Administration Systèmes

Adressages IP et NAT

COURS 09

Ahmed Amou El Arby

1

Adressage IP traditionnel

Une adresse IP (32 bits, 4 octets) est divisée en deux :

- un **numéro de réseau** ou adresse de réseau (network id) attribuée par une autorité
- un **numéro de hôte** ou identificateur local de machine (host id) attribué par l'administrateur du réseau

Le découpage dépend de la classe d'adresse …

Il existe 5 classes d'adresses :

- Classe A : N.H.H.H
- Classe B : N.N.H.H
- Classe C : N.N.N.H
- Classe D : Adresse utilisées pour le multicast
- Classe E : non utilisée

N = network

H = host

2

Classes d'adresses

Classe	Bits de poids forts 0	1	2	3	Numéro de réseau premier	dernier	Numéro de hôte premier	dernier
A	0	-	-	-	**0**.0.0.0	**127**.0.0.0	N.0.0.0	N.255.255.255
B	1	0	-	-	**128.0**.0.0	**191.255**.0.0	N.N.0.0	N.N.255.255
C	1	1	0	-	**192.0.0**.0	**223.255.255**.0	N.N.N.0	N.N.N.255
D	1	1	1	0	**224.0.0.0**	**239.255.255.255**	NA	
E	1	1	1	1	**240.0.0.0**	**255.255.255.255**	NA	

3

Adressage avec classe

Classe	Adresse	Réseaux
A	0nnnnnnn.H.H.H	**0**0000000.**H.H.H** à **0**1111111.**H.H.H** 0.0.0.0 à 127.0.0.0 (128 réseaux de classe A)
B	10nnnnnn.N.H.H	**10**000000.00000000**.H.H** à **10**111111.11111111**.H.H** 128.0.0.0 à 191.255.0.0 (16 384 réseaux de classe B)
C	110nnnnn.N.N.H	**110**00000.00000000.00000000.**H** à **110**11111.11111111.11111111.**H** 192.0.0.0 à 223.255.255.0 (2 097 152 réseaux de classe C)

- Un réseau " à classe" (classfull) à masque implicite:
  - Classe A: préfixe de longueur 8, masque 255.0.0.0
  - Classe B: préfixe de longueur 16, masque 255.255.0.0
  - Classe C: préfixe de longueur 24, masque 255.255.255.0
- Les anciens routeurs suivaient souvent le masque implicite.
- Les routeurs d'aujourd'hui utilisent toujours un masque explicite (/longueur de la portion réseau).

4

Adresses réservées

Certaines adresses sont réservées

- Soi-même : 127.0.0.1 (loopback ou localhost) pour tests
- Portion hôte = tous 0 : Adresse de réseau
- Portion hôte = tous 1 : Adresse de diffusion
- 0.0.0.0 : une machine qui ne connaît pas son adresse (station sans disque)

D'autres sont pour usage privé uniquement …

5

Adresses privées

Pour des réseaux privés qui sont directement ou indirectement connectés à Internet, il faut utiliser une plage d'adresses IP valides de classe A, B ou C.

Pour des réseaux privés qui sont indirectement connectés à Internet via un traducteur d'adresses réseau (NAT) ou une passerelle de couche d'application telle qu'un serveur proxy, l'IANA conseille d'utiliser des adresses IP privées :

Classe	ID de réseau privé	Plage d'adresses IP
A	10.0.0.0	10.0.0.1 - 10.255.255.254
B	172.16.0.0	172.16.0.1 - 172.31.255.254
C	192.168.0.0	192.168.0.1 - 192.168.255.254

Les nombres de ces plages sont réservés par l'IANA pour une utilisation privée sur les réseaux TCP/IP et ne sont pas utilisés sur Internet.

6

Adressage sans classe

- Oubliez les classes A, B et C ☹
- Le routage et la gestion des adresses se font aujourd'hui sans classe.
- **CIDR = Classless Inter Domain Routing**
  - Le routeur ne déduit pas le réseau à partir des trois premiers bits (classe).
  - Tous les adresses de réseaux sont annoncées avec leur préfixe.
- **VLSM = Variable Length Subnet Masks**
  - Avec l'adressage par classe, le masque de sous-réseau fixe le nombre de sous-réseaux et par conséquent le nombre de stations par sous-réseau.
  - Des longueurs de masque variables peuvent être utilisées, ce qui permet d'optimiser l'attribution des adresses.
  - Un groupe d'adresses peut être sous-réseauté, chaque sous-réseau peut également être sous-réseauté et ainsi de suite.
- Un fournisseur de service Internet (ISP) obtient un gros bloc d'adresses
  - Ex : un préfixe /16, c'est à dire 65536 adresses
- Il alloue des blocs plus petits à différents clients
  - Ex : un préfixe /22 (1024 adresses) à un client A
  - Ex : un préfixe /28 (16 adresses) à un client B
- Le client A qui obtient un /22 de son ISP peut à son tour le sous-diviser en blocs plus petits
  - Ex: un préfixe /26 (64 adresses) pour un département A1
  - Ex: un préfixe /27 (32 adresses) pour un département A2

7

Répartition des adresses IP

- Le problème de la répartition des adresses IP dans le réseau doit être résolu avec comme objectifs :
  - de rendre le réseau aussi lisible que possible (facilité de maintenance et modifications)
  - s'accommoder de la pénurie des adresses IP publiques
  - participer à la sécurité

8

Répartition des adresses IP

- Les outils utilisés pour faire les choix de répartition des adresses sont :
  - la translation d'adresses (Network Address Translation NAT) et translation de ports (Port Address Translation PAT)
  - le protocole DHCP
- Ces outils permettent d'organiser le réseau pour qu'un minimum d'adresses publiques soit utilisées, ce qui est :
  - bon pour la sécurité
  - satisfaisant dans le contexte de pénurie d'adresses

9

NAT : définitions

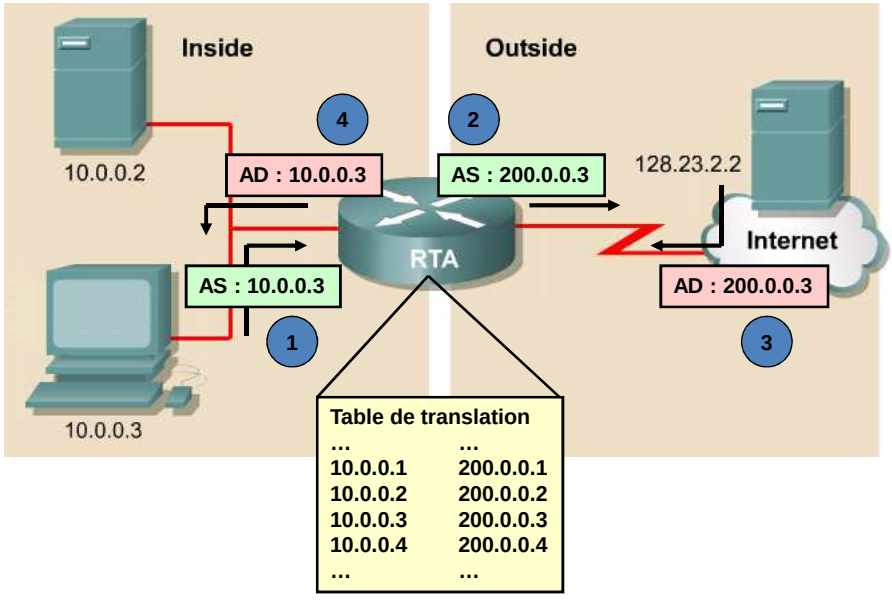
- Le NAT permet d'attribuer des adresses privées aux machines internes du réseau, et cependant de leur permettre d'accéder à Internet
- Dans un contexte NAT, pour comprendre une transmission, il faut faire intervenir 4 adresses IP :
  - adresse locale interne
  - adresse locale externe
  - adresse distante externe
  - adresse distante interne

10

NAT pur

- On utilise dans ce cas autant d'adresses publiques qu'il y a d'adresses privées
- Cette technique n'est jamais utilisée sous cette forme, elle est montrée ici pour expliquer le fonctionnement
- On parle aussi dans ce cas de NAT statique

NAT pur


Inside
Outside
10.0.0.2
4
AD : 10.0.0.3
2
AS : 200.0.0.3
128.23.2.2
Internet
RTA
AS : 10.0.0.3
AD : 200.0.0.3
1
3
10.0.0.3
Table de translation
... ...
10.0.0.1 200.0.0.1
10.0.0.2 200.0.0.2
10.0.0.3 200.0.0.3
10.0.0.4 200.0.0.4
... ...

12

NAT pur

1. Une machine locale envoie un paquet avec comme adresse source son adresse privée
2. Le routeur chargé de la translation fait correspondre à chaque adresse privée, une adresse publique. Il envoie vers l'extérieur le paquet IP en changeant l'adresse source privée par son correspondant publique
3. Le destinataire reçoit un paquet IP dont il pense qu'il vient d'une machine ayant une adresse publique et va donc y répondre
4. Le routeur reçoit la réponse, fait la correspondance dans le sens adresse publique – adresse privée et retransmet le paquet modifié à la bonne machine interne

NAT et PAT

- Il est illusoire de chercher à faire correspondre une adresse publique à chaque adresse privée
- Il faut combiner le NAT et le PAT pour utiliser en sortie un nombre d'adresses IP publiques largement inférieur au nombre des adresses privées à translater :

La translation se fait à la fois sur l'adresse IP et le numéro de port

14

NAT et PAT

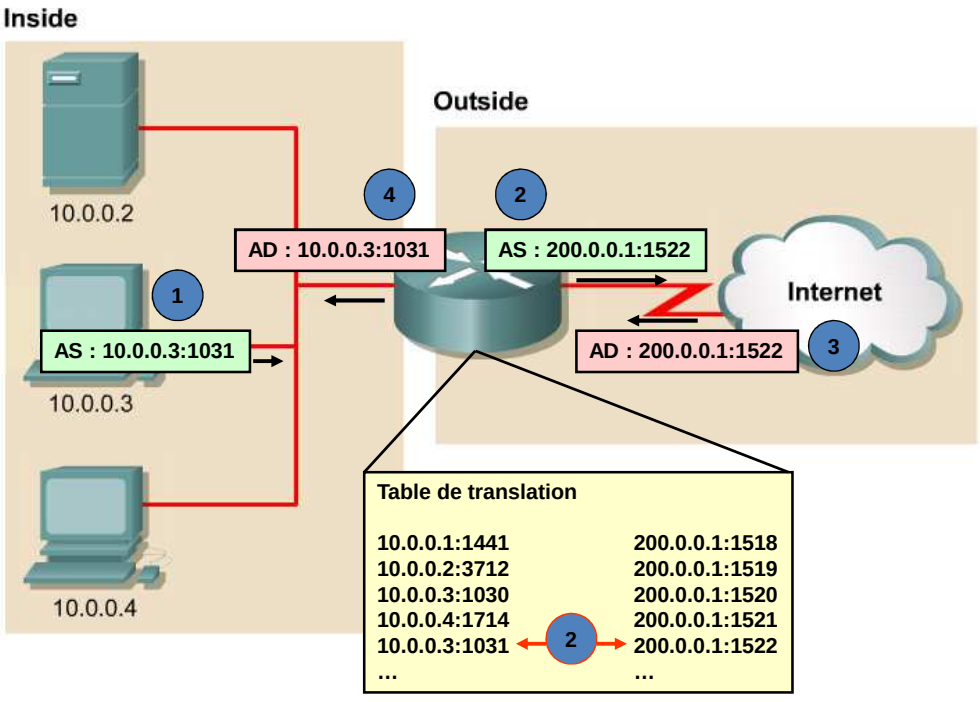
- Dans le cas de la translation vers une seule adresse IP en sortie, on parle de PAT pur
- Dans le cas de la translation vers plusieurs adresses en sortie (mais quand même beaucoup moins nombreuses que les adresses internes), on parle de NAT dynamique

15

PAT pur

- Dans le cas du PAT pur, toutes les adresses privées sont translatées vers une seule adresse publique
- Le routeur retrouvera la bonne adresse privée grâce au numéro de port TCP

PAT pur


Inside
Outside
10.0.0.2
10.0.0.3
10.0.0.4
1
AS : 10.0.0.3:1031
4
AD : 10.0.0.3:1031
2
AS : 200.0.0.1:1522
Internet
AD : 200.0.0.1:1522
3
Table de translation
10.0.0.1:1441
10.0.0.2:3712
10.0.0.3:1030
10.0.0.4:1714
10.0.0.3:1031
...
2
200.0.0.1:1518
200.0.0.1:1519
200.0.0.1:1520
200.0.0.1:1521
200.0.0.1:1522
...

17

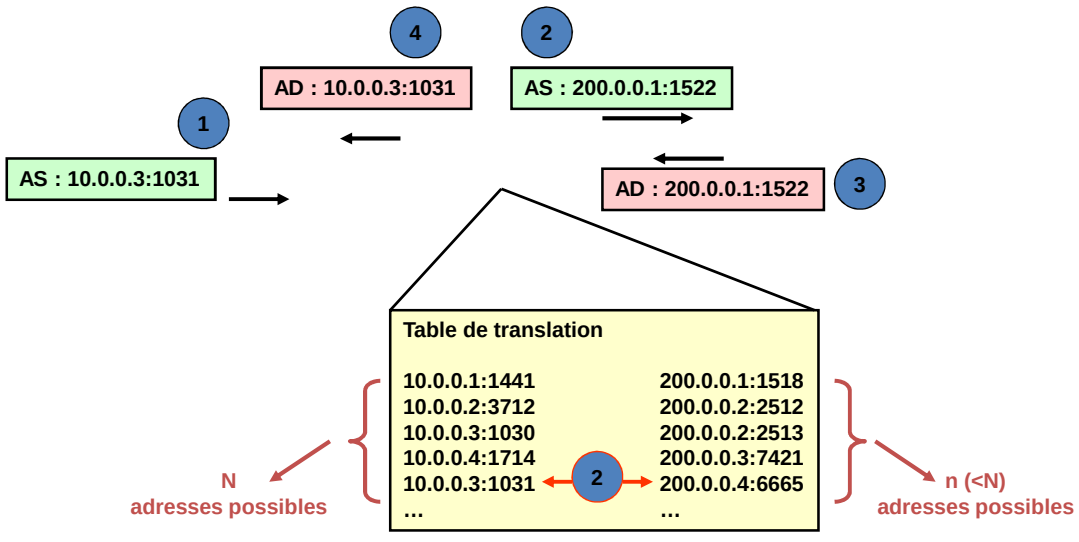
PAT pur

1. Une machine locale envoie un paquet IP en mettant son adresse privée comme source et en utilisant un certain numéro de port TCP
2. Le routeur local crée une ligne de plus dans sa table de translation, dans laquelle il inscrit :
   - l'adresse privée source avec le numéro de port TCP utilisé par l'utilisateur interne
   - l'adresse publique et le numéro de port qu'il utilise pour translater
3. Le serveur distant répond au routeur sans se rendre compte de quoi que ce soit
4. Le routeur procède à la translation inverse en cherchant la bonne entrée dans sa table de translation

NAT et PAT

- Dans le cas général, on utilise plusieurs adresses publiques en sortie, mais elles sont toujours beaucoup moins nombreuses que les adresses privées internes
- Le routeur applique un algorithme pour répartir les adresses et choisir les numéros de ports qu'il utilise

NAT et PAT

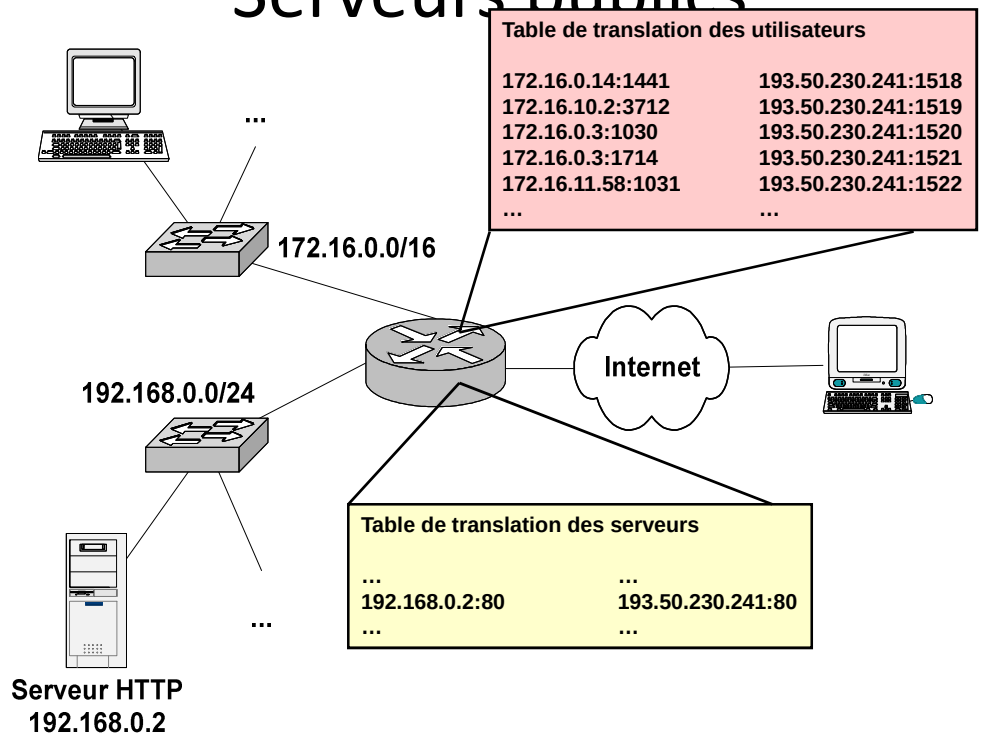

4
2
AD : 10.0.0.3:1031
AS : 200.0.0.1:1522
1
AS : 10.0.0.3:1031
AD : 200.0.0.1:1522
3
Table de translation
10.0.0.1:1441
10.0.0.2:3712
10.0.0.3:1030
10.0.0.4:1714
10.0.0.3:1031
...
200.0.0.1:1518
200.0.0.2:2512
200.0.0.2:2513
200.0.0.3:7421
200.0.0.4:6665
...
2
N
adresses possibles
n (<N)
adresses possibles

Serveurs publics

- Le NAT peut aussi être utilisé pour des serveurs publics
- Un administrateur peut faire le choix de donner des adresses privées à ses serveurs publics
- Il doit alors installer une translation statique pour les rendre visibles depuis l'Internet
- La translation peut alors être vue comme un autre niveau de filtrage, en plus des ACLs, dans le sens où, les paquets qui ne peuvent être translatés sont tout simplement ignorés

21

Serveurs publics



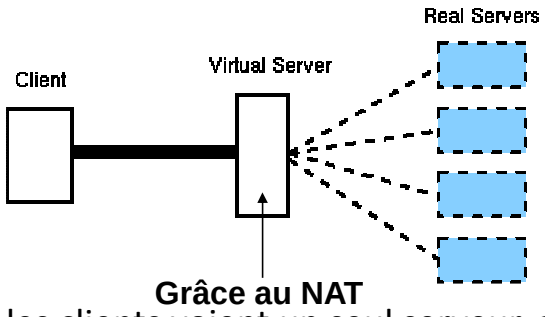
22

Translation du DNS

- Le serveur DNS pose un problème particulier pour la translation
- En effet, le DNS est utilisé à la fois :
  - par les postes internes pour lesquels les serveurs publics doivent être visibles par leur @IP privée
  - et par les utilisateurs externes pour lesquels les serveurs publics doivent être visibles par leur @IP publique
- Cela signifie que le DNS doit fournir des réponses différentes, en fonction de l'origine de la requête !
- Certains administrateurs choisissent d'installer deux DNS pour le même domaine :
  - un pour les utilisateurs internes
  - un autre pour les utilisateurs externes

NAT et équilibrage de charge

- Le NAT peut permettre l'équilibrage de charge entres plusieurs serveurs



- Grâce au NAT, les clients voient un seul serveur, alors que physiquement, plusieurs se partagent le travail

24

NAT et équilibrage de charge

- Le client se connecte en utilisant toujours la même adresse IP, celle donnée par le DNS
- Le translateur à l'entrée du réseau des serveurs translate l'@IP destination de la requête vers l'adresse de l'un des serveurs physiques
- Le choix du serveur physique repose sur un algorithme d'équilibrage de charge exécuté par le translateur
- Ainsi le translateur doit :
  - Suivre les sessions TCP pour diriger les bons paquets vers les bons serveurs
  - Mesurer la charge sur chaque serveur (en comptant les paquets par exemple)
  - Décider de la translation vers le serveur le moins chargé

25

NAT PAT : avantages

- Permet d'utiliser des adresses privées pour le réseau interne :
  - donne toute la souplesse utile pour le choix des adresses
  - rend les machines internes indétectables de l'extérieur
- Permet d'utiliser des adresses privées pour les serveurs publics :
  - permet de « cacher » plusieurs serveurs derrière une seule adresse
  - oblige l'administrateur à expliciter toutes les connexions autorisées
- Dans les deux cas, le changement des adresses publiques (pour cause de changement de FAI) se fera simplement en modifiant le NAT, et pas toutes les machines

Bénéfices pour la sécurité

- Les paquets qui entrent dans le réseau sont translatés seulement si l'entrée correspondante existe dans la table NAT
- Dans le cas contraire, les paquets sont simplement ignorés
- Ainsi, une connexion qui n'a pas été initiée par une requête sortante ne rentrera pas sur le réseau privé (sauf dans le cas des serveurs publics)

Cette propriété n'est cependant pas très performante pour la sécurité !

27

Bénéfices pour la sécurité

- Seules les connexions initiées depuis l'intérieur seront translatées en entrée, mais aucun compte n'est tenu des numéros de séquence/acquittement TCP

  Il ne s'agit donc pas du tout d'un vrai suivi de session TCP comme peuvent le faire certaines ACLs !

- Aucune protection n'est apportée par rapport au contenu des données
- Le contrôle des utilisateurs autorisés à initier des connexions depuis l'intérieur ne se fait qu'avec une ACL rudimentaire
- Il est souvent utile de préciser quels flux pourront être translatés en sortie en ajoutant des ACLs plus évoluées en plus du NAT

28

Bénéfices pour la sécurité

- Le NAT est utile d'abord pour donner une grande souplesse dans le choix des adresses IP des machines et des serveurs
- Le NAT présente des propriétés utiles pour la sécurité
- Pour la sécurité, l'utilisation du NAT n'est jamais suffisante, et ne dispense jamais la mise en place des autres outils (filtrage, firewall)

En aucun cas une stratégie de sécurité ne doit reposer que sur le NAT

29