------
1   0
2   0
3   0
SNAT config>
```

To modify the direction, the global interface and the global network in rule number 1, execute the following command:

```
SNAT config>rule 1 direction both
SNAT config>rule 1 global-interface serial0/1
SNAT config>rule 1 global-network 80.23.3.0 255.255.255.0
```

The result is as follows:

```
SNAT config>list all
Static NAT is: enabled
 Id    Local Ifc         Global Ifc     Local network            Global network
--- ---------------  ---------------  ------------------      ------------------
1   ethernet0/0      serial0/1        192.6.2.0/24      <-S-> 80.23.3.0/24
2   ethernet0/0      81.23.4.12       ...               !-S-< 81.23.5.0/24
3   10.15.67.3       serial0/0        192.6.2.0/24      <-S-> 80.23.4.0/24

 Id   Acces-List
---  ------------
1   0
2   0
3   0
SNAT config>
```

2.2.3 Deleting a NAT rule

To delete a NAT rule, use the following command:

no rule *<rule id>*

```
SNAT config>no rule 1
Rule deleted
```

2.2.4 Listing the configured NAT rules

To list the configured NAT rules, use the following command:

list rules

Each rule has an associated identifier. Said identifier establishes the rule order or position number in 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.

```
SNAT config>list rules
 Id    Local Ifc         Global Ifc     Local network            Global network
--- ---------------  ---------------  ------------------      ------------------
1   ethernet0/0      serial0/0        192.6.2.0/24      >-S-! ...
2   ethernet0/0      81.23.4.12       ...               !-S-< 81.23.5.0/24
3   10.15.67.3       serial0/0        192.6.2.0/24      <-S-> 80.23.4.0/24
SNAT config>
```

2.2.5 Enable / Disable the NAT functionality

You can activate or deactivate the NAT feature in global mode running the following commands:

enable

disable or **no enable**

```
SNAT config>enable
```

```
SNAT config>disable
```

2.2.6 Displaying the NAT functionality state

To display the NAT functionality global state, use the following command:

list state

```
SNAT config>list state
Static NAT is: enabled
SNAT config>
```

2.2.7 Displaying all the NAT functionality configuration

To list the whole of the static NAT configuration, enter the following command:

list all

All information that can be viewed separately with the rest of the **list** commands is presented.

Firstly the NAT feature global status is displayed:

Subsequently, the configured NAT rules are shown. Each rule has an identifier associated with it. This identifier establishes the order or position number for the rule within the list.

The transformation type and meaning are specified in the following way:

- <-S-> Type: Internal Source. Direction: Local to Global and Global to Local.
- <-D-> Type: Internal Destination. Direction: Local to Global and Global to Local.
- >-S-> Type: Internal Source. Direction: Local to Global.
- >-D-> Type: Internal Destination. Direction: Local to Global.
- <-S-< Type: Internal Source. Direction: Global to Local.
- <-D-< Type: Internal Destination. Direction: Global to Local.
- >-S-! Type: Internal Source. Direction: Does not change local.
- >-D-! Type: Internal Destination. Direction: Does not change local.
- !-S-< Type: Internal Source. Direction: Does not change global.
- !-D-< Type: Internal Destination. Direction: Does not change global.

Finally, the access lists associated with each rule are shown. A 0 value indicates the rule does not have an associated access list.

```
SNAT config>list all
Static NAT is: enabled
 Id    Local Ifc         Global Ifc     Local network            Global network
--- ---------------  ---------------  ------------------      ------------------
1   ethernet0/0      serial0/0        192.6.2.0/24      >-S-! ...
2   ethernet0/0      81.23.4.12       ...               !-S-< 81.23.5.0/24
3   10.15.67.3       serial0/0        192.6.2.0/24      <-S-> 80.23.4.0/24

 Id   Acces-List
---  ------------
1   21
2   0
3   0
SNAT config>
```

2.2.8 EXIT

Returns to the higher prompt level (IP).

```
SNAT config>exit
IP config>
```

2.3 Commands summary

disable

[**no**] **enable**

LIST	ACCES-LIST-RULES
	ALL
	RULES
	STATE
NO RULE <*id*>	
RULE <*id*>	DEFAULT
	TRANSLATE <SOURCE | DESTINATION>
	DIRECTION <BOTH |LOCAL-TO-GLOBAL |GLOBAL-TO-LOCAL |SKIP-LOCAL |SKIP-GLOBAL>
	LOCAL-INTERFACE < *IP address* | *Interface ID* | UNSPECIFIED>
	GLOBAL-INTERFACE < *IP address* | *Interface ID*>
	LOCAL-NETWORK {< *IP address*> <*IP mask*> | <*Interface ID*>}
	GLOBAL-NETWORK {< *IP address*> <*IP mask*> | <*Interface ID*>}
	ACCESS-LIST <access list ID>

Note

The default rule has the following configuration:

TRANSLATE SOURCE

DIRECTION BOTH

LOCAL-INTERFACE ethernet0/0

GLOBAL-INTEFACE ethernet0/0

LOCAL-NETWORK ethernet0/0

GLOBAL-NETWORK ethernet0/0

ACCESS-LIST 0

EXIT

Chapter 3 Monitoring

3.1 NAT monitoring

This section summarizes and explains all of the router's NAT feature monitoring commands. These commands allow you to monitor the behavior of the NAT feature on the router and thus reach the desired operating specifications. Additionally, there is a SNAT events subsystem where you can obtain real time operating information.

To access the monitoring prompt, enter the following:

```
*monitor
Console Operator
+PROTOCOL IP
IP+NAT STATIC
-- Static NAT monitoring --
SNAT monit+
```

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

3.1.1 ? (HELP)

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

Syntax:

```
SNAT monit+?
```

Example:

```
SNAT monit+?
  list    Lists static NAT parameters
  exit    Exit to parent menu
SNAT monit+
```

3.1.2 LIST

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

Syntax:

```
SNAT monit+list ?
  connections    Displays non-transparent connections to the NAT
SNAT monit+list
```

3.1.2.1 LIST CONNECTIONS

Displays the list of non-transparent connections to the NAT. For static NAT, only the FTP control connections that have clients in the local domain and the server in the global domain, and which have also transmitted **port** commands where the packet length has changed, belong to this category.

The connection list fields represent the following:

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

Syntax:

```
SNAT monit+list connections
```

Example:

```
SNAT 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
FTP_CTRL   192.6.1.169:1147       192.6.1.5:21           1440 YES
SNAT monit+
```

3.1.3 EXIT

Run **exit** to return to previous prompt level.

Syntax:

```
SNAT monit+exit
```

Example:

```
SNAT monit+exit
IP+
```

Chapter 4 Examples

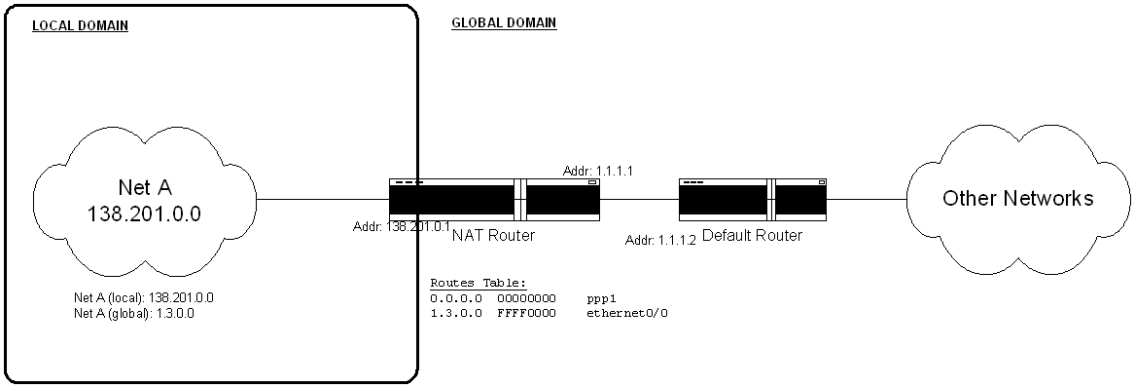
4.1 Static NAT

Over the previous chapters the static NAT application fields have been marked, here we have a series of examples to learn how to use the current implementation.

4.1.1 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 (1.0.0.0). 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, they randomly choose a network (138.201.0.0). Years pass and the time comes when they need total connectivity due to the development of new communication technologies. The first solution that arises is to change the local domain addresses for addresses belonging to the network assigned to the company. However, they quickly realize that this will not do because the department has many clients who have contracted continuous connectivity (24 hours per day and 7 days a week) with the local domain's addresses, and they would not accept solutions which would mean failure to comply with that contract.

The solution for the organization's department is to configure static NAT on the router making the connection between the department and the rest of the corporate Intranet, so that the network for said department is accessible for the rest of the Intranet as 1.3.0.0. The following shows how to configure the NAT router:



- Interface Configuration (basic)

```
*config
Config>set data-link sync serial0/0
Config>add device ppp 1
Config>network ppp1
-- Generic PPP User Configuration --
ppp1 config>base-interface
-- Base Interface Configuration --
ppp1 Base IFC config>base-interface serial0/0 link
ppp1 Base IFC config>exit
ppp1 config>ip address 1.1.1.1 255.0.0.0
ppp1 config>exit
Config>network ethernet0/0
-- Ethernet Interface User Configuration --
ethernet0/0 config>ip address 138.201.0.1 255.255.0.0
ethernet0/0 config>exit
Config>
```

- IP Configuration

```
Config>protocol ip
-- Internet protocol user configuration --
; routing process default route
IP config>route 0.0.0.0 0.0.0.0 ppp1
; static route to help NAT process
IP config>route 1.3.0.0 255.255.0.0 ethernet0/0
IP config>
```

Note

As the local interface is specified (ethernet0/0) in the NAT rule, to help the NAT process you need to add a static IP route whose destination is the global network (1.3.0.0) with the second hop being the local interface (ethernet0/0). This static route is not used in the routing process, but rather is a helper route that NAT consults before performing the global translation to identify the local interface and consequently select the appropriate rule.

When the local interface isn't specified (**unspecified**) the helper route isn't required.

- NAT configuration

```
IP config>nat static
-- Static NAT configuration --
SNAT config>enable
SNAT config>rule 1 default
SNAT config>rule 1 local-interface ethernet0/0
SNAT config>rule 1 local-network 138.201.0.0 255.255.0.0
SNAT config>rule 1 global-interface serial0/0
SNAT config>rule 1 global-network 1.3.0.0 255.255.0.0
SNAT config>
```

Note

The "rule 1 default" command is equivalent to the commands:

"rule 1 translate source"

"rule 1 direction both"

4.1.2 Selecting traffic through an access list

In the above scenario, let's suppose we want to perform NAT only on traffic coming from 138.201.1.0/24 going towards network 5.5.0.0/16. This is a classic static NAT case where you need to use an access list to refine the selection.

- Configuring the access lists:

The access list has two entries: entry 1 that selects outgoing traffic (local # global direction); entry 2 that selects incoming traffic (global # local direction). Entry two is inverted (see note), in addition the addressing for said entry is prior to undoing the NAT.

```
   feature access-lists
; -- Access Lists user configuration --
      access-list 100
         entry 1 default
         entry 1 permit
         entry 1 source address 138.201.1.0 255.255.255.0
         entry 1 destination address 5.5.0.0 255.255.0.0
;
         entry 2 default
         entry 2 permit
         entry 2 source address 1.3.1.0 255.255.255.0
         entry 2 destination address 5.5.0.0 255.255.0.0
;
      exit
;
   exit
```

Note

To correctly configure the access list, bear in mind the following aspects:

Note

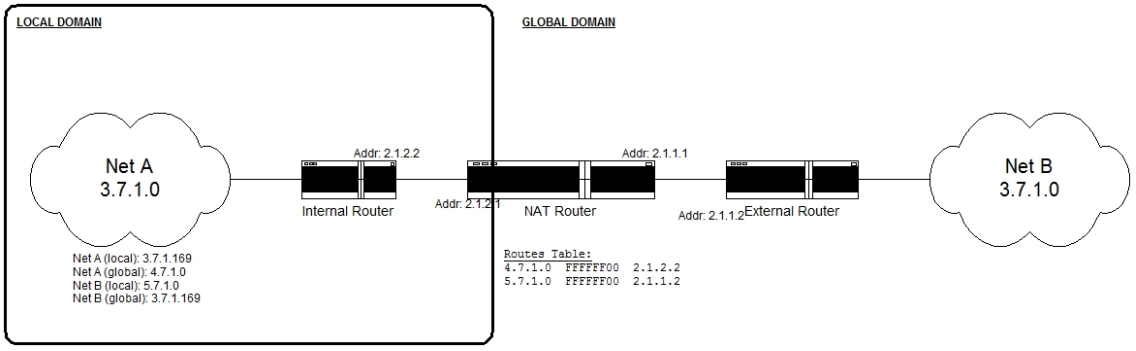
- The access list is consulted in both output (local # global transformation) and input (global # local transformation).
- This consultation is carried out before executing the corresponding transformation.
- In the input transformation (global # local), the NAT inverts the IP header before carrying out the query: the source address and source port become the destination address and the destination port; the destination address and the destination port become the source address and the source port.

- Configuring NAT: add the access list

```
IP config>nat static
-- Static NAT configuration --
SNAT config>enable
SNAT config>rule 1 default
SNAT config>rule 1 local-interface ethernet0/0
SNAT config>rule 1 local-network 138.201.0.0 255.255.0.0
SNAT config>rule 1 global-interface serial0/0
SNAT config>rule 1 global-network 1.3.0.0 255.255.0.0
SNAT config>rule 1 access-list 100
```

4.1.3 Connecting two networks using the same address space

When a private network wishing to connect to a public network has IP addresses that officially belong to that public network, this is known as *overlapping*. NAT can be used to connect these networks. In the local domain, the public network that already has a global address must be seen as having another address (NAT type: change inside destination), while in the global domain the private network is seen with global addresses (NAT type: change inside source). The problem is solved with two bi-directional rules.



- IP Configuration

```
*config
Config>network ethernet0/0
-- Ethernet Interface User Configuration --
ethernet0/0 config> ip address 2.1.2.1 255.255.255.0
ethernet0/0 config>ip address 2.1.1.1 255.255.255.0 secondary
ethernet0/0 config>exit
Config>protocol ip
-- Internet protocol user configuration --
; help static route to the NAT process
IP config>route 4.7.1.0 255.255.255.0 2.1.2.2 1
; help static route to the NAT process
IP config>route 5.7.1.0 255.255.255.0 2.1.1.2 1
IP config>
```

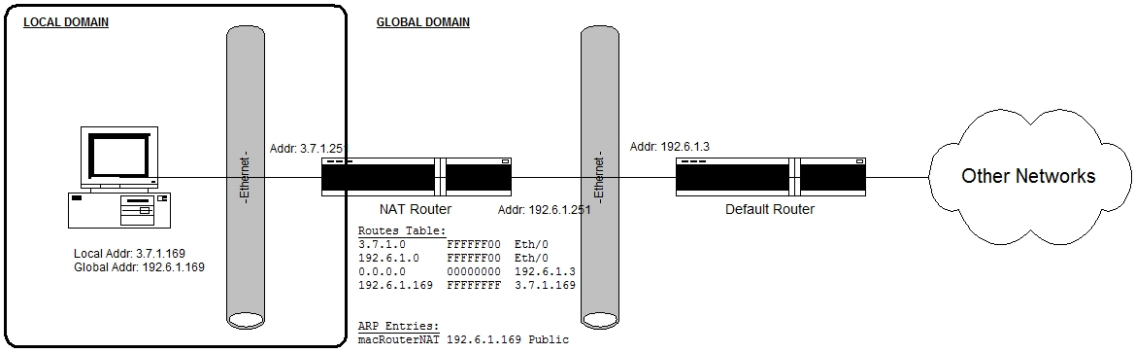
- NAT Configuration

```
IP config>nat static
-- Static NAT configuration --
SNAT config>enable
SNAT config>rule 1 translate source
SNAT config>rule 1 direction both
SNAT config>rule 1 local-interface 2.1.2.1
SNAT config>rule 1 local-network 3.7.1.0 255.255.255.0
SNAT config>rule 1 global-interface 2.1.1.1
```

```
SNAT config>rule 1 global-network 4.7.1.0 255.255.255.0
SNAT config>rule 2 translate destination
SNAT config>rule 2 direction both
SNAT config>rule 2 local-interface 2.1.2.1
SNAT config>rule 2 local-network 5.7.1.0 255.255.255.0
SNAT config>rule 2 global-interface 2.1.1.1
SNAT config>rule 2 global-network 3.7.1.0 255.255.255.0
SNAT config>
```

4.1.4 Address overlapping (autoaliasing)

This case is known as “autoaliasing”. Multiple clients want to configure NAT so they can translate their local addresses into unused subnet global addresses directly connected to the NAT router. This means the router must respond to ARP requests from said global addresses, so that any packet that is sent to one of these global addresses is accepted and translated by the NAT router. To achieve this, configure the permanent and public ARP entries in the router. The creation of these ARP entries is not automatic and must be carried out by the NAT router administrator in the NAT procedure. The following shows a simple example of this:



- Configuring the addresses and the routes:

```
*config
Config>network ethernet0/0
-- Ethernet Interface User Configuration --
ethernet0/0 config>ip address 3.7.1.251 255.255.255.0
ethernet0/0 config>ip address 192.6.1.251 255.255.255.0 secondary
ethernet0/0 config>exit
Config>protocol ip
-- Internet protocol user configuration --
IP config>route 0.0.0.0 0.0.0.0 192.6.1.3
IP config>route 192.6.1.169 255.255.255.255 3.7.1.169
IP config>exit
Config>
```

Route 192.6.1.169/32 via 3.7.1.169 is required so packets directed to IP address 192.6.1.169 are not routed through interface 192.6.1.251, but through interface 3.7.1.251.

- Configuring ARP:

```
*p 4
Config>protocol arp
-- ARP user configuration --
ARP config>entry ethernet0/0 192.6.1.169 00-a0-26-5c-1-1c public
ARP config>
```

Note

The NAT router MAC address can be obtained through the following:

```
*monitor
Console Operator
+
+device ethernet0/0
                                  Auto-test   Auto-test     Maintenance
Interface            CSR    Vect      valids    failures        failures
ethernet0/0     FA200E00      27           1           0               0
Physical address:  00A02670074C
```

```
PROM address:      00A02670074C
Speed:             10 Mbps

 Input statistics:
  failed, frame too long             0  failed, FCS error                 0
  failed, alignment error            0  failed, FIFO overrun              0
  internal MAC rcv error             0  packets missed                    0
 Output statistics:
  deferred transmission              0  single collision                  0
  multiple collisions                0  total collisions                  0
  failed, excess collisions          0  failed, FIFO underrun             0
  failed, carrier sense err          0  SQE test error                   0
  late collision                     0  internal MAC trans errors         0
  Ethernet MAC code release 1
+
```

- Configuring NAT:

```
SNAT Config>enable
SNAT config>rule 1 translate source
SNAT config>rule 1 direction skip-global
SNAT config>rule 1 local-interface 3.7.1.251
SNAT config>rule 1 global-interface 192.6.1.251
SNAT config>rule 1 global-network 192.6.1.255 255.255.255.255
SNAT config>rule 2 translate source
SNAT config>rule 2 direction skip-global
SNAT config>rule 2 local-interface 3.7.1.251
SNAT config>rule 2 global-interface 192.6.1.251
SNAT config>rule 2 global-network 192.6.1.0 255.255.255.255
SNAT config>rule 3 translate source
SNAT config>rule 3 direction skip-global
SNAT config>rule 3 local-interface 3.7.1.251
SNAT config>rule 3 global-interface 192.6.1.251
SNAT config>rule 3 global-network 192.6.1.251 255.255.255.255
SNAT config>rule 4 translate source
SNAT config>rule 4 direction both
SNAT config>rule 4 local-interface 3.7.1.251
SNAT config>rule 4 local-network 3.7.1.0 255.255.255.0
SNAT config>rule 4 global-interface 192.6.1.251
SNAT config>rule 4 global-network 192.6.1.0 255.255.255.0
SNAT config>
```

Listing the complete configuration:

```
Config>show config
; Showing System Configuration for access-level 15 ...
; XXX Router 2 156 Version 10.7.0
log-command-errors
no configuration
set data-link x25 serial0/0
set data-link x25 serial0/1
set data-link x25 serial0/2
;
network ethernet0/0
; -- Ethernet Interface User Configuration --
   ip address 3.7.1.251 255.255.255.0
   ip address 192.6.1.251 255.255.255.0 secondary
;
;
;
;
exit
;
;
;
network x25-node
; -- X25-node interface configuration --
   no ip address
;
```

```
exit
;
;
protocol ip
; -- Internet protocol user configuration --
   route 0.0.0.0 0.0.0.0 192.6.1.3
   route 192.6.1.169 255.255.255.255 3.7.1.169
;
;
   nat static
; -- Static NAT configuration --
      enable
      rule 1 default
      rule 1 direction skip-global
      rule 1 local-interface 3.7.1.251
      rule 1 global-interface 192.6.1.251
      rule 1 global-network 192.6.1.255 255.255.255.255
;
      rule 2 default
      rule 2 direction skip-global
      rule 2 local-interface 3.7.1.251
      rule 2 global-interface 192.6.1.251
      rule 2 global-network 192.6.1.0 255.255.255.255
;
      rule 3 default
      rule 3 direction skip-global
      rule 3 local-interface 3.7.1.251
      rule 3 global-interface 192.6.1.251
      rule 3 global-network 192.6.1.251 255.255.255.255
;
      rule 4 default
      rule 4 local-interface 3.7.1.251
      rule 4 global-interface 192.6.1.251
      rule 4 local-network 3.7.1.0 255.255.255.0
      rule 4 global-network 192.6.1.0 255.255.255.0
;
   exit
;
exit
;
protocol arp
; -- ARP user configuration --
   entry ethernet0/0 192.6.1.169 00-a0-26-5c-01-1c public
exit
;
;
dump-command-errors
```