Un lecteur Flash doit être installé pour profiter des animations liées à ce document.

Je vous recommande aussi le très bon cours d'openclassrooms sur le sujet.
Le NAT et le port forwarding

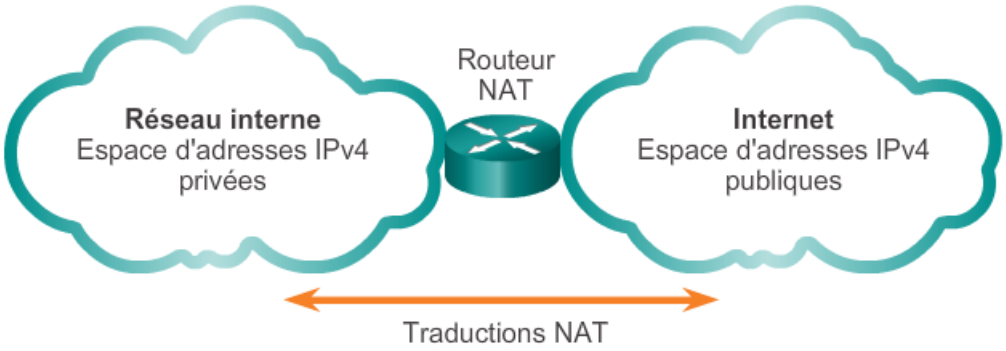


# TRADUCTION D'ADRESSE RESEAU IPV4 (NAT ET PAT)

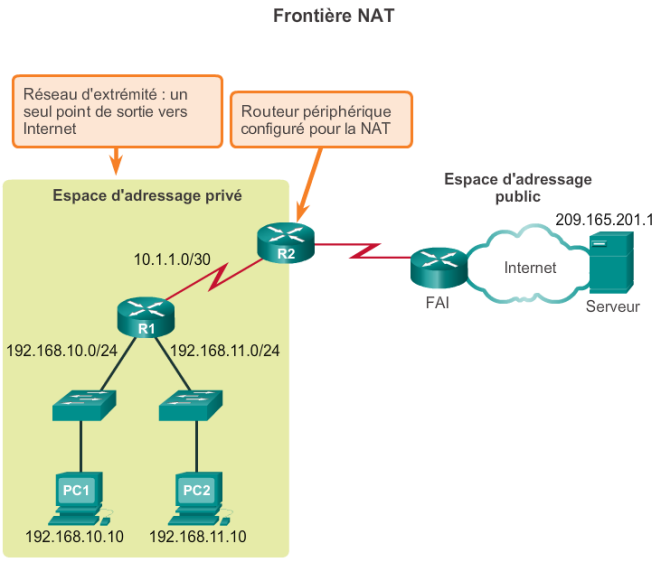
## 1 Objectif recherché

Pour pouvoir accéder à Internet, il faut disposer d'une adresse IP publique. Le nombre d'adresses IPv4 est limité théoriquement à 4,3 milliards, mais en pratique ce nombre est plus petit. Cette valeur peut paraître énorme, ou tout au moins suffisante, mais dans les faits c'est loin d'être le cas. Le gaspillage lié à l'utilisation des classes d'adresses IP ($2^{24}$-2 hôtes pour les réseaux de classe A), l'explosion des demandes émanant tant des industries que des particuliers, ont rapidement épuisé les adresses disponibles.

Dans la plupart des cas, on utilise les **adresses privées**[1] pour paramétrer les postes informatiques d'une entreprise. Cependant, comme ces adresses n'identifient aucune entreprise ou organisation unique, les adresses IPv4 privées ne peuvent pas être acheminées sur Internet. Pour permettre à un périphérique possédant une adresse IPv4 privée d'accéder aux périphériques et aux ressources situées en dehors du réseau local, l'adresse privée doit d'abord être traduite en adresse publique ; c'est le rôle de **NAT** (**N**etwork **A**ddress **T**ranslation)




La fonction NAT peut être utilisée à différentes fins, mais son utilisation principale consiste à limiter la consommation des adresses IPv4 publiques. Ainsi, elle permet aux réseaux d'utiliser des adresses IPv4 privées en interne, et assure la traduction de ces adresses en une adresse publique lorsque nécessaire uniquement. La NAT permet également d'ajouter un niveau de confidentialité et de sécurité à un réseau, car elle empêche les réseaux externes de voir les adresses IPv4 internes.




Les routeurs configurés pour la NAT peuvent être configurés avec une ou plusieurs adresses IPv4 publiques valides. Ces adresses publiques sont appelées collectivement « **pool NAT** ». Lorsqu'un périphérique interne envoie du trafic hors du réseau, le routeur configuré pour la NAT traduit l'adresse IPv4 interne du périphérique en une adresse publique du pool NAT. Pour les périphériques externes, tout le trafic entrant sur le réseau et sortant de celui-ci semble posséder une adresse IPv4 publique du pool d'adresses fourni.

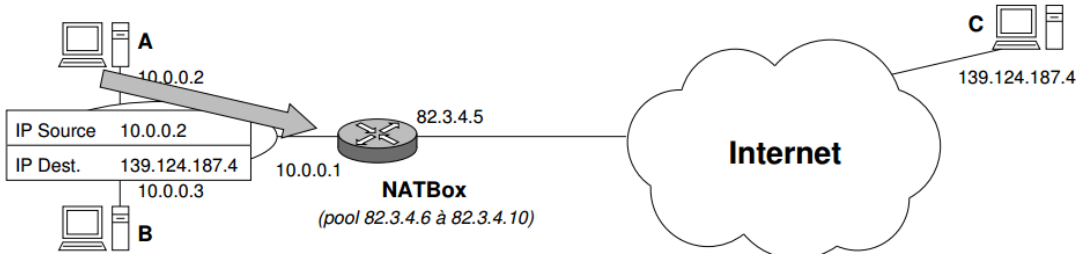
[1] Classe A : 10.0.0.0 à 10.255.255.255 (10.0.0.0 /8)
Classe B : 172.16.0.0 à 172.31.255.255 (172.16.0.0 /12)
Classe C : 192.168.0.0 à 192.168.255.255 (192.168.0.0 /16)

# 2 Principe et terminologie

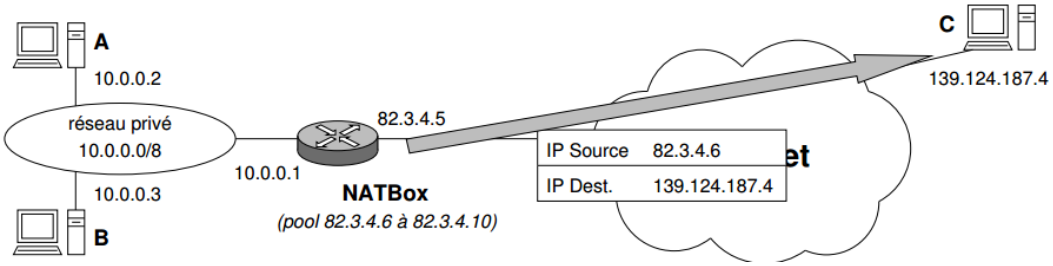
## 2.1 Analyse d'un exemple

Un poste A (10.0.0.2) d'un réseau local veut discuter avec une station C externe du réseau public (139.124.187.4)

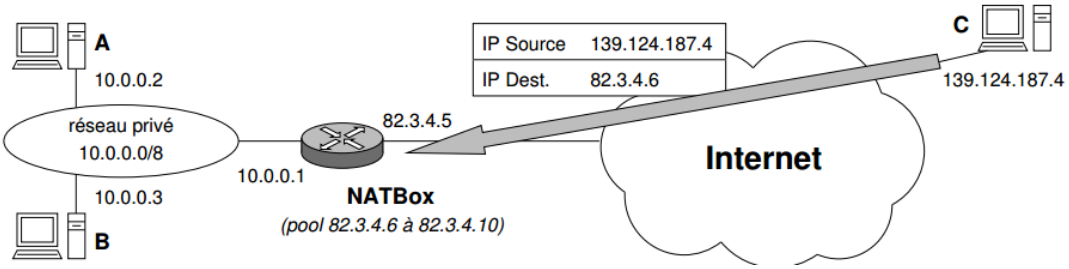
1. **A envoie le datagramme qui parvient au routeur (NATBox[2])**



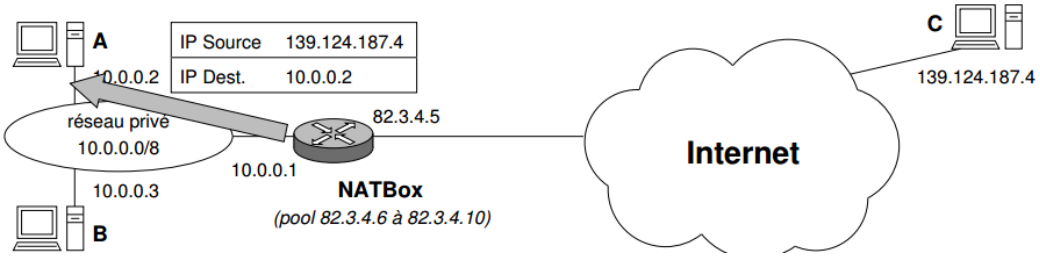

2. **la NATBox remplace l'adresse source (privée) par une adresse publique disponible (82.3.4.6), enregistre une association (82.3.4.6, 10.0.0.2) dans sa table de traductions, et transmet le datagramme vers C**




3. **C répond à l'adresse source du datagramme (82.3.4.6)**




4. **la NATBbox reçoit le datagramme, consulte sa table de traductions, trouve l'association (82.3.4.6, 10.0.0.2), remplace l'adresse destination par 10.0.0.2 et retransmet le datagramme à A**




[2] Une NATBox est un routeur avec les fonctionnalités NAT (la plupart des routeurs et les Box des FAI)

## 2.2 Terminologies

Issue de CISCO, la terminologie fait la distinction entre :

- les adresses **globales** : adresses publiques routables (sur Internet) car elles ont une signification à portée globale
- les adresses **locales** : n'ont un sens que localement, dans le Site NAT

Selon où l'on se trouve, on utilise l'un de ces types d'adresses :

- à l'**intérieur** (inside) du Site NAT, on utilise des adresses locales
- à l'**extérieur** (outside), on utilise des adresses globales

Les termes "interne" et "externe" sont associés respectivement aux termes "local" et "global" pour définir au final 4 types d'adresses

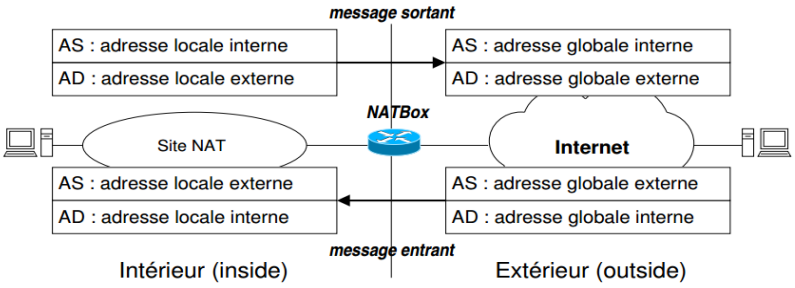
**Adresse Locale interne ou ALI** : adresse IP (généralement privée) assignée à un hôte à l'intérieur d'un réseau local d'extrémité.

**Globale interne** : adresse IP publique (vue par les hôtes situés du côté public) traduite représentant une ou plusieurs adresses IP locales internes. Ce sont les adresses publiques de la NATBox.

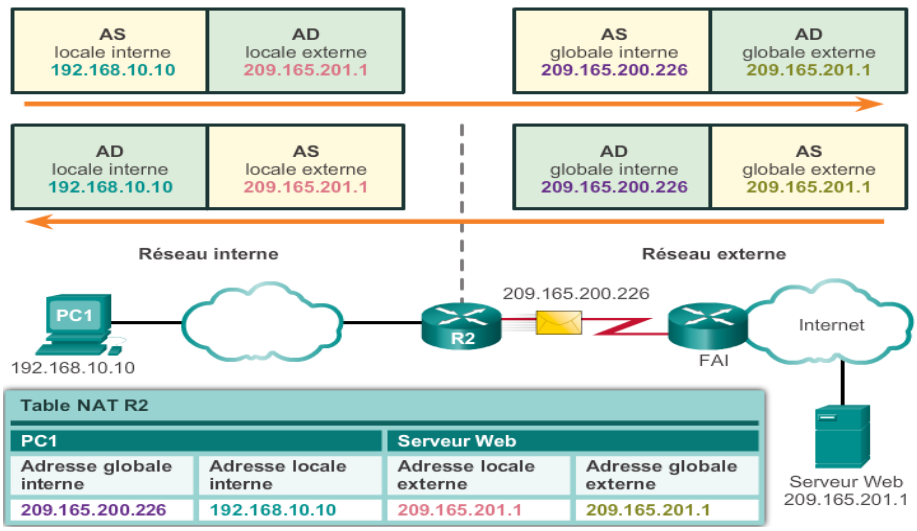
**Locale externe** : adresse IP d'un périphérique public (comme un serveur web) comme elle apparaît au réseau interne. Ce n'est pas nécessairement une adresse légitime, elle est allouée à partir d'un espace d'adresses routable à l'intérieur. Cette adresse est très souvent la même que l'adresse **globale externe**

**Globale externe** : adresse IP d'un périphérique externe public (comme un serveur web) vue par les hôtes d'une autre entreprise.

La NATBox traduit les adresses source (AS) et destination (AD) des messages qui franchissent la frontière inside/outside :




Exemples de traduction d'adresse réseau




Entrainez-vous avec cet exercice 

# 3 Types de NAT

Il existe 3 types de traduction NAT :

- **NAT statique** : correspondance un pour un établie entre les adresses locale et globale.
- **NAT dynamique** : mappage de plusieurs adresses locales vers plusieurs adresses globales.
- **Traduction d'adresses de port (PAT)** : mappage de plusieurs adresses locales et globales vers une seule. Cette méthode est également appelée « surcharge » (**surcharge NAT**).

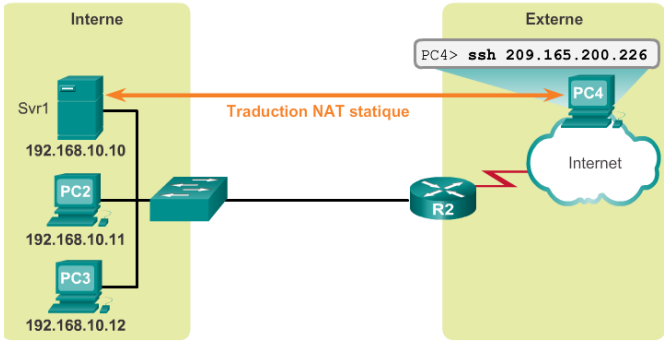
## 3.1 NAT statique (ou 1 pour 1)

La NAT statique fait correspondre **une adresse locale avec une adresse globale**. Le mot "statique" indique que ces mappages sont configurés par l'administrateur du routeur et restent constants (comme pour les routes statiques).

La NAT statique est particulièrement utile pour les périphériques qui doivent posséder une adresse permanente accessible depuis Internet comme la plupart des serveurs en DMZ (zone démilitarisée). En effet ce réseau isolé de l'entreprise est l'emplacement idéal pour les serveurs web, de messagerie ou autres qui doivent être accessibles depuis l'extérieur de l'organisation.

NAT statique

| Table NAT statique | |
|---|---|
| **Adresse locale interne** | **Adresse globale interne - adresses accessibles via R2** |
| 192.168.10.10 | 209.165.200.226 |
| 192.168.10.11 | 209.165.200.227 |
| 192.168.10.12 | 209.165.200.228 |




Il est possible également d'utiliser cette méthode pour accéder à distance à des périphériques pour des questions de gestion (exemple une connexion SSH vers un serveur ou un commutateur interne). Cette technique sera utilisée dans un laboratoire à des fins de pratique et de test. Dans la réalité, il vaut mieux privilégier la mise en place d'un VPN.

Comme le nombre de connexions simultanées vers le réseau public correspond au nombre d'adresses publiques disponibles pour le pool de la NAT (relation 1 pour 1), la quantité d'adresses publiques nécessaires risque vite de devenir importante. Imaginons, par exemple : le PC11 (192.168.1.1) qui a comme adresse réservée 99.34.24.2 et le PC12 qui a comme adresse réservée 99.34.24.3. PC11 et 12 utiliseront toujours et uniquement leur adresse réservée. Si PC23 ne possède pas de réservation NAT, il sera impossible pour lui d'exploiter la NAT et donc de joindre un serveur public.

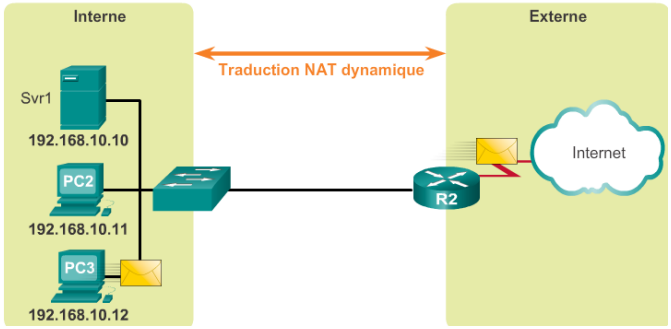
## 3.2 NAT dynamique

La NAT dynamique utilise un pool d'adresses publiques et les attribue selon la méthode du premier arrivé, premier servi. Lorsqu'un périphérique interne demande l'accès à un réseau externe, la NAT dynamique attribue une adresse IPv4 publique disponible du pool.

Sur la figure, PC3 a accédé à Internet à l'aide de la première adresse disponible dans le pool NAT dynamique. Les autres adresses sont toujours disponibles. Comme la fonction NAT statique, la NAT dynamique nécessite qu'il existe suffisamment d'adresses publiques disponibles pour satisfaire le nombre total de sessions utilisateur simultanées.

NAT dynamique

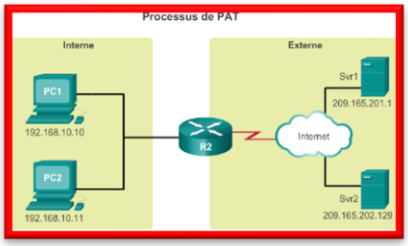
| Pool NAT IPv4 | |
|---|---|
| **Adresse locale interne** | **Pool d'adresses globales internes - adresses accessibles via R2** |
| 192.168.10.12 | 209.165.200.226 |
| Disponible | 209.165.200.227 |
| Disponible | 209.165.200.228 |
| Disponible | 209.165.200.229 |
| Disponible | 209.165.200.230 |



## 3.3 Traduction d'adresses de port (PAT) également appelée surcharge NAT

La traduction d'adresses de port (PAT), également appelée surcharge NAT, mappe plusieurs adresses IPv4 privées à une seule adresse IPv4 publique unique ou à quelques adresses. **C'est ce que font la plupart des routeurs de particuliers (vos box).** Le FAI attribue une adresse au routeur, mais plusieurs membres de la famille peuvent accéder simultanément à Internet. **C'est la forme la plus courante de NAT**.

Grâce à la PAT, plusieurs adresses peuvent être mappées à une ou quelques adresses, car chaque adresse privée est également identifiée par un numéro de port. Lorsqu'un périphérique établit une session TCP/IP, il génère une valeur de port source TCP ou UDP pour identifier de manière unique la session. Lorsque le routeur NAT reçoit un paquet du client, il utilise son numéro de port source pour identifier de manière unique la traduction NAT spécifique.




L'animation illustre le processus PAT. La fonction PAT ajoute des numéros de port source uniques à l'adresse globale interne, de façon à permettre de distinguer les traductions.

Lorsque R2 traite chaque paquet, il utilise un numéro de port (1331 et 1555 dans cet exemple) pour identifier le périphérique expédiant le paquet. L'adresse source (SA) correspond à l'adresse locale interne à laquelle a été ajouté le numéro de port TCP/IP attribué. L'adresse de destination (DA) est l'adresse locale externe à laquelle le numéro de port de service a été ajouté. Dans cet exemple, le port de service est 80 : HTTP.

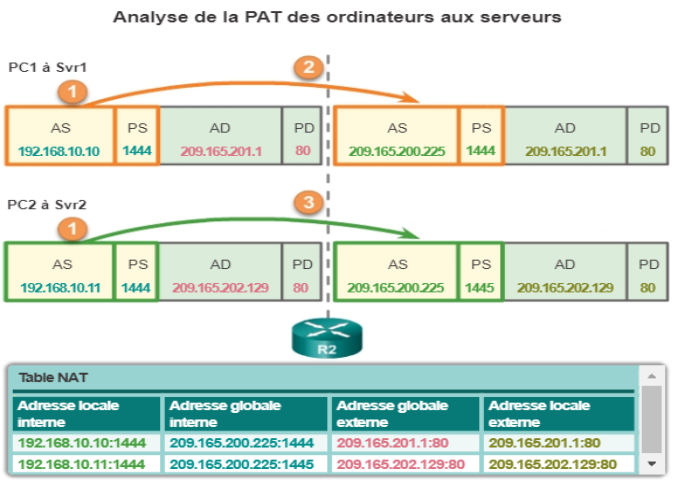
Concernant l'adresse source, R2 traduit l'adresse locale interne en une adresse globale interne à laquelle est ajouté le numéro de port. L'adresse de destination n'est pas modifiée, mais est désormais appelée adresse IP globale externe. Lorsque le serveur Web répond, le chemin est inversé. Dans l'exemple précédent, les numéros de port du client, 1331 et 1555, n'ont pas été modifiés par le routeur configuré pour la NAT. Ce scénario est peu probable, car il y a de fortes chances que ces numéros de port soient déjà liés à d'autres sessions actives.

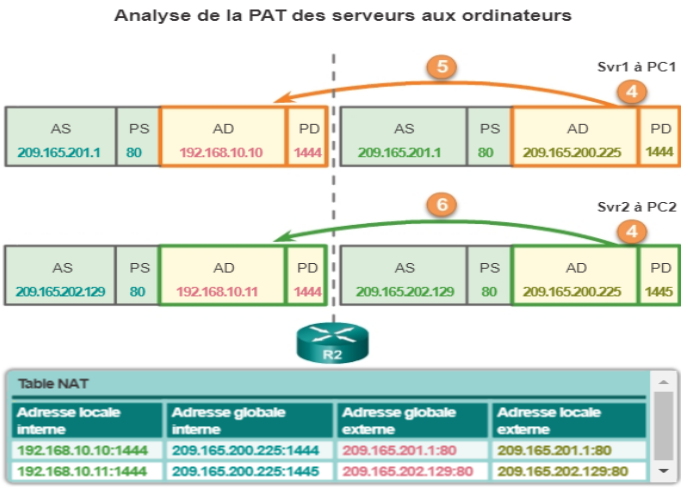
**La fonction PAT tente de conserver le port source d'origine**. Cependant, **si le port source d'origine est déjà utilisé, la PAT attribue le premier numéro de port disponible en commençant au début du groupe de ports approprié 0 à 511, 512 à 1 023 ou 1 024 à 65 535**. Lorsqu'il n'y a plus de ports disponibles et que le pool d'adresses comporte plusieurs adresses externes, la PAT passe à l'adresse suivante pour essayer d'attribuer le port source d'origine. Ce processus se poursuit jusqu'à ce qu'il n'y ait plus de ports ou d'adresses IP externes disponibles.

Dans l'exemple ci-dessous, les hôtes ont choisi le même numéro de port 1444. Cela est acceptable pour l'adresse interne, car les hôtes possèdent des adresses IP privées uniques.

Cependant, sur le routeur NAT, les numéros de port doivent être modifiés pour éviter que les paquets de deux hôtes différents quittent R2 avec la même adresse source.

Dans cet exemple, la PAT a attribué le port disponible suivant (1445) à la deuxième adresse d'hôte.




**Entraînez-vous avec cet exercice**

# 4 Avantages et inconvénients de la NAT

**Avantages**

- Elle conserve le schéma d'adressage officiellement inscrit et **elle économise les adresses** au moyen d'un multiplexage au niveau du port de l'application. Avec la surcharge NAT, plusieurs hôtes internes peuvent partager une même adresse IPv4 publique pour toutes leurs communications externes. Avec ce type de configuration, il suffit d'un très petit nombre d'adresses externes pour desservir un grand nombre d'hôtes internes.

- Elle **augmente la souplesse des connexions au réseau public** car Il est possible de mettre en œuvre des pools multiples, des pools de secours et des pools d'équilibrage de la charge pour assurer des connexions plus fiables au réseau public.

- Elle assure la **cohérence des schémas d'adressage** du réseau interne. Sur un réseau qui n'utilise pas d'adresses IPv4 privées ni la NAT, la modification du schéma des adresses IPv4 publiques nécessite le réadressage de tous les hôtes du réseau existant. Le coût de cette opération peut être considérable.

- Elle garantit la **sécurité du réseau**. Les réseaux privés ne divulguant pas leurs adresses ou leur topologie interne, ils restent raisonnablement sécurisés quand ils sont utilisés conjointement à la fonction NAT pour obtenir un accès externe. La fonction NAT ne remplace cependant pas les pare-feu.

**Inconvénients**

- **Dégradation des performances**. La fonction NAT augmente les délais de commutation car la traduction de chaque adresse IPv4 des en-têtes de paquet prend du temps. Le premier paquet est commuté par le processus, ce qui veut dire qu'il emprunte toujours le chemin le plus lent. Le routeur examine chaque paquet pour déterminer s'il doit être ou non traduit. Il doit modifier l'en-tête IPv4 et éventuellement l'en-tête TCP ou UDP. La somme de contrôle de l'en-tête IPv4 ainsi que la somme de contrôle TCP ou UDP doivent être recalculées à chaque traduction. Les paquets restants passent par le chemin à commutation rapide s'il existe une entrée de cache ; sinon, ils sont également retardés.

- **Dégradation de la fonctionnalité de bout en bout**. De nombreux protocoles et applications Internet dépendent de l'adressage de bout en bout de la source à la destination. Certaines applications ne sont pas compatibles avec la NAT. Par exemple, certaines applications de sécurité, telles que les signatures numériques échouent, car l'adresse IPv4 source change avant d'atteindre la destination. Les applications qui utilisent des adresses physiques au lieu d'un nom de domaine qualifié n'atteignent pas les destinations qui sont traduites sur le routeur NAT. Ce problème peut parfois être évité par l'utilisation de mappages NAT statiques.

- **Perte de la traçabilité IP de bout en bout**. Il devient bien plus difficile de suivre les paquets qui subissent de nombreux changements d'adresse sur plusieurs sauts NAT, ce qui complique le dépannage.

- **Perturbations éventuelles de l'établissement des connexions TCP**. Les services nécessitant l'établissement de connexions TCP depuis le réseau externe ou les protocoles sans état tels que ceux utilisant UDP peuvent être perturbés. Si le routeur NAT n'a pas été configuré pour prendre en charge ce type de protocole, les paquets entrants ne peuvent pas atteindre leur destination. Certains protocoles peuvent accepter une instance de NAT entre les hôtes participants (FTP en mode passif, par exemple), mais échouent lorsque les deux systèmes sont coupés d'Internet par la NAT.

# TP de découverte de la NAT

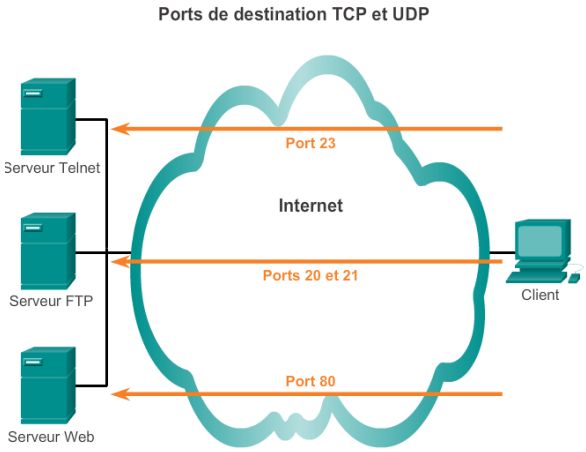
# 5 La redirection d'adresses réseau (ou port forwarding)

La redirection (parfois appelée transmission tunnel ou port forwarding) consiste à transférer un port réseau d'un nœud réseau à un autre. **Cette technique permet à un utilisateur externe d'atteindre un port sur une adresse IPv4 privée (dans un réseau local) à partir de l'extérieur**, via un routeur configuré pour la NAT. **C'est par exemple ce qui va vous permettre d'accéder à votre serveur Web installé sur le réseau de votre domicile.**

En règle générale, les programmes et opérations de partage de fichiers peer to peer, tels que les services Web et le FTP sortant, exigent que les ports du routeur soient redirigés ou ouverts pour que ces applications puissent fonctionner (voir Figure 1). La NAT masquant les adresses internes, l'opération peer to peer ne fonctionne que de l'intérieur vers l'extérieur, car la NAT peut mapper les requêtes sortantes avec les réponses entrantes.

Le problème est que la NAT n'autorise pas les requêtes provenant de l'extérieur. Ce problème peut être résolu par une intervention manuelle. La redirection de port peut être configurée pour identifier des ports spécifiques pouvant être redirigés vers des hôtes internes.

Rappelez-vous que les applications Internet interagissent avec des ports utilisateur qui doivent être ouverts ou à la disposition de ces applications. Les applications utilisent des ports différents. Cela permet aux applications et aux routeurs d'identifier les services réseau de manière prévisible. Par exemple, HTTP fonctionne sur le port réservé 80. Lorsque quelqu'un saisit l'adresse http://cisco.com, le navigateur affiche le site Web de Cisco Systems, Inc. Notez qu'il n'est pas nécessaire de préciser le numéro de port HTTP pour demander la page, car l'application suppose qu'il s'agit du port 80.




Si un autre numéro de port est requis, il peut être ajouté à la fin de l'URL après le signe deux-points (:). Par exemple, si le serveur Web écoute le port 8080, l'utilisateur saisit http://www.example.com:8080.

La redirection permet aux utilisateurs sur Internet d'accéder aux serveurs internes à l'aide de l'adresse du port WAN du routeur et du numéro de port externe correspondant. Les serveurs internes sont généralement configurés avec des adresses IPv4 privées de l'espace RFC 1918. Lorsqu'une requête est envoyée à l'adresse IPv4 du port WAN via Internet, le routeur transfère la demande au serveur approprié sur le réseau local. Pour des raisons de sécurité, les routeurs à large bande n'autorisent pas par défaut le transfert d'une requête réseau externe vers un hôte interne.

Sur la figure, le gérant d'une petite entreprise utilise un serveur de point de vente (PoS) pour suivre les ventes et le stock dans le magasin. Le serveur est accessible dans le magasin, mais comme il ne possède pas d'adresse IPv4 publique, il n'est pas accessible publiquement sur Internet. L'activation de la redirection sur le routeur local permet au gérant d'accéder au serveur de point de vente en tout lieu à partir d'Internet. La redirection sur le routeur est configurée avec le numéro de port de destination et l'adresse IPv4 privée du serveur de point de vente. Pour accéder au serveur, le logiciel client utilise l'adresse IPv4 publique du routeur et le port de destination du serveur.