7. NAT (Network address Translation)

NAT (Network address Translation - RFC 3022) е подход, осигуряващ преобразуване на локални в един или няколко глобални IP адреса. Целта е представяне на локалните хостове в Интернет пространството чрез ограничено използване на глобални IP адреси. Съществуват три основни реализации на този подход, поддържани от маршрутизиращите устройства:

- статична – съпоставя на всеки вътрешен адрес различен глобален адрес;
- динамична – обвързва група от локални адреса с един или няколко глобални адреса. За целта, в NAT таблиците на маршрутизаторите, където се асоциират локален с глобален IP адрес, се добавя и порт, идентифициращ комуникационния процес;
- смесена – обединява изброените преди това реализации.

локален адрес	**глобален адрес**
192.168.0.5	87.97.197.51
192.168.0.15	87.97.197.52
...	...

таблица 1 *Статично разпределение*

локален адрес	**порт**	**глобален адрес**	**порт**
192.168.0.5	80	87.97.197.51	6880
192.168.0.15	3389	87.97.197.51	6689
...	...	...	...

таблица 2 *Динамично разпределение*

7.1. Конфигуриране и потвърждаване на динамичната NAT в Cisco рутер

Динамична NAT (където вътрешните локални адреси се транслират във вътрешен глобален адрес, като динамично им се присвоява адрес от група със свободни адреси) може да се конфигурира със следните стъпки:

Стъпка 1: Създаване на списък за контрол на достъпа (ACL), който да съпоставя вътрешните локални адреси, които ще се транслират. Въпреки че може да се използва или именуван или номериран ACL, или стандартен или разширен ACL, командата за създаване на стандартен номериран ACL (в глобален режим на конфигуриране) е:

access-list **{1 - 99}** *permit* network_address wildcard_mask

Стъпка 2: Дефиниране на NAT група, съдържаща наличните вътрешни глобални адреси чрез командата

ip nat pool **pool_name** startingjp endinfjp *netmask* subnet_mask

Стъпка 3: Посочване на вътрешен за NAT интерфейс чрез командата

ip nat inside

Стъпка 4: Посочване на външен за NAT интерфейс

ip nat outside

Стъпка 5: Свързване на ACL (идентифициращ вътрешните локални адреси) с групата NAT (идентифицираща вътрешните глобални адреси)

ip nat inside source list **acl** *pool* **nat_pool**

7.2. Конфигуриране и потвърждаване на статична NAT в Cisco рутер

За разлика от динамичното конфигуриране на NAT, конфигурирането на статична NAT не изисква ACL или група NAT. Вместо това могат да бъдат подадени серия от команди за да инструктиране на NAT как да изпълнява транслациите си.

Стъпките за изпълняване на конфигурирането на статична NAT са както следва:

Стъпка 1: Създайте едно или повече съпоставяния на вътрешни локални адреси към вътрешни глобални адреси с командата

ip nat inside source static inside_local_address inside_global_address,

Стъпка 2: Посочване на вътрешен за NAT интерфейс чрез командата

ip nat inside

Стъпка 3: Посочване на външен за NAT интерфейс

ip nat outside

7.3.PAT в Cisco рутер

Едно неудобство в базовата NAT е това, че съществува съпоставяне едно-към-едно между вътрешните локални адреси и вътрешните глобални адреси, което означава, че една компания би имала нужда от толкова публично маршрутизирани IP адреси, колкото на брой вътрешни устройства с нужда от IP адреси има. Това не се мащабира добре, тъй като доставчикът на услуги често ще осигурява клиента с един IP адрес или малък брой от IP адреси.

За щастие маршрутизаторите на Cisco поддържат Port Address Translation (PAT), която позволява на множество вътрешни локални адреси да споделят един вътрешен глобален адрес (т.е., един публично маршрутизиран IP адрес). Спомнете си, че когато един клиент изпраща IP пакет, пакетът не само има IP адрес на източника и на получателя, но също така има и номер на порта на източника и получателя. PAT използва тези номера на портове, за да проследява отделните комуникационни потоци.

Стъпка 1: Създаване на списък за контрол на достъпа (ACL), който да съпоставя вътрешните локални адреси, които ще се транслират. Въпреки че може да се използва или именуван или номериран ACL, или стандартен или разширен ACL, командата за създаване на стандартен номериран ACL (в глобален режим на конфигуриране) е:

access-list **{1 - 99}** *permit* network_address wildcard_mask

Стъпка 2: Посочване на вътрешен за NAT интерфейс чрез командата

ip nat inside

Стъпка 3: Посочване на външен за NAT интерфейс

ip nat outside

Стъпка 4: Асоцииране на ACL (идентифициращ вътрешните локални адреси) с външния интерфейс на маршрутизатора, и активиране на прехвърляне с командата

ip nat inside source list **acl** *interface* **outsideinterface**