M1 Info - Cours de Réseaux

Cours 5

« CIDR & NAT»

2018 – 2019

Dr Saadbouh O CHEIKH EL MEHDI

Adresse sans classe -CIDR

Un peu d'histoire !

- Lors de la conception d'IP et de son format d'adressage, Internet (ARPANET) ne rassemblait que les principales universités de recherche américaines, quelques entreprises et sites militaires
- En connectant les 2000 établissements d'enseignement supérieur des États-unis et de nombreuses universités étrangères, on ne devait pas dépasser 16 000 sites connectés
- Personne ne pensait qu'Internet deviendrait un réseau public mondial !!
- En 1996, 100 000 réseaux étaient déjà connectés à Internet
- **La moitié des réseaux de classe B ne contenait pas plus de 50 hôtes !!! (Gaspillage d'adresses !!?)**

Adresse sans classe - CIDR

Problèmes des classes !

- En 1993, il n'y avait déjà plus d'adresse de classe B disponible, à cause du découpage en classes (A, B et C) et du sous-adressage.
- A cette époque, pour une organisation donnée :
  - Une adresse de classe A, c'était trop
  - Une adresse de classe C, ce n'était pas confortable même si l'entreprise ne comptait que 50 hôtes (A cause la forte croissance du nombre d'ordinateurs)
  - En conclusion, une adresse de classe B, c'était bien mieux.

En attendant l'achèvement et le déploiement d'IPv6 avec ses adresses sur 16 octets, il a fallu trouver une solution temporaire: *Le sur adressage ou adressage hors-classe (CIDR)*

Adresse sans classe -CIDR

Idée générale

Une entreprise désire une adresse de classe B (notamment pour faire du sous-adressage sur le 3ème octet).

- **Problème :** plus d'adresse de classe B disponible !!?
- **Solution :** Au lieu d'une seule adresse de classe B → prendre 256 adresses de classe C
- **Nouveau problème :** ces 256 adresses génèrent 256 entrées dans les tables de routage d'Internet pour cette seule entreprise.
- **Solution :**
  - Les adresses attribuées doivent se suivre (**être contiguës**), débuter à une puissance de 2 et former un bloc d'une puissance de 2 adresses.
  - Le 3ème octet n'étant plus significatif, les 256 entrées peuvent se résumer en la seule entrée de masque 255.255.0.0
  - **En notation CIDR**, cette entrée s'écrit par ex: **xxx.xxx.0.0/16**

Adresse sans classe -CIDR

Intérêts :

- Optimiser (réduire) les tables de routage!
  - Agrégation des routes
- Éviter le gâchis (le gaspillage) d'adresses IP

Translation d'adresses – NAT
- Network Address Translation -

Pénurie d'adresses IP

- Si le CIDR a permis de régler en partie le problème, l'espace d'adressage IPv4 demeure insuffisant !
- La pénurie d'adresses IPv4 s'est traduite par la situation suivante:
  « ***Il n'est plus possible d'attribuer une adresse IP ''routable'' a chaque station connectée à Internet***. »
- Autrement dit:
  «***Une organisation (entreprise/particulier,…) qui possède un certain nombre m de stations ayant besoin d'un accès Internet n'obtient généralement qu'un petit nombre n d'adresses IP dites publiques***
  Où : n est bien plus petit que m (et peut même valoir 1 !) »
- En attendant le déploiement d'IPv6, la technique de traduction d'adresse **NAT** a été développé pour permettre a ces ***m*** stations d'avoir accès a Internet.

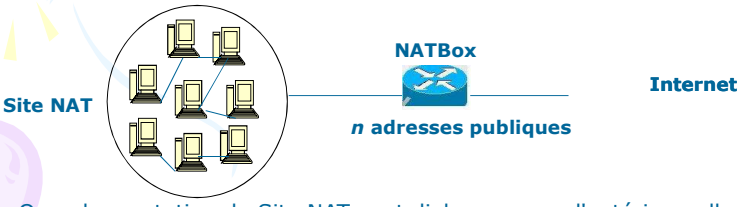
Translation d'adresses – NAT

Principe de la traduction d'adresse

Permettre à n adresses publiques d'être partagées par un grand nombre m de stations (*périphériques réseau****).***

Pour cela :

- Il faut placer une **NATBox** qui doit être le seul point de passage entre le Site NAT (réseau de l'organisation) et le WAN (Internet)
- La **NATBox** est la seule qui possède et gère les ***n*** adresses publiques

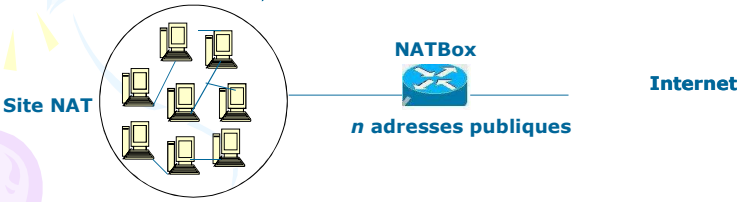


Quand une station du Site NAT veut dialoguer avec l'extérieur, elle passe par la **NATBox** qui utilisera (temporairement) l'une des n adresses publiques

Translation d'adresses – NAT

Précisions

- une **NATBox** est «typiquement» un routeur avec les fonctionnalités NAT (***mais peut être un hôte quelconque avec les fonctionnalité NAT***).
- Les stations du Site **NAT** n'ont pas connaissance des adresses publiques de la **NATBox** et ne les utilisent pas
- Mais ont des adresses privées qu'il est fortement conseillé de prendre dans les plages définies par la [RFC 1918]:
  - 10.0.0.0/8 ⟹ 16 777 216 adresses (de 10.0.0.0 a 10.255.255.255)
  - 172.16.0.0/12 ⟹ 1 048 576 adresses (de 172.16.0.0 a 172.31.255.255)
  - 192.168.0.0/16 ⟹ 65 536 adresses (de 192.168.0.0 a 192.168.255.255)



*Pour les stations de l'Internet , seules les **n** adresses de la **NATBox** existent et le Site NAT avec ses adresses privées est invisible.*

Translation d'adresses – NAT

Précisions (suite)

- A l'intérieur du Site NAT, les stations communiquent entre elles en utilisant leurs adresses privées
- Sans le NAT, un message envoyé a l'extérieur ne pourrait avoir de réponse car les adresses privées ne sont pas routables dans le WAN
- La **NATBox** doit traduire (remplacer) dans un tel message, l'adresse privée par une adresse publique, et inversement pour la réponse

Sur un routeur CISCO, on définit les adresses publiques à utiliser pour la traduction (dynamique) dans un pool.

Exemple :

ip nat pool adrpub 82.3.4.6 82.3.4.10 netmask 255.255.255.0

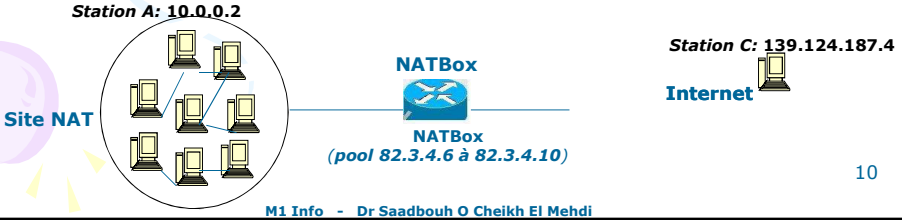
définit un pool de 5 adresses publiques nommé adrpub

Translation d'adresses – NAT

Fonctionnement

A (10.0.0.2) veut discuter avec la station externe **C** (139.124.187.4) :

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



Translation d'adresses – NAT

NAT statique

- A chaque adresse privée est associée de manière statique une adresse publique
- Une table de correspondance statiquement définie par un administrateur réseau
- Correspondance bijective
- Activation sur un routeur Cisco :
  - # ***ip nat inside source static 15.1.3.1 92.7.4.10***
  - associe statiquement l'adresse privée 15.1.3.1 et l'adresse publique 92.7.4.10. Cette association est permanente.
- **Ne règle pas le problème de pénurie d'adresses IP !!**

NAT dynamique

- La traduction d'une adresse source IPV4 privée est effectuée vers une adresse source IPV4 publique qui est prise dans un bloc d'adresses publiques disponibles.
- L'adresse publique utilisée n'est donc pas toujours la même

Translation d'adresses et de ports – NAPT

Network **A**ddress **P**ort **T**ranslation

Caractéristiques!

- Le NAT limite l'accès simultané à l'extérieur (Internet) à ***n*** stations si l'on dispose de ***n*** adresses publiques!!? (Si n=1 !!!!!?)
- Le NAPT, en plus de traduire l'adresse IP à la volée, attribue également un numéro de port différent.
  - Ce dispositif autorise l'usage simultané d'une même adresse IP publique par des milliers d'hôtes du réseau privé.
- Le NAPT est normalisé pour fonctionner avec des datagrammes IP contenant des messages ICMP, UDP ou TCP

Le NAPT est la variante la plus utilisée du NAT

Tous les routeurs modernes ont les fonctions de translation d'adresses et de ports incluses dans leurs fonctionnalités standards

Translation d'adresses – NAT

Avantages du NAT

- Économiser le nombre d'adresses IP publiques
- Simplifier la gestion du réseau en laissant l'administrateur libre d'adopter le plan d'adressage interne qu'il souhaite
- Sécurité **:** les terminaux disposent en effet d'une protection supplémentaire, puisqu'ils ne sont pas directement adressables de l'extérieur
  - La passerelle NAT représente un passage obligé pour tous les flux
  - L'administrateur peut concentrer les mécanismes de sécurisation à un point de contrôle unique et centralisé
  - Souvent, les boîtiers NAT sont couplés avec des pare-feu filtrant les flux.

Translation d'adresses – NAT

Inconvénients du NAT

1. **Protocoles sensible au NAT**

Le problème le plus important concerne les protocoles dits «sensibles » au NAT.

- Protocoles incluant des adresses IP dans la partie applicative
  - Protocoles de partage de fichiers tels que **FTP**
  - Protocoles de signalisation utilisés pour les échanges multimédias

2. **Sécurité avec le NAT**

le NAT modifie les paquets IP et cela a pour conséquence directe de **casser tout contrôle d'intégrité** au niveau IP et même aux niveaux supérieurs (puisque TCP par Ex inclut les adresses dans ses checksums!)

- La passerelle NAT doit recalculer les codes de contrôle et remplacer les originaux afin que les paquets restent valides et ne soient pas considérés par le destinataire comme corrompus.
- **Mais**, si l'émetteur crypte ses flux avec une couche IPsec, il devient impossible pour la passerelle NAT d'accéder aux en-têtes TCP des paquets