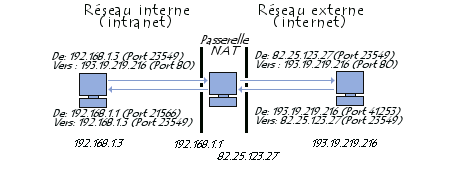
**NAT – Network address Translation**

Le principe du NAT consiste à utiliser une adresse IP routable (ou nombre limité d'adresses IP) pour connecter l'ensemble des machines d’un réseau LAN en réalisant, au niveau de la passerelle de connexion à internet, une translation (littéralement une « traduction ») entre l'adresse privée (local et non routable) et une adresse public (routable sur internet).



Configuration :

Dans un premier temps il faut définir sur le routeur WAN la partie LAN et la partie WAN.

**Fa0/1 = PORT vers le LAN**

**Fa0/2 = PORT vers le WAN**

|  |  |
| --- | --- |
| Définir le port LAN (Fa0/1) | Définir le port WAN (Fa0/2) |
| conf t  int Fa0/1  **ip nat inside**  exit | conf t  int Fa0/2  **ip nat outside**  exit |

L’objectif est ensuite de sélectionner le trafic concerné par la translation d’adresse, pour cela on utilise une ACL standard.

|  |  |
| --- | --- |
| Définition du trafic cible à translater par la suite. | ip access-list standard ACL-NAT  permit @IpRéseau @MasqueRéseau  exit  exemple :  ip access-list standard ACL  permit 10.0.0.0 0.0.0.255  exit  Information : Une des pratiques les plus sûres est de bloquer le NAT à destination des plages privées d’IP (LAN) et n’autoriser le NAT que sur des IP dites publics (Routable sur internet).  Exemple :  ip access-list extended ACL-NAT  deny ip any 10.0.0.0 0.255.255.255  deny ip any 172.16.0.0 0.15.255.255  deny ip any 192.168.0.0 0.0.255.255  permit ip any any |
| Traduction des IP en inside (local) à effectuer en s’appuyant sur l’ACL | ip nat inside source list **NOM-ACL** interface **@IntDeSortie** overload  Exemple :  ip nat inside source list ACL-NAT interface FastEthernet0/0 overload |

Il faut ensuite définir la route par défaut dans le routeur WAN

|  |  |
| --- | --- |
| Définition d’une route par défaut | conf t  ip route 0.0.0.0 0.0.0.0 @IpDeSortie  exemple : (voir schéma NAT)  conf t  ip route 0.0.0.0 0.0.0.0 192.169.1.1 |

Il est ensuite important de définir une route par défaut sur tous les routeurs du LAN pour envoyer le trafic ne correspondant pas aux plages locales vers le routeur WAN.

Le NAT possède une seconde application, dans le cas où nous souhaitons rendre joignable depuis l’extérieur une machine du LAN par exemple.

|  |  |
| --- | --- |
| Définition d’un port à écouter avec redirection sur une ip du LAN | ip nat inside source static tcp **@IpMachineCible @PortMachineCible** interface **@InterfaceD’écouteWAN** **@PortQuiEcouteWAN**  Exemple :  ip nat inside source static tcp 10.2.1.1 23 interface FastEthernet0/0 2323 |