

NAT, DHCP

1

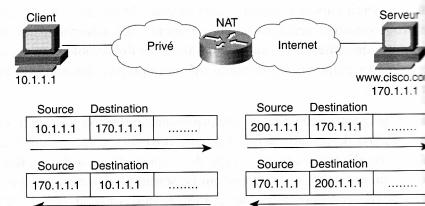
NAT

- Le NAT a été proposé en 1994 sous la RFC 1631 comme solution à court terme face au manque d'adresses IP.
 - Son objectif principal était de permettre aux adresses IP d'être partagées par un grand nombre de périphériques réseau. En une dizaine d'années d'existence, il a donné le temps nécessaire pour concevoir le nouveau protocole d'adressage IPv6 et, aujourd'hui, le début de son déploiement.
-

2

Définition: NAT

- Le NAT est défini dans la RFC 1631. Le NAT permet d'utiliser des adresses n'ayant pas de signification globale (par exemple des adresses privées définies dans la RFC 1918, non routables) pour se connecter à travers l'Internet en traduisant celles-ci en adresses globales routables.



- Le NAT permet aussi de fournir une solution élégante de renumérotation pour les organisations qui changent de fournisseur de service ou qui migrent vers le CIDR

3

La portée du NAT

- On peut utiliser le NAT dans différents cas :
 - On dispose d'une multitude d'hôtes adressés de manière privée et on a une seule ou quelques adresses IP globales (publiques).
 - Le NAT est configuré sur un routeur en bordure d'un réseau d'extrémité, étant identifié comme étant le côté interne (**inside**), qui connecte un réseau public comme l'Internet, identifié comme étant le côté externe (**outside**).
 - Le NAT traduit les adresses locales internes en une adresse globale unique avant d'envoyer les paquets vers le réseau externe.

4

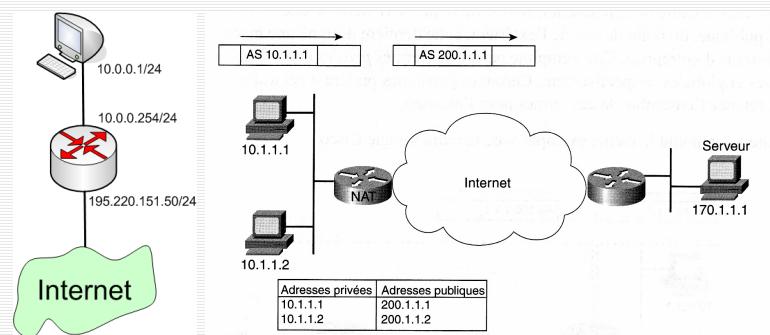
La portée du NAT

- On doit changer des adresses internes. Au lieu de les changer, on les traduit par du NAT.
- On veut rendre accessible des hôtes qui sont localement et globalement dans le même adressage, autrement dit on permet une connectivité d'adresses qui se chevauchent (**overlapping**) de part et d'autre du routeur NAT.
- On peut utiliser également le NAT pour distribuer la charge TCP vers un hôte virtuel qui répond à la place de plusieurs serveurs réels selon un principe de type round-robin.
- Il contribue à améliorer la sécurité des réseaux internes puisqu'il les cache.

5

La traduction NAT statique

- La traduction statique fonctionne à l'aide d'une table statique, adresses associées statiquement.



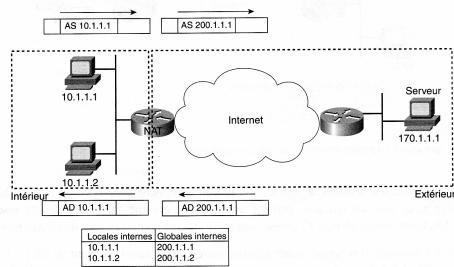
- A chaque adresse privée correspond à une adresse publique

6

Traduction NAT statique

□ La terminologie de CISCO

- Cisco emploie les termes ***inside local address*** pour spécifier le côté interne et ***inside global address*** pour spécifier le côté externe.
- Pour bien comprendre: locale/global privée/publique

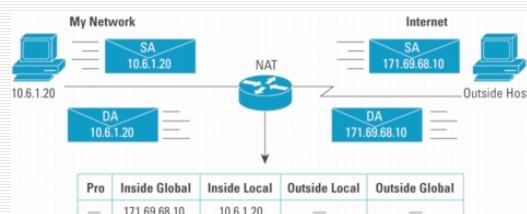


7

Traduction NAT statique



An IP address is either local or global
Local IP addresses are seen in the inside network
Global IP addresses are seen in the Outside network



10.6.1.20 is inside local address
171.69.68.10 is inside global address

8

Traduction NAT statique

- La plupart des applications NAT ne changent que les adresses internes. Par conséquent les tables concernées montrent les **adresses locales et globales internes**.
- Dans certaines configurations il est possible de changer une adresse désignant un hôte externe. Dans ce cas, les adresses seront qualifiées de **globales externes et locales internes**.

9

La traduction NAT statique

Concrètement, on trouvera dans les tables NAT jusqu'à quatre types d'adresses :

Inside local address - L'adresse IP assignée à un hôte à l'intérieur d'un réseau d'extrémité. Il s'agit probablement d'une adresse privée, non routable.

Inside global address - La ou les adresses IP publiques qui représentent les adresses IP locales internes, les adresses IP routables du routeur NAT.

Outside local address - L'adresse IP d'un hôte telle qu'elle apparaît aux hôtes d'un réseau interne. Il ne s'agit pas nécessairement d'une adresse légitime routable.

Outside global address - L'adresse IP réelle routable d'un hôte qui se situe à l'extérieur du réseau du routeur NAT.

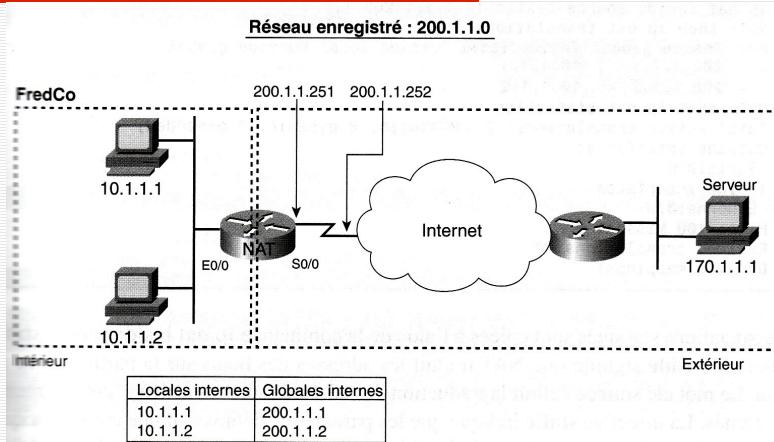
10

Traduction NAT statique

- Définition du NAT
 - (config)#ip nat inside source static local_inside_ip global_inside_ip
- Définition des interfaces Inside/Outside
 - (config)#interface type number
 - (config-if)#ip nat inside
 - (config)# interface type number
 - (config-if)#ip nat outside

11

Exemple traduction NAT statique



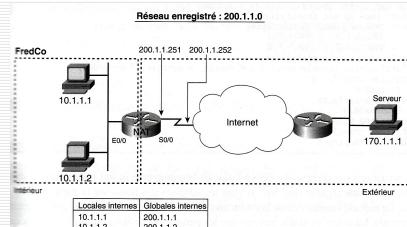
12

Exemple traduction NAT statique

```

interface Ethernet 0/0
ip address 10.1.1.3 255.255.255.0
ip nat inside
!
interface Serial 0/0
ip address 200.1.1.251 255.255.255.0
ip nat outside
!
ip nat inside source static 10.1.1.2 200.1.1.2
ip nat inside source static 10.1.1.1 200.1.1.1

```



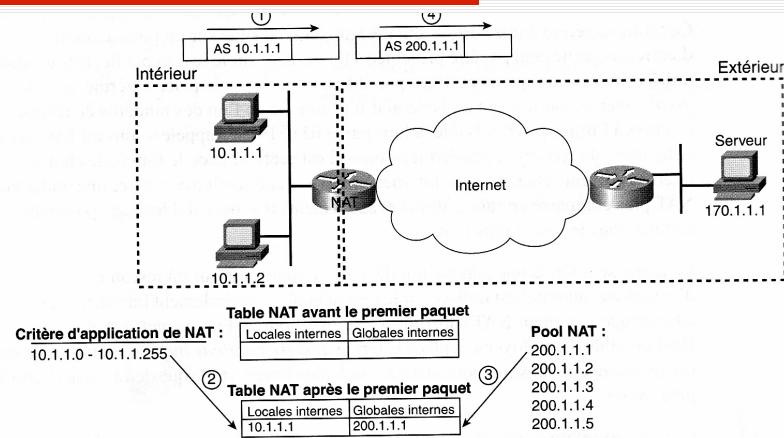
13

Traduction NAT dynamique

- La traduction NAT dynamique ressemble à la traduction statique car elle crée une relation de cardinalité (1adr globale correspond une adresse globale).
- La différence réside dans le fait que la substitution se fait dynamiquement.
- Cette configuration définit un pool d'adresses globales internes et des critères pour désigner l'ensemble des adresses locales internes qui doivent être remplacées.

14

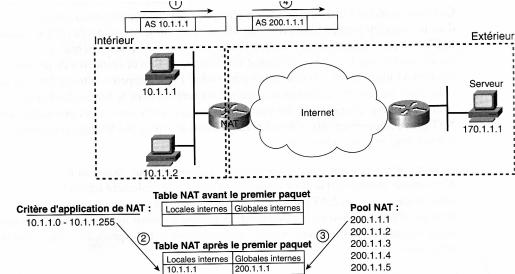
Traduction NAT dynamique



15

Traduction NAT dynamique

- L'hôte 10.1.1.1 envoie son paquet au serveur 170.1.1.1
- Lors de l'arrivée du paquet sur l'interface interne du routeur NAT, celui ci applique la traduction définie
- Le routeur doit donc allouer une adresse publique à partir du pool d'adresses globales internes disponibles
- Le routeur remplace alors l'adresse source inscrite par l'adresse prélevée dans le pool et transmet le paquet sur l'interface adéquate.



16

Traduction NAT dynamique

- L'entrée dynamique demeure dans la table tant que du trafic est échangé occasionnellement entre ces deux adresses.
- Vous pouvez configurer un délai d'expiration (timeout) qui indique la durée pendant laquelle le routeur doit attendre en l'absence d'échanges avant de supprimer l'entrée de la table.
 - `ip nat translation timeout <seconds>`
- Vous pouvez aussi supprimer la table manuellement par
 - `clear ip nat translation *`

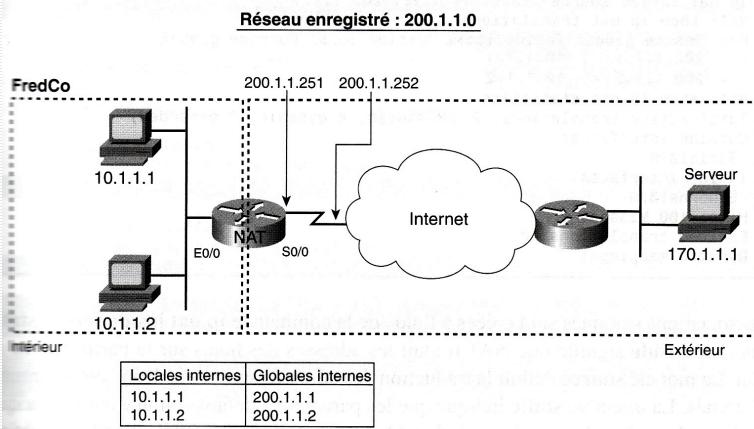
17

Traduction NAT dynamique

- Adresses locales soumises au NAT
 - `(config)#access-list access-list_number permit source_ip wildcard_mask`
- Pool d'adresses globales
 - `(config)#ip nat pool name start_ip end_ip`
- Définition du NAT
 - `(config)#ip nat inside source list access-list_number pool name`
- Définition des interfaces Inside/Outside
 - `(config)#interface type number`
 - `(config-if)#ip nat inside`
 - `(config)# interface type number`
 - ~~`(config-if)#ip nat outside`~~

18

Exemple traduction NAT dynamique



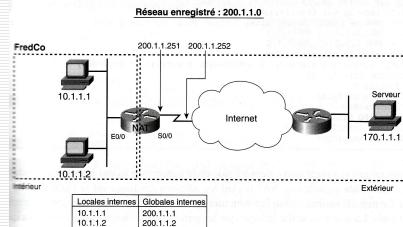
19

Exemple traduction NAT dynamique

```

interface Ethernet 0/0
ip address 10.1.1.3 255.255.255.0
ip nat inside
!
interface Serial 0/0
ip address 200.1.1.251 255.255.255.0
ip nat outside
!
ip nat pool monpool 200.1.1.1 200.1.1.2 netmask 255.255.255.252
ip nat inside source list 1 pool monpool
!
access-list 1 permit host 10.1.1.2
access-list 1 permit host 10.1.1.1

```



20

Autre exemple NAT dynamique

```
Router(config)#ip nat pool fred prefix-length 24
Router(config-ipnat-pool)#address 171.69.233.225 171.69.233.226
Router(config-ipnat-pool)#address 171.69.233.228 171.69.233.238
```

Créé un pool d'adresses de 171.69.233.225 à 171.69.233.238
en excluant le 171.69.233.227

21

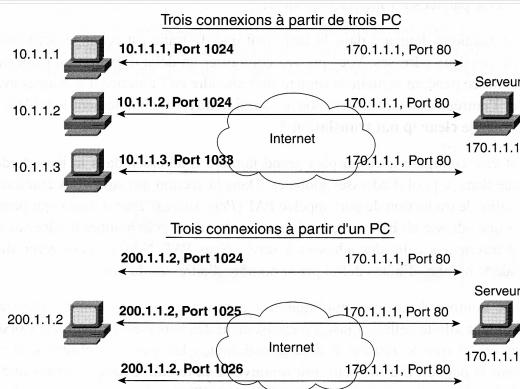
Traduction étendue avec PAT (overloading)

- Dans la traduction NAT dynamique, il faut avoir suffisamment d'adresses publiques pour assurer une bonne connectivité des postes clients (adr privées). Dans l'absolu, un nombre identique.
- L'overloading, ou traduction PAT, permet à NAT de s'adapter à l'augmentation des clients Internet d'une entreprise.

22

Overloading (PAT)

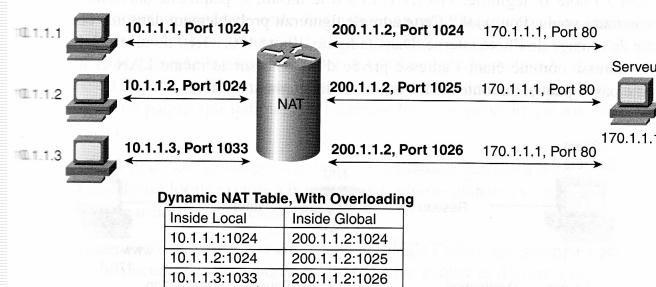
- 1er cas:
 - Un réseau interne avec 3 hôtes
- 2ème cas:
 - Un hôte avec 3 connexions
- NAT tire parti du fait que le serveur ne fait pas la différence.



23

Overloading (PAT)

- Pour servir une grande quantité d'adresses locales internes à l'aide d'une ou quelques adresses globales internes enregistrées, la traduction étendue PAT emploie les ports en plus de l'adresse



24

Overloading (PAT) avec 1 seule adresse publique

□ Adresses locales soumises au NAT

- (config)#access-list access-list_number
permit source_ip wildcard_mask

□ Définition du NAT

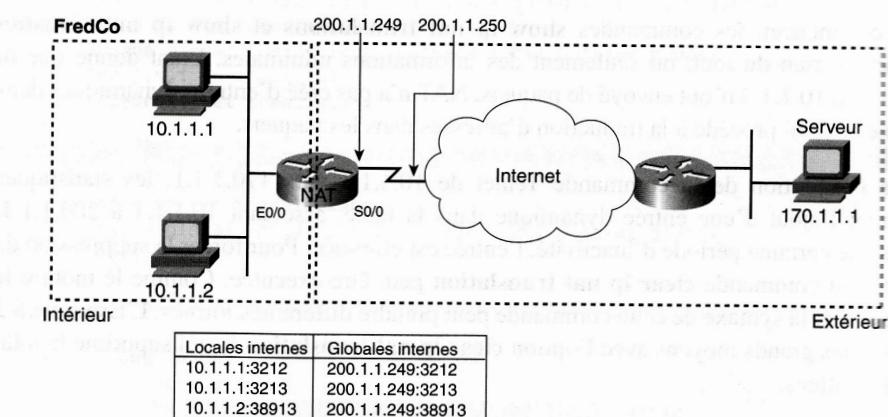
- (config)#ip nat inside source list
access-list_number interface type number
overload

□ Définition des interfaces Inside/Outside

- (config)#interface type number
- (config-if)#ip nat inside
- (config)# interface type number
- (config-if)~~#ip nat outside~~

25

Exemple PAT Overloading



26

Exemple PAT Overloading

```

interface Ethernet 0/0
ip address 10.1.1.3 255.255.255.0
ip nat inside
!
interface Serial 0/0
ip address 200.1.1.251 255.255.255.0
ip nat outside
!
ip nat inside source list 1 interface Serial 0/0 overload
!
access-list 1 permit host 10.1.1.2
access-list 1 permit host 10.1.1.1

```

show ip nat translations pour afficher les tables

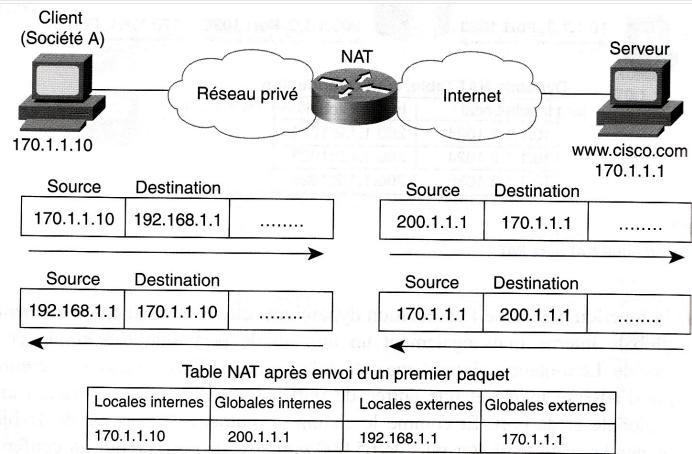
27

Traduction avec chevauchement d'adresses (overlapping)

- La traduction dynamique peut également être utilisée dans le cas où un réseau interne ne recourt pas aux adresses réservées à l'usage privé telles que définies dans la RFC 1918 mais à des adresses publiques déjà enregistrées par une autre société.
- **Exemple:** Si une société se trouve malencontreusement dans cette situation ou elle utilise des adresses déjà enregistrées et utilisées sur le réseau public et que les hôtes internes se connectent à Internet, la traduction NAT apporte une solution à ce problème.
- Dans ce cas, l'adresse source et destination sont remplacées.

28

Traduction avec chevauchement (overlapping)



29

Port Forwarding

- Le **port forwarding** consiste à rediriger un paquet vers une machine précise en fonction du port de destination de ce paquet.
- Ainsi, lorsque l'on n'a qu'une seule adresse publique avec plusieurs machines derrière en adressage privé. On peut initialiser une connexion de l'extérieur vers l'une de ses machines (une seule par port TCP/UDP).
- Prenons l'exemple précédent et disons que la machine 10.0.0.1 possède un serveur FTP. Maintenant, on configure le routeur pour qu'il redirige les connexions arrivant sur le port 21 vers la machine 10.0.0.1. Et hop, on rend notre machine ayant une adresse privée disponible depuis l'extérieur !!

Ainsi, le port forwarding nous a permis de rendre nos machines du réseau local joignables d'Internet, même si l'on ne possède qu'une seule adresse IP publique !!

30

Port forwarding

- `ip nat inside source static { tcp | udp } <localaddr> <localport> <globaladdr> <globalport>`
- **Exemple:**
 - `ip nat inside source static tcp 192.168.10.1 25 171.69.232.209 25`
- Dans cet exemple, les connexions initiées depuis l'extérieur sur le port 25 (SMTP) sont envoyées sur la machine 192.168.10.1 sur le port 25

31

Rappel des commandes

Tableau 8.5 : Commandes de configuration de NAT

Commande	Mode de configuration
<code>ip nat {inside outside}</code>	Sous-commande d'interface
<code>ip nat inside source [list {num-liste-accès nom-liste-accès}] [route-map nom] {interface type num pool nom-pool} [overload]</code>	Commande globale
<code>ip nat inside destination list {num-liste-accès nom-liste-accès} [pool nom]</code>	Commande globale
<code>ip nat outside source [list {num-liste-accès nom-liste-accès}] [route-map nom] pool nom-pool [add-route]</code>	Commande globale
<code>ip nat pool nom ip-début ip-fin {netmask masque prefix-length long-préfixe} [type rotary]</code>	Commande globale

Tableau 8.6 : Commandes exec pour NAT

Commande	Mode de configuration
<code>show ip nat statistics</code>	Affiche les compteurs pour les paquets et les entrées de la table NAT ainsi que des informations de configuration basiques.
<code>show ip nat translations [verbose]</code>	Affiche la table NAT.
<code>clear ip nat translation [* {inside ip-globale ip-locale} [outside ip-locale ip-globale]]</code>	Supprime certaines ou la totalité des entrées dynamiques de la table NAT selon les paramètres utilisés.
<code>clear ip nat translation protocol inside ip-globale port-global ip-locale port-local [outside ip-locale ip-globale]</code>	Supprime certaines des entrées dynamiques de la table NAT, selon les paramètres utilisés.
<code>debug ip nat</code>	Produit un message de journal décrivant chaque paquet dont l'adresse IP a été traduite.

32

NAT et FTP

- En quoi une implémentation NAT peut-elle poser problème à une architecture NAT ?
- Pour du trafic FTP, on diagnostiquera la problématique par une connexion établie sans possibilité d'exécuter les commandes FTP, notamment de listing (LS).
- La problématique peut se poser soit du côté client, soit du côté serveur

33

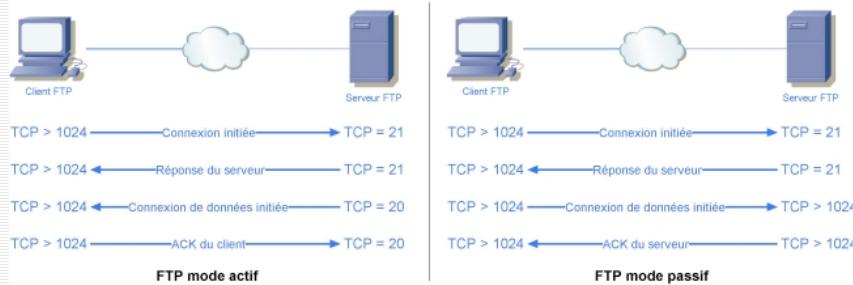
NAT et FTP

- Problématique côté client
 - Le trafic FTP qui vise à négocier les ports de transfert des données du client vers le serveur est initié par le serveur (port d'origine TCP 20) à destination d'un port TCP supérieur à 1024 vers le client. Ce mode FTP appelé mode actif est celui qui est supporté par défaut par les serveur FTP

34

NAT et FTP: côté client

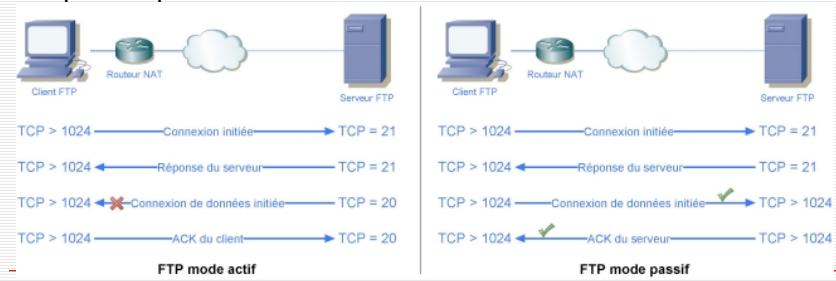
- Si le client est protégé par un routeur NAT dynamique, ce trafic ne sera pas traduit car il ne fait pas partie d'une règle NAT configurée pour un trafic initié de l'intérieur. Alors que l'établissement d'une connexion de contrôle FTP sera possible, le transfert de données ne le sera pas. A moins de réaliser une traduction statique de l'adresse locale interne vers l'adresse globale interne, il n'y a pas de solution NAT



35

NAT et FTP: côté client

- La solution consiste à établir une connexion FTP à partir du client en mode passif. Dans ce mode, le client initie la négociation du port que le serveur propose. Vu qu'ici le trafic est initié derrière le routeur NAT, le NAT en tant que tel ne pose plus de problème. Faut-il encore que le serveur supporte ce mode, ce qui est de plus en plus courant



36

NAT et FTP

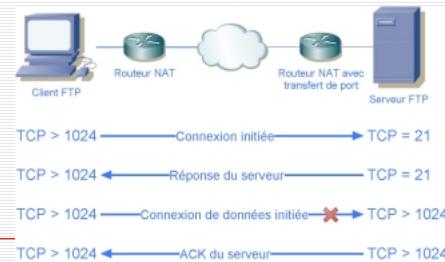
□ Problématique côté serveur

- A côté du premier problème côté client, on peut rencontrer un problème cumulatif côté serveur. Il faut supposer que le serveur est hébergé derrière, lui aussi, un routeur NAT configuré avec un transfert de ports. Si le client initie lui-même le transfert de données vers des ports supérieurs à 1024 à destination du serveur, comment le routeur NAT du serveur peut-il traduire le trafic entrant à destination de ces ports qui ne font pas l'objet d'une configuration spécifique ?

37

NAT et FTP : côté serveur

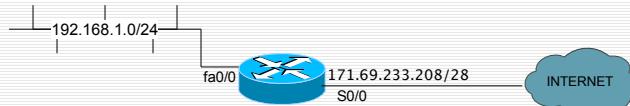
- Heureusement les passerelles sont aujourd'hui capable de suivre le trafic FTP qui nécessite une inspection du trafic FTP lui-même au niveau de la couche applicative.
- Sur les passerelles Linux, il faudra par exemple activer et configurer les modules **`ip_conntrack_ftp`** et **`ip_nat_ftp`** du noyau. Si un routeur Cisco avec un IOS récent supportera cette fonctionnalité nativement pour le trafic initié sur le port TCP 21, **il n'en sera pas de même pour les services FTP écoutant sur un autre port que le port légal.**



38

Exercices 1

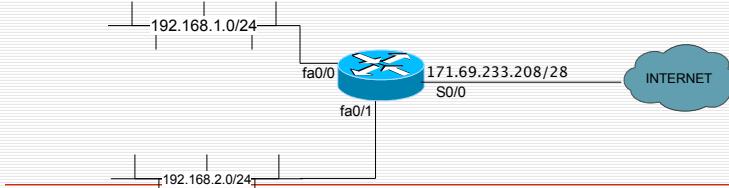
- Adresses locales soumises au NAT
 - (config)#access-list access-list_number permit source_ip wildcard_mask
- Pool d'adresses globales
 - (config)#ip nat pool name start_ip end_ip
- Definition du NAT
 - (config)#ip nat inside source list access-list_number pool name
- Définition des interfaces Inside/Outside
 - (config)#interface type number
 - (config-if)#ip nat inside
 - (config)# interface type number
 - (config-if)#ip nat outside



39

Exercice 2

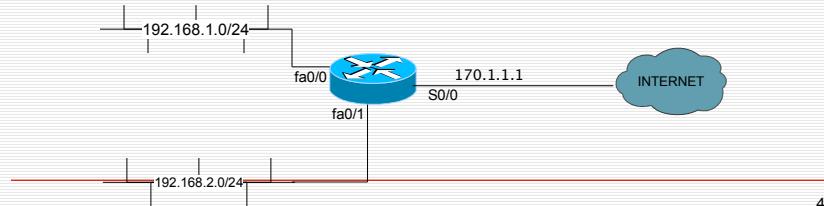
- Adresses locales soumises au NAT
 - (config)#access-list access-list_number permit source_ip wildcard_mask
- Pool d'adresses globales
 - (config)#ip nat pool name start_ip end_ip
- Definition du NAT
 - (config)#ip nat inside source list access-list_number pool name
- Définition des interfaces Inside/Outside
 - (config)#interface type number
 - (config-if)#ip nat inside
 - (config)# interface type number
 - (config-if)#ip nat outside



40

Exercice 3

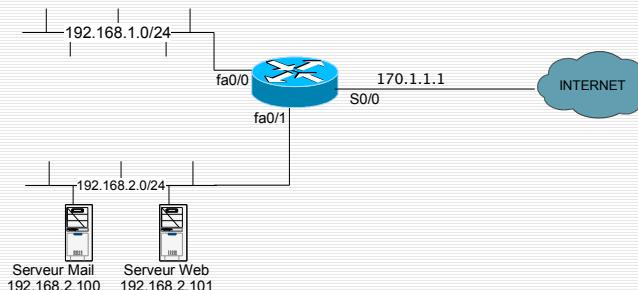
- Adresses locales soumises au NAT
 - (config)#access-list access-list_number permit source_ip wildcard_mask
- Définition du NAT
 - (config)#ip nat inside source list access-list_number interface type number overload
- Définition des interfaces Inside/Outside
 - (config)#interface type number
 - (config-if)#ip nat inside
 - (config)# interface type number
 - (config-if)#ip nat outside



41

Exercice 4

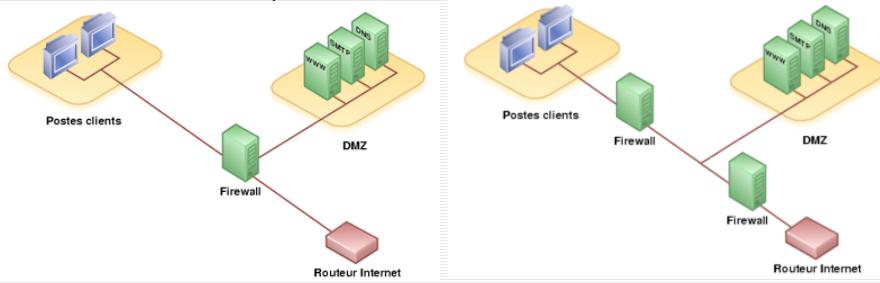
- ip nat inside source static { tcp | udp } <localaddr> <localport> <globaladdr> <globalport>



42

NAT et DMZ

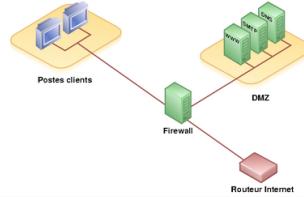
- Zone Démilitarisée
- À l'origine, la zone démilitarisée (ou DMZ) désigne la zone qui sépare la Corée du Nord de la Corée du Sud aux alentours du 38e parallèle. Elle assure que chacun des deux camps pourra apercevoir une manœuvre de l'ennemi de pénétration de la zone (et donc une volonté de guerre)



43

DMZ

- Les serveurs situés dans la DMZ sont appelés « bastions » en raison de leur position d'avant poste dans le réseau de l'entreprise.
- La politique de sécurité mise en œuvre sur la DMZ est généralement la suivante :
 - Traffic du réseau externe vers la DMZ autorisé ;
 - Traffic du réseau externe vers le réseau interne interdit ;
 - Traffic du réseau interne vers la DMZ autorisé ;
 - Traffic du réseau interne vers le réseau externe autorisé ;
 - Traffic de la DMZ vers le réseau interne interdit ;
 - Traffic de la DMZ vers le réseau externe refusé.



44

Pare feux

- Statefull (CBAC: Context Base Access List)
- Stateless (ACL)

45

DHCP

- La configuration d'un serveur DHCP permet :
 - D'assigner des adresses privées dans des groupes prédéfinis
 - De fournir plus de trente paramètres de configuration
 - De définir spécifiquement les adresses MAC afin de recevoir les adresses IP.

46

DHCP: Avant ?

BOOTP	DHCP
Mappages statiques	Mappages dynamiques
Assignation permanente	Bail
Ne prend en charge que quatre paramètres de configuration	Prend en charge plus de 30 paramètres de configuration

47

DHCP

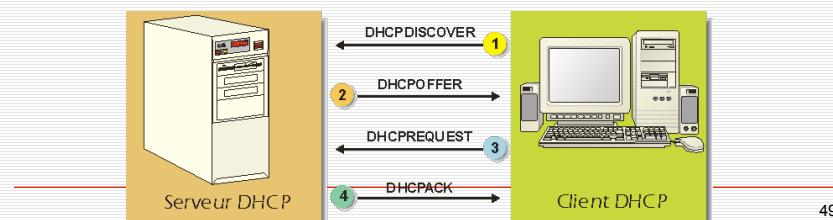
- DHCP s'appuie sur le protocole de transport UDP. Le client envoie des messages au serveur sur le port 67 et le serveur envoie des messages aux clients sur le port 68. Trois mécanismes existent afin d'attribuer une adresse IP :
 - L'allocation automatique attribue une adresse IP permanente à un client
 - L'allocation manuelle transfère une adresse IP attribuée par l'administrateur
 - L'allocation dynamique concède une adresse IP pendant une durée limitée (bail).

48

DHCP: comment?

- Les choses se passent avec le peu de moyens dont vous disposez:

- Votre "MAC Address" que vous ne perdez jamais, puisqu'elle est écrite "en dur" dans votre interface Ethernet.
- Le "Broadcast" ou "Diffusion" qui permet d'envoyer des trames à toutes les machines du réseau physique.



49

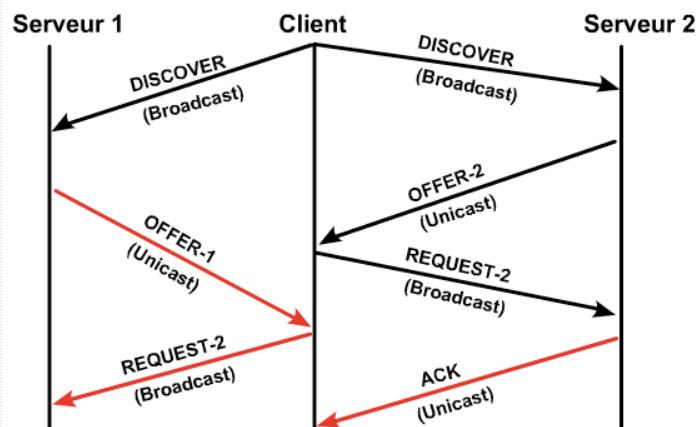
DHCP: 4 messages de base

1. Lorsque le client DHCP démarre, il envoie donc une trame "**DHCPDISCOVER**", destinée à trouver un serveur DHCP. Cette trame est un "broadcast", donc envoyé à l'adresse 255.255.255.255. N'ayant pas encore d'adresse IP, il adopte provisoirement l'adresse 0.0.0.0. Comme ce n'est pas avec cette adresse que le DHCP va l'identifier, il fournit aussi sa "MAC Address".
2. Le, ou les serveurs DHCP du réseau qui vont recevoir cette trame vont se sentir concernés et répondre par un "**DHCPOFFER**". Cette trame contient une proposition de bail et la "MAC Address" du client, avec également l'adresse IP du serveur. Tous les DHCP répondent et le client normalement accepte la première réponse venue. Le "DHCPOFFER" sera un broadcast (Ethernet) ou non, suivant le serveur DHCP utilisé. Nous y reviendrons plus en détail sur l'exemple.
3. Le client répond alors par un **DHCPREQUEST** à tous les serveurs (donc toujours en "Broadcast") pour indiquer quelle offre il accepte.
4. Le serveur DHCP Concerné répond définitivement par un **DHCPACK** qui constitue une confirmation du bail. L'adresse du client est alors marquée comme utilisée et ne sera plus proposée à un autre client pour toute la durée du bail.



50

DHCP: Plusieurs offres



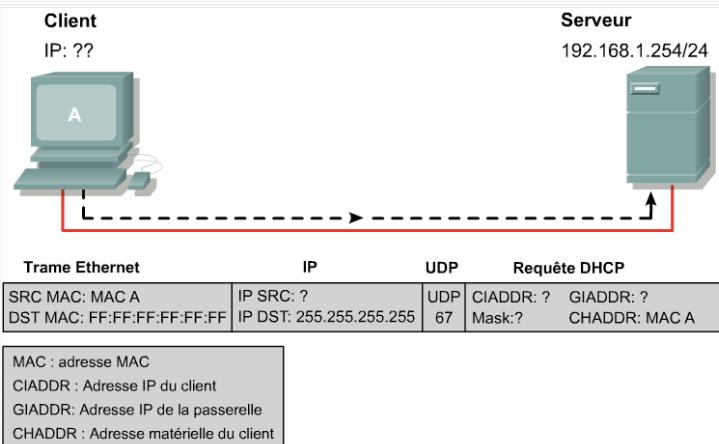
51

DHCP: 3 messages de plus...

- Si le client détecte que l'adresse est en cours d'utilisation sur le segment local, il envoie un message DHCPDECLINE et le processus recommence. Si le client a reçu un DHCPNACK du serveur après avoir envoyé le DHCPREQUEST, il recommence tout le processus.
- Si le client n'a plus besoin de l'adresse IP, il envoie un message DHCPRELEASE au serveur

52

DHCP: Trame



53

DHCP: Le bail

- Dans le bail, il y a non seulement une adresse IP pour le client, avec une durée de validité, mais également d'autres informations de configuration comme:
 - L'adresse d'un ou de plusieurs DNS (Résolution de noms)
 - L'adresse de la passerelle par défaut (pour sortir du réseau où le DHCP vous a installé).
 - L'adresse du serveur DHCP (nous allons voir pourquoi).
 - ...
- Lorsque le bail arrive à environ la moitié de son temps de vie, le client va essayer de renouveler ce bail, cette fois-ci en s'adressant directement au serveur qui le lui a attribué. Il n'y aura alors qu'un DHCPREQUEST et un DHCPACK.
- Si, au bout des 7/8e de la durée de vie du bail en cours, ce dernier n'a pu être renouvelé, le client essaiera d'obtenir un nouveau bail auprès d'un DHCP. Il pourra alors se faire que le client change d'adresse IP en cours de session. Normalement, cette situation ne devrait pas se produire, sauf en cas de panne du DHCP.
- Dans les manuels, il est recommandé de ne pas créer de baux inutilement courts, ceci entraînant une augmentation significative du broadcast sur le réseau. Le compromis est à trouver entre la durée moyenne de connexion des utilisateurs, la réserve d'adresses IP du serveur, le nombre d'abonnés...
- En règle générale, un FAI dispose toujours de moins d'adresses que d'abonnés, parce que tous les abonnés ne se connectent pas en même temps. Une mauvaise analyse des statistiques peut alors entraîner de graves problèmes (que nous avons connus sur le câble) aux heures de pointe.

54

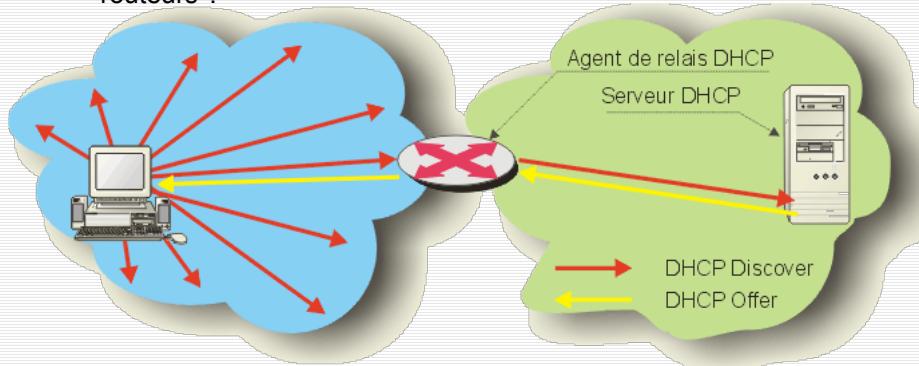
DHCP: Sniffer

No.	Time	Source	Destination	Protocol	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x6719436e
2	0.001182	192.168.0.253	192.168.0.9	ICMP	Echo (ping) request (*)
3	0.342454	192.168.0.253	192.168.0.9	DHCP	DHCP Offer - Transaction ID 0x6719436e
4	0.344405	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x6719436e
5	0.348264	192.168.0.253	192.168.0.9	DHCP	DHCP ACK - Transaction ID 0x6719436e
6	0.353014	CIS_b9:49:37	Broadcast	ARP	Who has 192.168.0.9? Tell 192.168.0.9
7	0.571241	CIS_b9:49:37	Broadcast	ARP	Who has 192.168.0.9? Tell 192.168.0.9
8	1.571441	CIS_b9:49:37	Broadcast	ARP	Who has 192.168.0.9? Tell 192.168.0.9

55

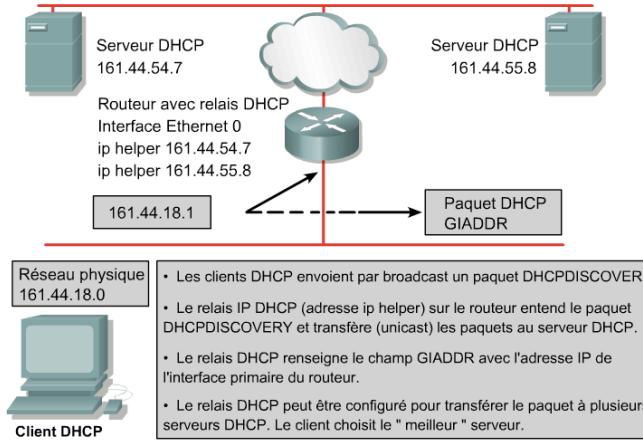
DHCP: relais

- comment la négociation peut-elle se faire, puisque, normalement, un "broadcast" n'est pas retransmis par les routeurs ?



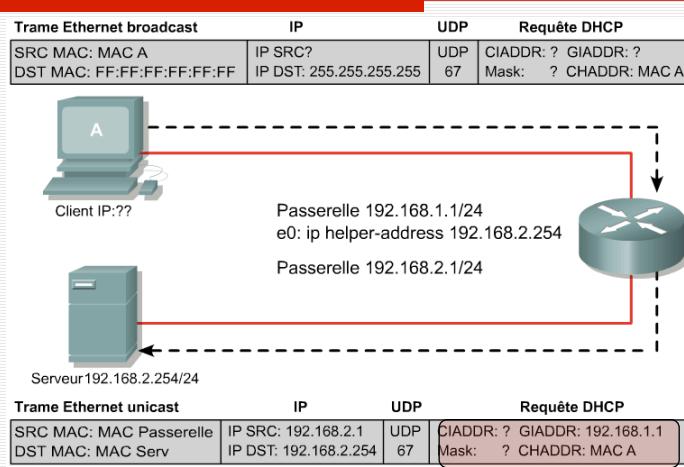
56

DHCP: relais



57

DHCP: relais



58

DHCP: Relais

Trame Ethernet unicast	IP	UDP	Réponse DHCP
SRC MAC: MAC Passerelle DST MAC: MAC A	IP SRC: 192.168.2.254 IP DST: 192.168.1.10	UDP 68	GIADDR: 192.168.1.1 CHADDR: MAC A Mask: 255.255.255.0 CIADDR: 192.168.1.10



Trame Ethernet unicast	IP	UDP	Réponse DHCP
SRC MAC: MAC Serv DST MAC: MAC Passerelle	IP SRC: 192.168.2.254 IP DST: 192.168.1.10	UDP 68	GIADDR: 192.168.1.1 CHADDR: MAC A Mask: 255.255.255.0 CIADDR: 192.168.1.10

59

DHCP: Configurations

- Pour configurer le serveur DHCP, il est nécessaire de définir un groupe d'adresses attribuables,
- puis passer en mode DHCP pour paramétriser la configuration.
- Plusieurs groupes d'adresses peuvent être configurés sur un seul serveur.
- Les commandes principales
 - « ip dhcp pool nom » crée un groupe et place le routeur en mode DHCP.
 - « network *adresse_reseau masque* » définit la plage d'adresses à octroyer.
 - « ip dhcp excluded-address *adresse* » exclut une adresse de la liste et est utilisé pour réservé des adresses statiques à certains hôtes.

60

Exemple

```
Router(config)#ip dhcp pool pool-name
Router(dhcp-config)#network network-number [mask]/prefix-length
Router(config)#ip dhcp excluded-address low-address [high-address]
Router(config)#ip dhcp excluded-address 172.16.1.1 172.16.1.10
Router(config)#ip dhcp excluded-address 172.16.1.254
```

```
Router(config)#ip dhcp pool subnet12
Router(dhcp-config)#network 172.16.12.0 255.255.255.0
Router(dhcp-config)#default-router 172.16.12.254
Router(dhcp-config)#dns-server 172.16.1.2
Router(dhcp-config)#netbios-name-server 172.16.1.3
Router(dhcp-config)#domain-name foo.com
```

61

DHCP

- « no service dhcp » / « service dhcp » désactive ou respectivement active le service dhcp.

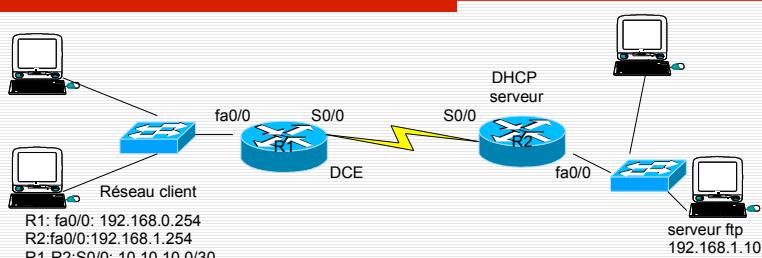
62

DHCP: Relais

- Sur l'interface réseau local du routeur
 - ip helper address
- Par défaut, la commande ip helper-address transfère les huit services UDP suivants:
 - Protocole Time
 - TACACS
 - Le protocole DNS
 - Le serveur BOOTP/DHCP
 - Le client BOOTP/DHCP
 - TFTP
 - Le service de noms NetBIOS
 - Le service de datagramme NetBIOS

63

A vous de jouer



Plages DHCP: 192.168.0.10-100
Plage DHCP: 192.168.1.100-150 à l'exception du 192.168.1.101

Empêcher l'accès au serveur ftp depuis le réseau 192.168.0.0/24

64