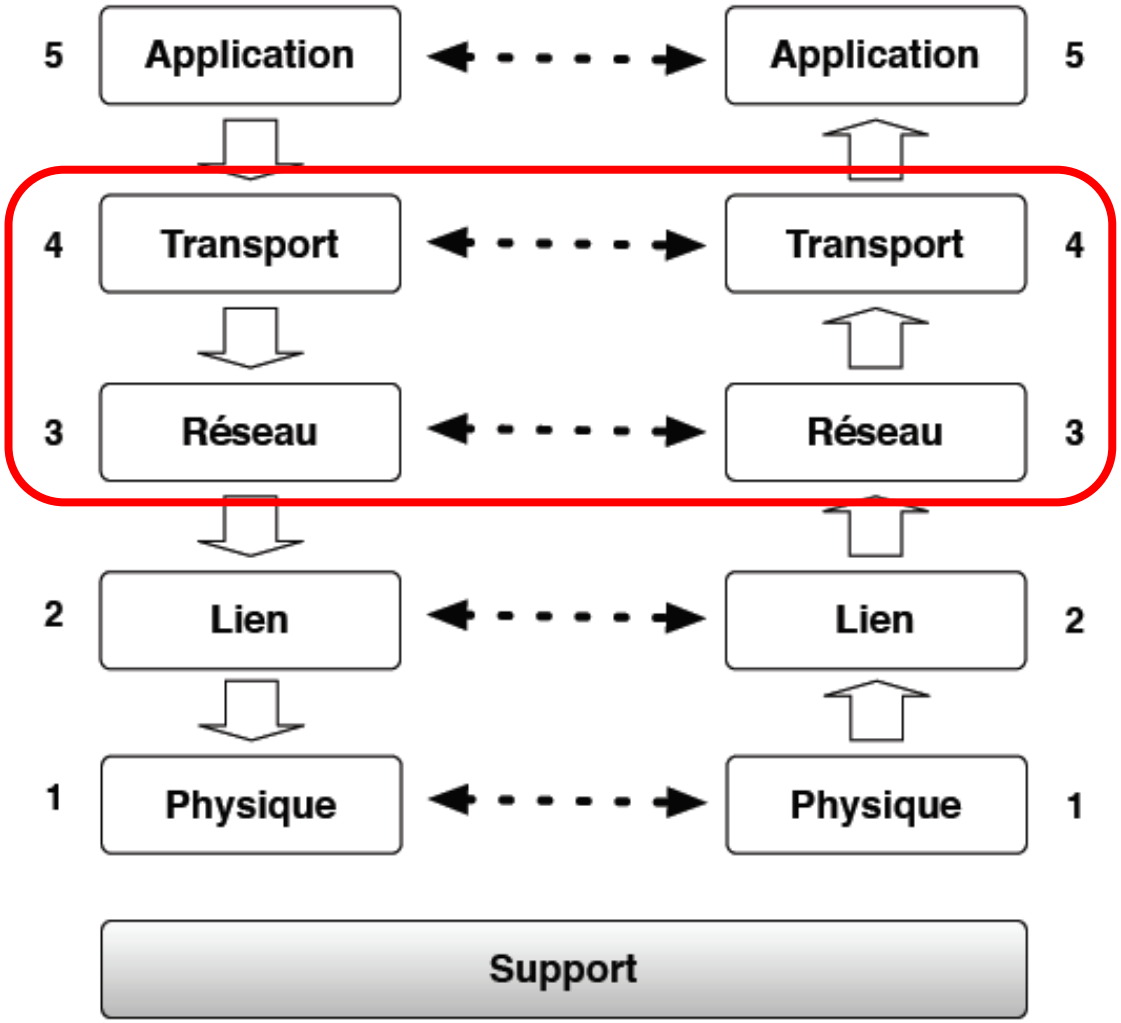
Applications en réseau

Couche application
NAT, DNS, DHCP, SMTP/POP, HTTP

Rappels



Transmet et reconstitue le fichier

Transmet et reconstitue les paquets

Transmet et reconstitue les datagrammes dans le réseau global

Transmet et reconstitue les trames sur le réseau local

Transmet et reconstitue les données sur le support physique

A retenir

- La couche réseau (IP) est responsable du
  - Routage : acheminer les paquets IP d'un émetteur vers un destinataire en se propageant d'un nœud à l'autre.
  - Adressage : les nœuds sont identifiées par une adresse IP sur 4 octets notée X.X.X.X
  - Les paquets (datagrammes) IP contiennent les adresses émetteur et destinataire.
- La couche réseau n'est pas responsable
  - D'assurer la fiabilité de la transmission: certains paquets peuvent être perdus ou dupliqués.
  - De reconnaître les différentes applications qui s'exécutent sur une machine

A retenir

- Les protocoles de routage ont pour fonction de décider sur quel lien transmettre un paquet IP.
- Chaque nœud maintient une table de routage contenant des règles de la forme
  - *<pour aller à X, passer par Y, distance d>*
- La route qu'emprunte un paquet peut être déterminée
  - Statiquement : chaque route est entrée manuellement par l'administrateur réseau.
  - Dynamiquement : les nœuds découvrent incrémentalement leurs voisins puis le reste du réseau en échangeant leur table de routage. Détecte les pannes.

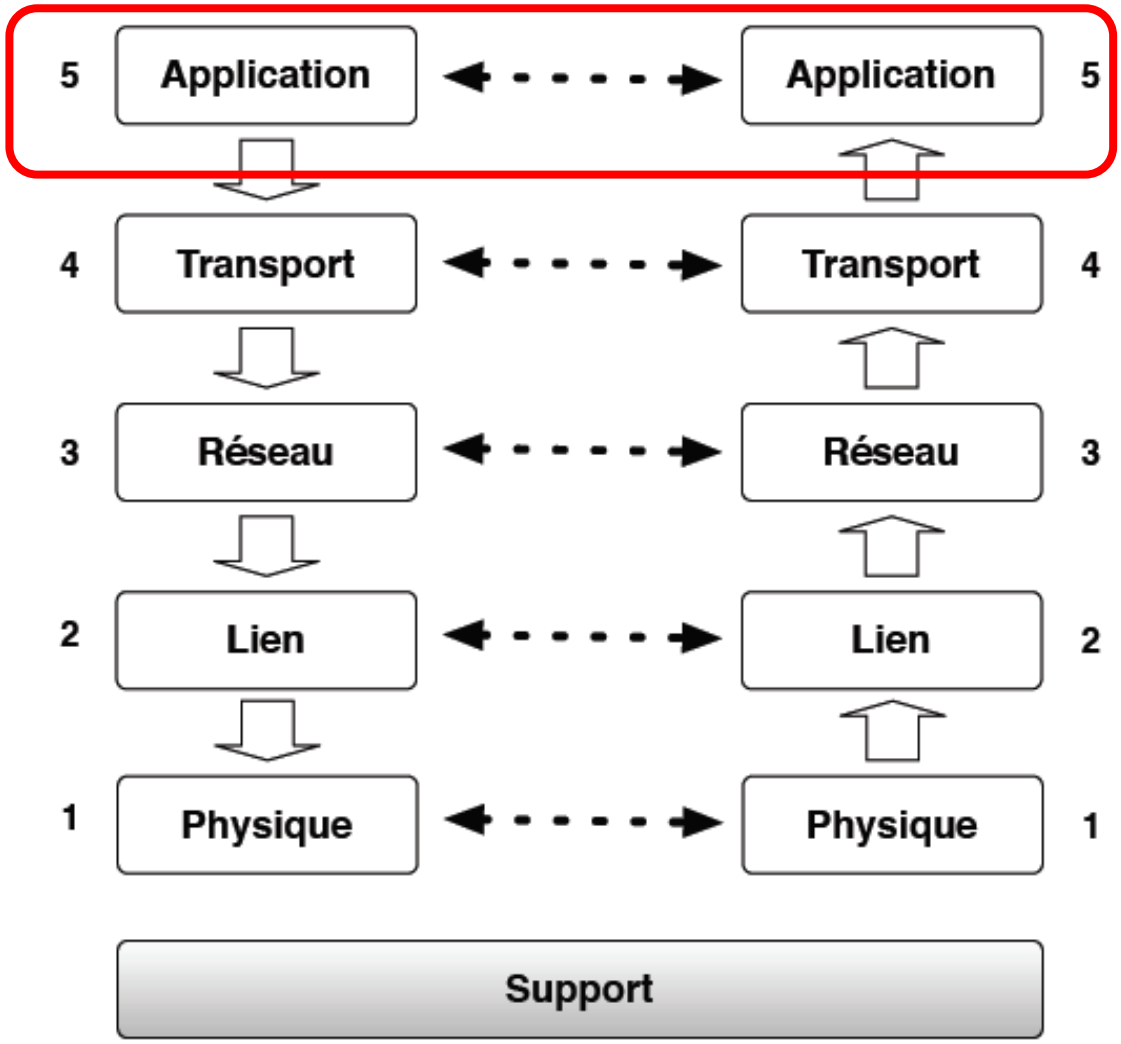
A retenir

- Les adresses IP sont des adresse logiques qui identifient des machines interconnectées via internet
- Les routeurs examinent l'adresse du destinataire pour déterminer sur quel lien transmettre le message
- Un routeur ne conserve que les adresses des réseaux dans ses tables et non de tous les hôtes.
- Il utilise le masque de réseau fourni dans le message pour déterminer sur l'adresse réseau associée au destinataire
- Localement, la passerelle peut router les paquets sur des sous-réseaux locaux via une table de routage locale qui stocke les adresses des sous-réseaux.
- Les sous-réseaux sont invisibles à l'extérieur de la passerelle.

A retenir

- La couche transport a pour fonctions:
  - L'adressage des applications via un identifiant de la forme <@Ip + port>, port entier.
    - UDP, TCP
  - La fiabilité de la communication en cas de perte de paquet ou de déséquencement via :
    - La numérotation des segments
    - L'acquittement des segments. Les segments non acquittés sont réémis et peuvent être à nouveau perdus ou bien redondants.
  - Pour limiter les erreurs, TCP tente de limiter la congestion du réseau en ajustant la cadence d'envoi des paquets aux capacités du réseau.

Plan du cours



Transmet et reconstitue le fichier

Transmet et reconstitue les paquets

Transmet et reconstitue les datagrammes dans le réseau global

Transmet et reconstitue les trames sur le réseau local

Transmet et reconstitue les données sur le support physique

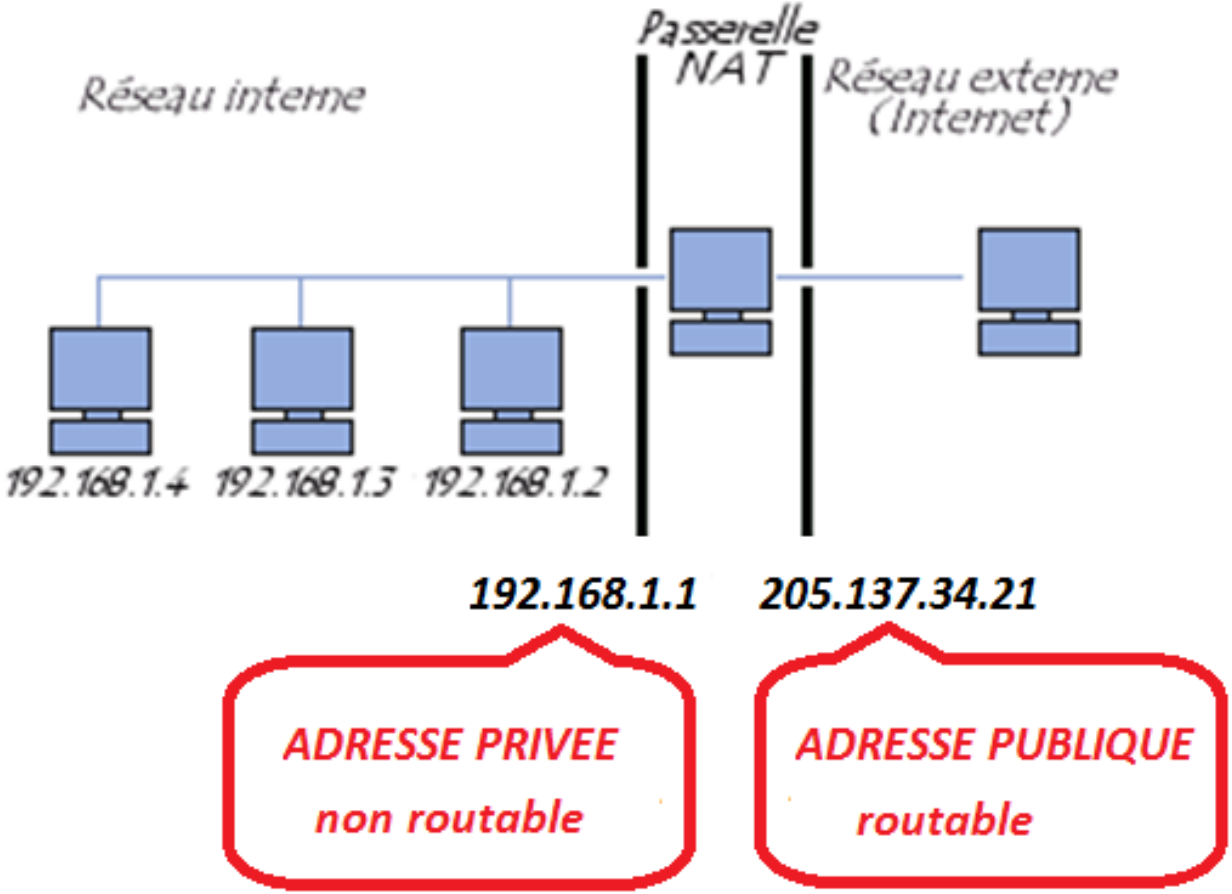
Applications

- NAT
  - Réseaux privés
- DHCP
  - Attribution dynamique de configuration réseau
- DNS
  - Convertir les noms de domaine en adresses IP
- SMTP/POP
  - Protocoles texte
- HTTP
  - Web

Réseaux privés et NAT

- Situation
  - Une machine ne possède pas d'adresse IP connue par le réseau
- Problème 1
  - Se connecter à internet pour envoyer des requêtes et obtenir des réponses
  - Ex : navigation web, envoi de mail, obtenir une page web
  - Solution : *Adresse Translation*
- Problème 2
  - Etre joignable par une machine du réseau public
  - Ex: installer un serveur web dans un réseau privé
  - Solution : *Port forwarding*

Exemple


Passerelle
NAT
Réseau interne
Réseau externe
(Internet)
192.168.1.4
192.168.1.3
192.168.1.2
192.168.1.1
205.137.34.21
ADRESSE PRIVEE
non routable
ADRESSE PUBLIQUE
routable

NAT (Translation d'adresses)

- Adresses routables et adresses non routables
  - **Routable** = qui peut être utilisé dans les tables de routage des routeurs internet. Identifie un routeur ou une passerelle
  - **Non routable** = qui identifie un hôte avec une adresse ayant une signification locale, donc inutilisable par un routeur
- **Mascarade IP** (*IP masquerading*)
  - Transformer une @ip non routable en une @ip routable
  - Table de correspondance <@ip privé <-> @ip publique>
  - Lorsqu'une machine du réseau effectue une requête vers Internet
    - 1) la passerelle effectue la requête à sa place en modifiant l'@ip privé de l'expéditeur avec l'@ip routable
    - 2) la passerelle reçoit la réponse et interroge sa table de correspondance
    - 3) elle transmet la réponse à la machine ayant fait la demande.
  - De l'extérieur, toutes les requêtes semblent provenir de l'adresse publique.

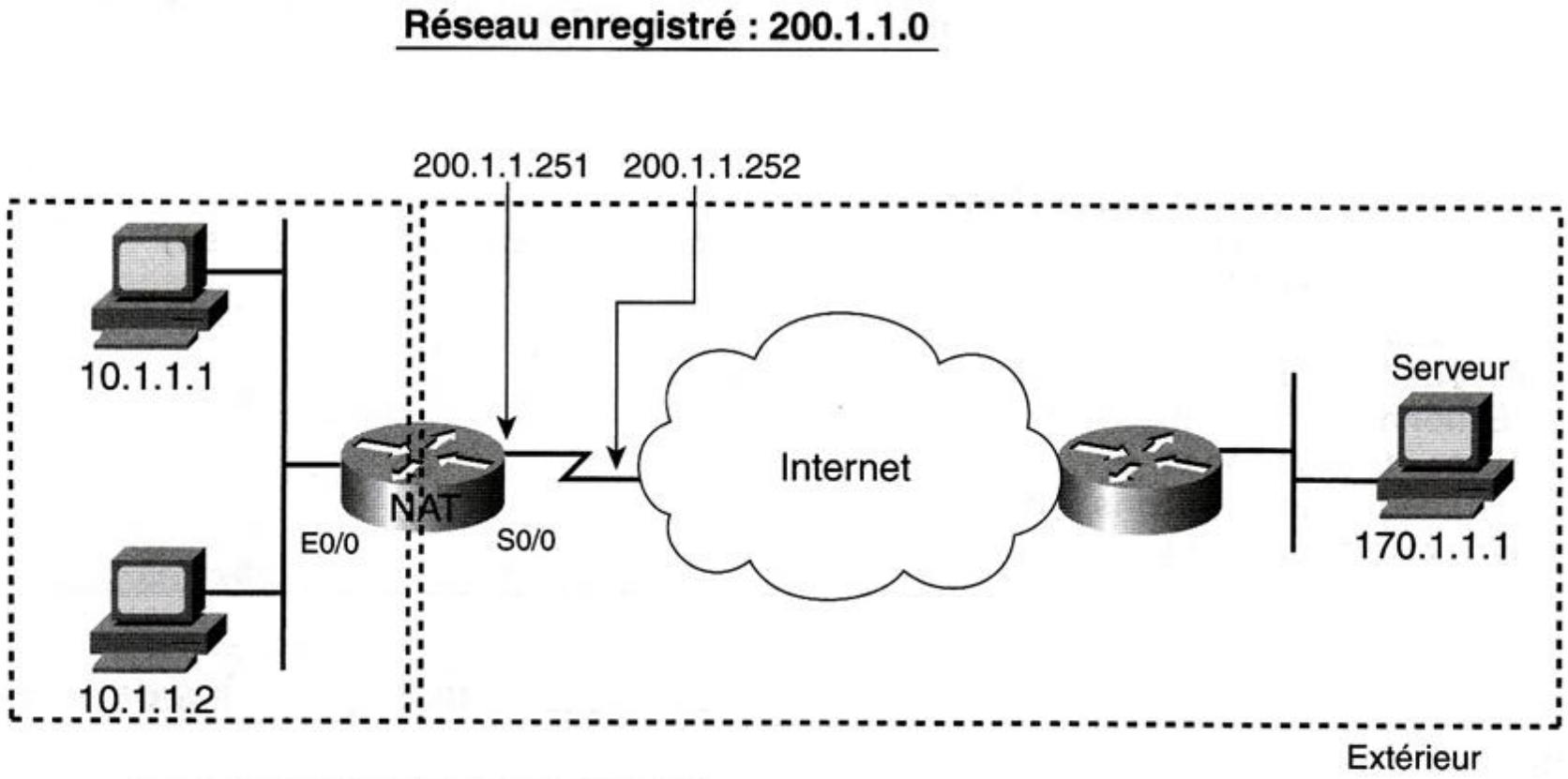
NAT (Translation d'adresses)

- IANA (*Internet Assigned Number Authority)*
  - L'organisme gérant l'espace d'adressage public (adresses IP routables)
- RFC 1918
  - Norme réseau qui définit un espace d'adressage privé permettant à toute organisation d'attribuer des adresses IP aux machines de son réseau interne sans risque d'entrer en conflit avec une adresse IP publique allouée par l'IANA.
  - Ces adresses sont dites non-routables
- Plages d'adresses non-routables
  - Classe A : plage de 10.0.0.0 à 10.255.255.255 ;
  - Classe B : plage de 172.16.0.0 à 172.31.255.255 ;
  - Classe C : plage de 192.168.0.0 à 192.168.255.55 ;
  - Pour les petits réseaux domestiques, la plage d'adresses de 192.168.0.1 à 192.168.0.255 est généralement utilisée.

NAT statique

- Principe
  - Associer une adresse IP publique à une adresse IP privée interne au réseau dans une table de correspondance *(translation)*.
  - Chaque adresse IP privée est associée à une adresse IP publique différente statiquement
  - *n* adresses IP routables sont nécessaires pour connecter *n* machines du réseau interne
  - L'adresse de l'émetteur du paquet IP est modifiée par la passerelle
- Avantage
  - La translation d'adresse statique permet de connecter des machines du réseau interne à internet de manière transparente
- Inconvénient
  - Ne résout pas le problème de la pénurie d'adresse

Exemple



Locales internes	Globales internes
10.1.1.1	200.1.1.1
10.1.1.2	200.1.1.2

NAT dynamique

- Principe
  - La traduction NAT dynamique ressemble à la traduction statique car elle crée une 1 @ip publique correspondant à une @ip privée unique
  - La différence réside dans le fait que la substitution se fait dynamiquement, au fur et à mesure des besoins/requêtes
  - Configuration
    - un pool d'adresses publiques
    - des critères pour désigner l'ensemble des adresses locales internes qui doivent être remplacées.
- Avantage
  - Une seule @ip publique est attribuée à plusieurs machines
- Inconvénient
  - Il faut avoir suffisamment d'adresses publiques pour assurer une bonne connectivité des postes clients (adr privées). Dans l'absolu, un nombre identique.

Exemple de NAT dynamique

L'hôte 10.1.1.1 envoie son paquet destiné au serveur 170.1.1.1 via sa passerelle

Le routeur remplace alors l'adresse source inscrite par l'adresse prélevée dans le pool et transmet le paquet sur l'interface adéquate.

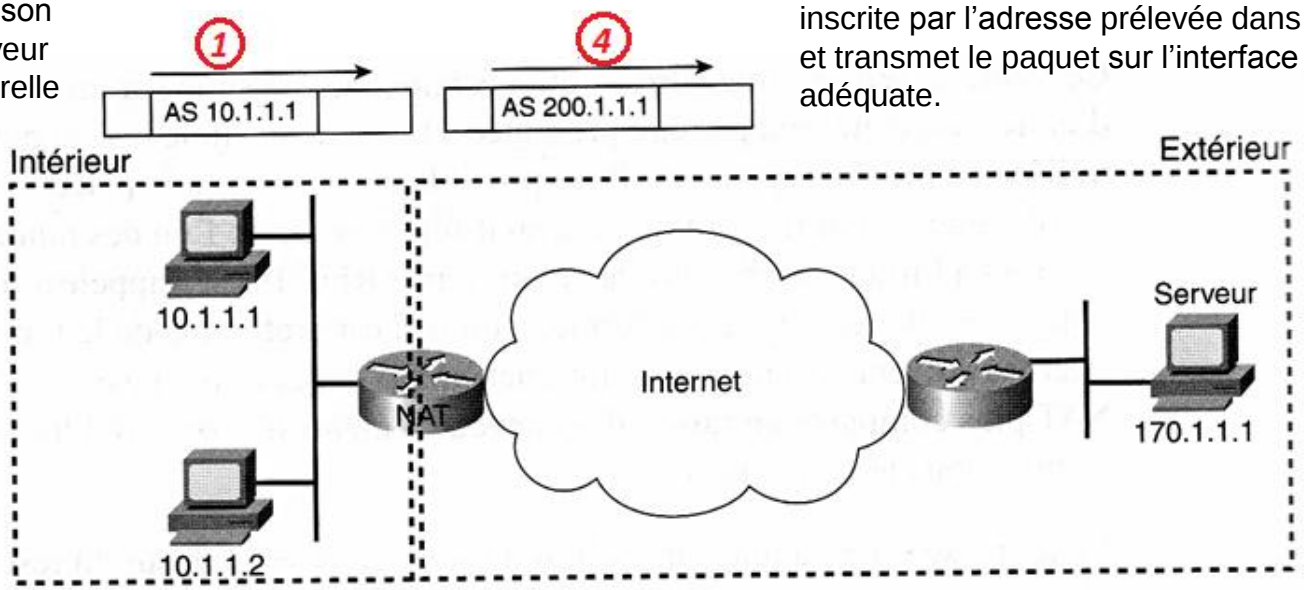


Table NAT avant le premier paquet

Locales internes	Globales internes

Critère d'application de NAT :
10.1.1.0 - 10.1.1.255

Pool NAT :
200.1.1.1
200.1.1.2
200.1.1.3
200.1.1.4
200.1.1.5

2

Table NAT après le premier paquet

Locales internes	Globales internes
10.1.1.1	200.1.1.1

3

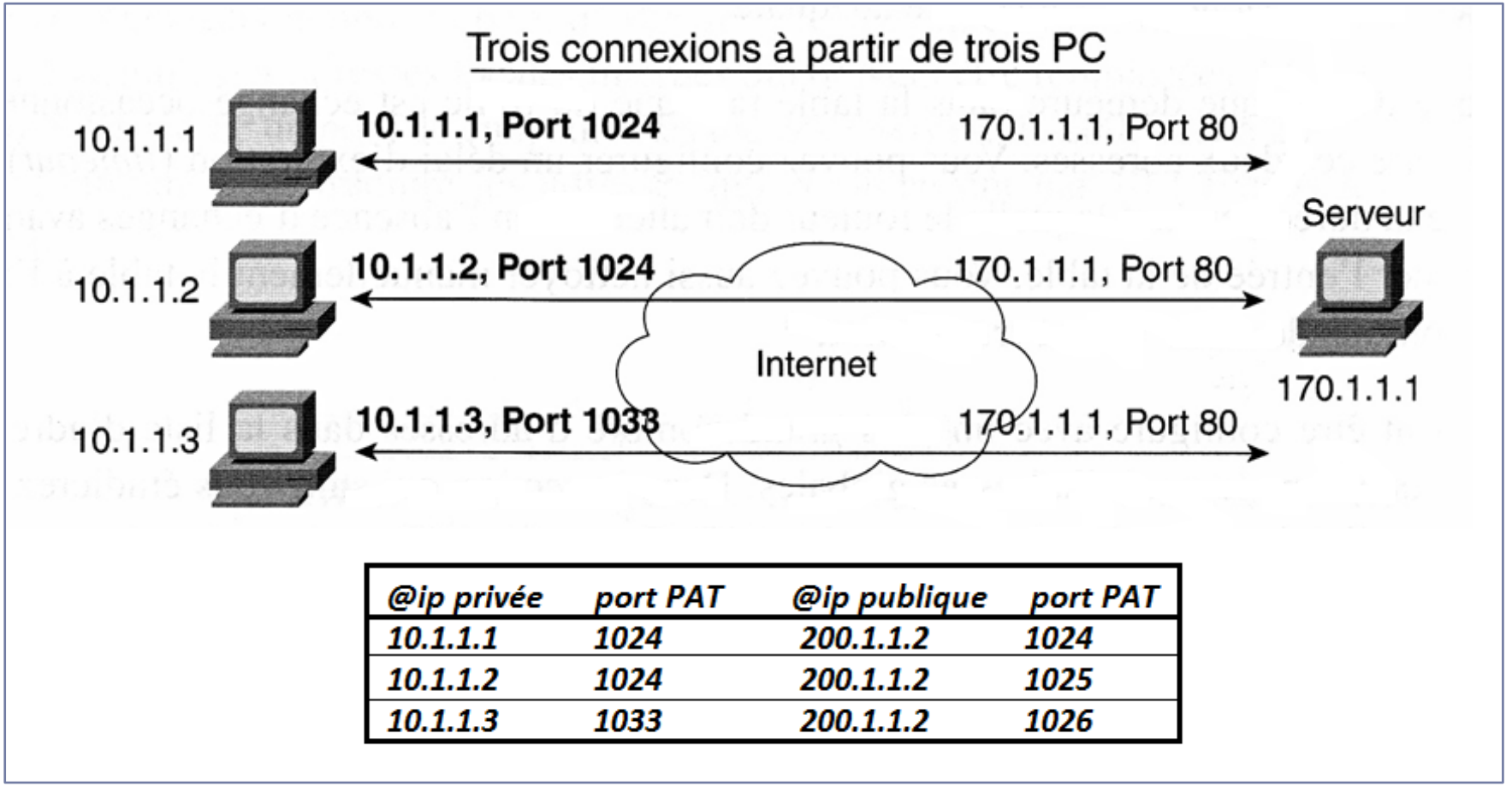
Lors de l'arrivée du paquet sur l'interface interne du routeur NAT, celui ci applique la traduction définie

Le routeur doit donc allouer une adresse publique à partir du pool d'adresses globales internes définies disponibles

NAT dynamique avec overloading

- L'overloading, ou traduction PAT, permet à NAT de s'adapter à l'augmentation des clients Internet d'une entreprise.
- **PAT** - *Port Address Translation*
  - Port NAT : affectation d'un port source différent à chaque requête
  - **(@ip privée, PAT)<->(@ip pub. src, @ip pub. dest, PAT)**
  - Maintient une correspondance entre les requêtes provenant du réseau interne et les réponses des machines sur Internet, toutes adressées à l'adresse IP du routeur

Exemple de NAT dynamique avec overlaping



@ip privée	*port PAT*	*@ip publique*	*port PAT*
10.1.1.1	*1024*	*200.1.1.2*	*1024*
10.1.1.2	*1024*	*200.1.1.2*	*1025*
10.1.1.3	*1033*	*200.1.1.2*	*1026*

- Le serveur 170.1.1.1 ne fait pas la différence

Port forwarding

- Objectif
  - Rediriger un paquet vers une machine précise en fonction du port de destination de ce paquet.
- Principe de fonctionnement
  - Une machine extérieure de se connecte à la passerelle sur un port TCP/UDP.
  - Les connexions arrivant sur ce port sont redirigées vers une machine interne possédant une @ip privée.
- 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

A retenir

- NAT est un mécanisme de correspondance entre des @ip privées (non routables) et des @ip publiques (routables)
- NAT : autoriser une machine interne à envoyer des requêtes vers internet
  - Le NATage dépend du nombre N d'@ip publiques à dispostion
  - NAT statique : N<->N statiquement
  - NAT dynamique : N<->1 choisi à chaque requête (IP masquerading)
  - NAT dynamique avec PAT : M<->1, avec M>N
- Port forwarding : autoriser une machine externe à envoyer des requêtes sur une machine interne
  - Le port de connexion est redirigé vers une machine donnée

DHCP (**Dynamic Host Configuration Protocol**)

- Protocole qui permet à un ordinateur qui se connecte sur un réseau d'obtenir *dynamiquement* (c'est-à-dire sans intervention particulière) sa configuration réseau
  - Adresse IP, masque de sous-réseau
  - Adresse IP de la passerelle
  - Adresse IP du serveur DNS
- But
  - Simplification de l'administration d'un réseau
  - Economie des adresses IP

DHCP

- Un ou plusieurs serveur(s) DHCP dans un réseau local
  - Plusieurs clients
- Initialement, un client n'a pas de configuration réseau
- La machine source émet un broadcast pour trouver son serveur DHCP
- Le serveur répond avec un broadcast contenant toutes les infos pour la configuration réseau
  - @ip temporaire
  - Masque de sous-réseau
  - @ip DHCP
- Cas 1 : le client accepte la config et diffuse son accord. Le serveur enregistre le client
- Cas 2 : le client n'accepte pas la config et recommence

DHCP : les baux

- Bail
  - Les @ip fournies pas le serveur DHCP sont temporaires
- Bail arrive à expiration
  - Cas 1 : le client demande une prolongation de son bail
  - Cas 2 : le serveur demande au client s'il veut une prolongation
- Adresse IP dynamique
  - Il peut exister plus de machines clientes que d'@IP temporaires
  - Le protocole repose sur l'hypothèse que toutes les machines ne sont pas connectées toutes en même temps

DHCP : baux

- Problèmes
  - Eviter que le serveur DHCP n'ait plus d'@ip à disposition quand une nouvelle machine en demande
  - Eviter de surcharger le réseau local avec des broadcast DCHP trop fréquents
- Solution
  - Jouer sur la durée des baux
- Bail de courte durée
  - Un réseau où beaucoup d'ordinateurs se connectent et se déconnectent souvent
  - réseau d'école ou de locaux commerciaux
- Bail de longue durée
  - Sur un réseau constitué en majorité de machines fixes, très peu souvent rebootées

DHCP : configuration réseau

```
#/usr/local/etc/dhcpd.conf
option domain-name "example.com";
option domain-name-servers 192.168.4.100;
option subnet-mask 255.255.255.0;

default-lease-time 3600;
max-lease-time 86400;
ddns-update-style none;

subnet 192.168.4.0 netmask 255.255.255.0 {
  range 192.168.4.129 192.168.4.254;
  option routers 192.168.4.1;
}

host mailhost {
  hardware ethernet 02:03:04:05:06:07;
  fixed-address mailhost.example.com;
}
```

DNS par défaut
Serveurs DNS
Masque de sous-réseau

Informations sur le bail

@ip allouables
@ip de la passerelle

@ethernet du serveur DHCP
@fixe

DHCP : protocole

- Le premier paquet émis par le client est un paquet de type DHCPDISCOVER.
- Le serveur répond par un paquet DHCPOFFER, en particulier pour soumettre une adresse IP au client.
- Le client établit sa configuration, puis fait un DHCPREQUEST pour valider son adresse IP (requête en broadcast car DHCPOFFER ne contient par son adresse IP).
- Le serveur répond simplement par un DHCPACK avec l'adresse IP pour confirmation de l'attribution.
- Normalement, c'est suffisant pour qu'un client obtienne une configuration réseau efficace, mais cela peut être plus ou moins long selon que le client accepte ou non l'adresse IP

DHCP : protocole

- **DHCPDISCOVER** : localiser les serveurs DHCP disponibles
- **DHCPOFFER** : réponse du serveur à un paquet DHCPDISCOVER, qui contient les premiers paramètres
- **DHCPREQUEST** : requête diverse du client pour par exemple prolonger son bail
- **DHCPACK** : réponse du serveur qui contient des paramètres et l'adresse IP du client
- **DHCPNAK** : réponse du serveur pour signaler au client que son bail est échu ou si le client annonce une mauvaise configuration réseau
- **DHCPDECLINE** : le client annonce au serveur que l'adresse est déjà utilisée
- **DHCPRELEASE** : le client libère son adresse IP
- **DHCPINFORM** : le client demande des paramètres locaux, il a déjà son adresse IP

Protocole DHCP

- A quoi sert le message DHCPDECLINE ?
  - le client refuse une configuration proposée par le serveur DHCP
  - Si le client DHCP a reçu plusieurs messages DHCPOFFER, il recourt au message DHCPDECLINE pour refuser les offres qu'il n'utilise pas.
  - Si le serveur DHCP envoie une mise à jour de configuration IP que le client DHCP n'utilise pas, ce dernier emploie le message DHCPDECLINE pour refuser la mise à jour.
  - Le serveur DHCP utilise le message DHCPDECLINE pour refuser la requête d'un client DHCP relative aux informations de configuration IP.
  - Si le client DHCP détecte que l'adresse fournie par le serveur DHCP est utilisée sur le réseau, il emploie le message DHCPDECLINE pour refuser l'offre.

Format trame DHCP

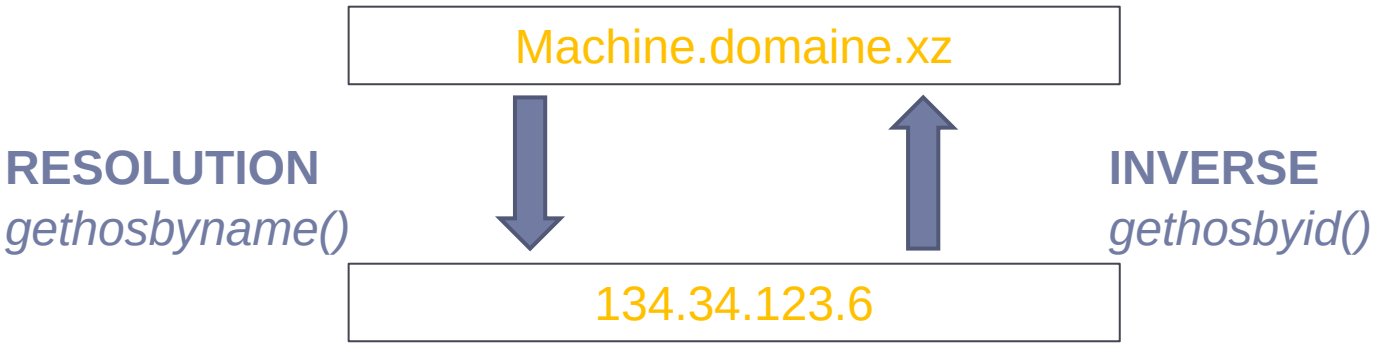
Code OP	Type de matériel	Longueur de matériel	Sauts
Secondes : 2 octets		Indicateurs : 2 octets	
Adresse IP client (CIADDR) : 4 octets			
Votre adresse IP (YIADDR) : 4 octets			
Adresse IP serveur (SIADDR) : 4 octets			
Adresse IP passerelle (GIADDR) : 4 octets			
Adresse matérielle client (CHADDR) : 16 octets			
Nom de serveur (SNAME) : 64 octets			
Nom de fichier : 128 octets			
Options DHCP : variable			

A retenir

- Dynamique
  - Le protocole DHCP permet d'attribuer dynamiquement des @IP à des machines d'un réseau local
- Centralisé
  - Le serveur DHCP centralise les requêtes DHCP et est configuré manuellement
- Bail
  - Les @ip sont attribuées temporairement
  - Un client interroge le serveur DHCP lorsqu'il se connecte pour la première fois sur le réseau ou bien lorsque lorsque son bail arrive à expiration

DNS

- *Domain Name System*
- Utiliser des noms propres (adresses textuelles) plutôt que des adresses IP
  - Ex : www.google.fr plutôt que …
- Résolution de noms de domaines
  - Trouver la correspondance entre un nom de domaine et une @ip

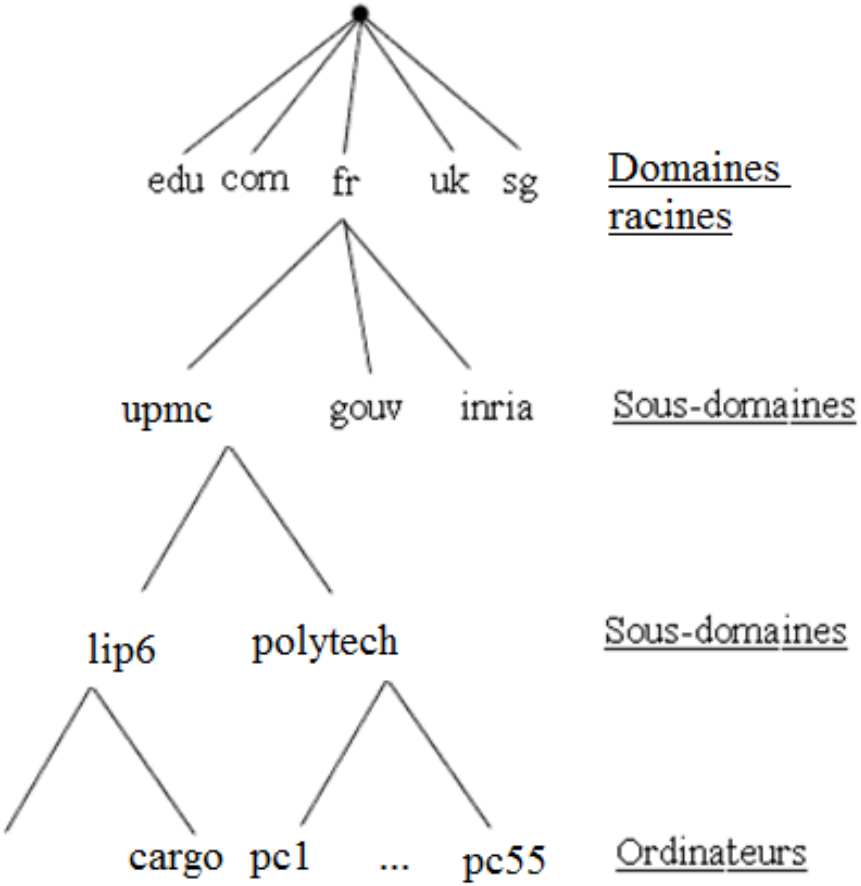


DNS

- Histoire
  - *hosts :* système de gestion manuel de correspondance dans un fichier texte de correspondance
  - *DNS :* base de données distribuée de noms de domaines (1984)
- DNS
  - Espace d'adressage de noms de domaines
  - Architecture distribuée de serveurs de noms hiérarchiques
  - Protocole de communication client/serveur udp/tcp sur le port 53.

DNS : espace de noms

- Structure arborescente



- Domaines racines
  - 7 réservés (com, edu, gov, mil, net, org, int)
  - arpa
  - Organisations nationales : fr, uk, de, it, us, au, ca, se, etc
- Sous-domaines
  - A réserver auprès de l'ICANN *(Internet Corporation for Assigned Names and Numbers*)
  - Récursifs
- Ordinateur
  - Réservés localement
  - Ex: pc55
- Nom de domaine (*domain name*)
  - Liste des labels en parcourant l'arbre vers la racine
  - Ex : pc55.polytech.upmc.fr
  - Le serveur web d'un domaine porte généralement le nom www

DNS : espace de noms

- Nommage non bijectif
  - Interface réseau = un nom d'hôte peut désigner plusieurs adresses ip pour des interfaces différentes
  - Alias = une adresse ip peut être associée à plusieurs noms
    - ftp.domaine.xz
    - www.domaine.xz
    - mail.domaine.xz

DNS : sous-domaines

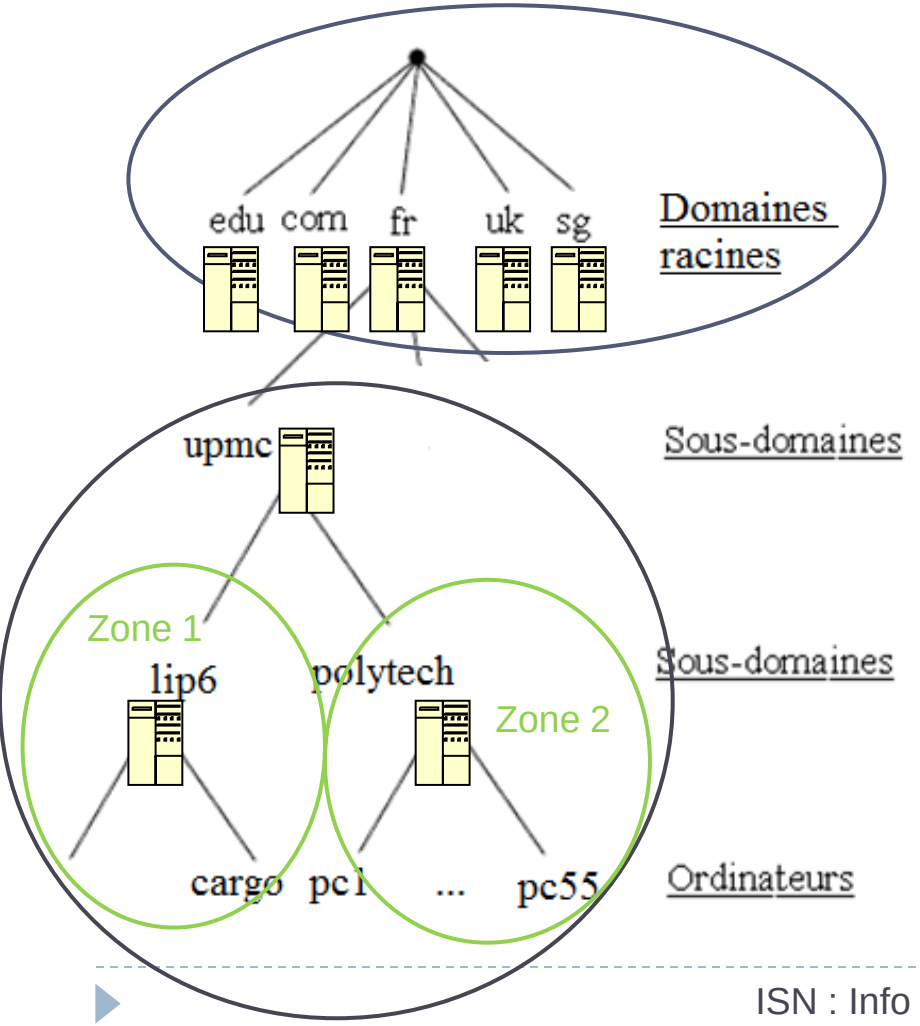
Dans un domaine, on peut créer un ou plusieurs sous-domaines

Pour chaque sous-domaine, on peut créer (ou non) une *délégation* pour ceux-ci.

- Délégation
  - Une indication que les informations relatives à ce sous-domaine sont enregistrées sur **un autre serveur**.
- Délégation récursive
  - Ces sous-domaines peuvent à leur tour déléguer des sous-domaines vers d'autres serveurs.
- FQDN (Fully Qualified Domaine Name)
  - Nom de domaine écrit de façon absolue, y compris tous les domaines jusqu'au domaine de premier niveau
  - il est ponctué par un point final, par exemple **fr.google.com.**
  - Taille max = 253 caractères

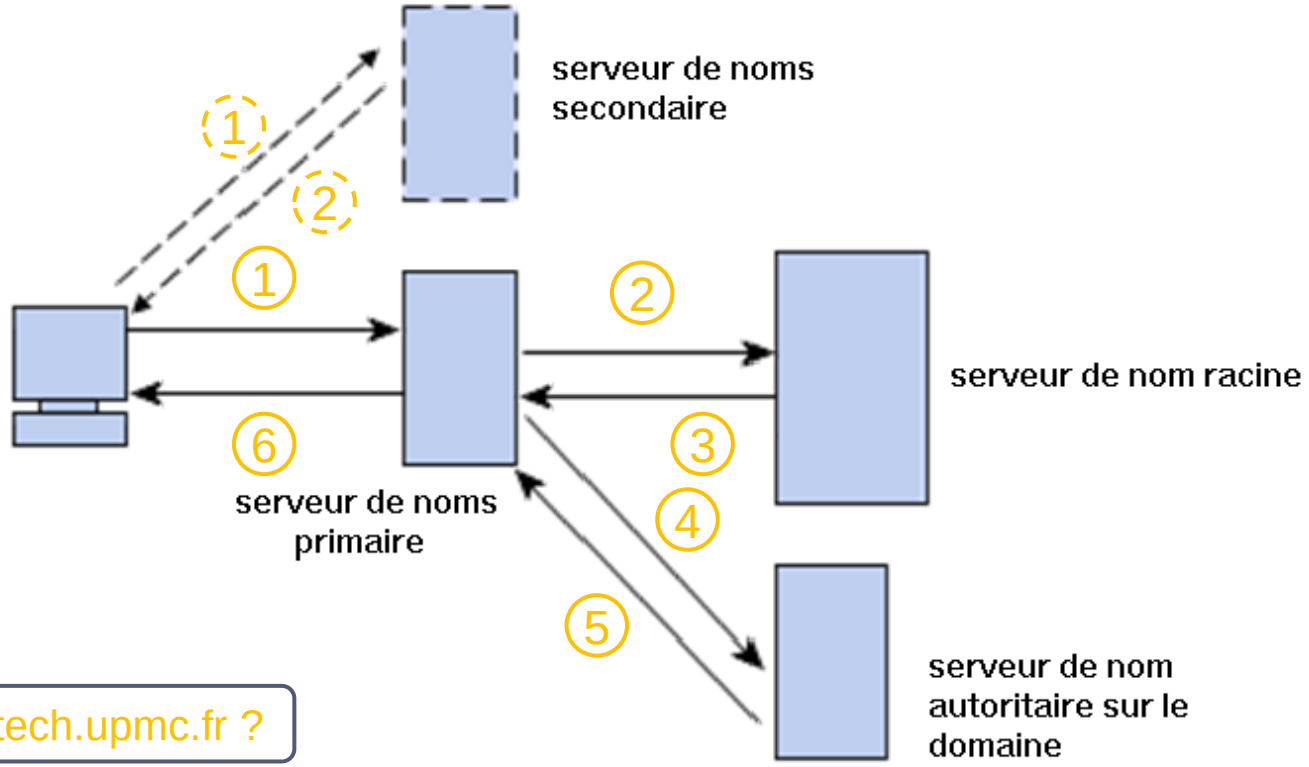
DNS : architecture

- Administration distribuée



- Serveur racines
  - Administrés par un organisme international (Registration Authority)
  - Se connaissent tous entre eux
  - Connaissent les serveurs de domaine
- Serveur de domaine (NS)
  - Administre des serveurs de zone
- Zone
  - Un sous arbre de l'arbre des noms de domaines sur lesquels un NS possède une information complète.
  - Une zone est géré par une entité administrative particulière. L'autorité sur ce sous-arbre est déléguée.
  - Délégation totale : libre organisation, changements sans préavis et délégation de sous-zones.

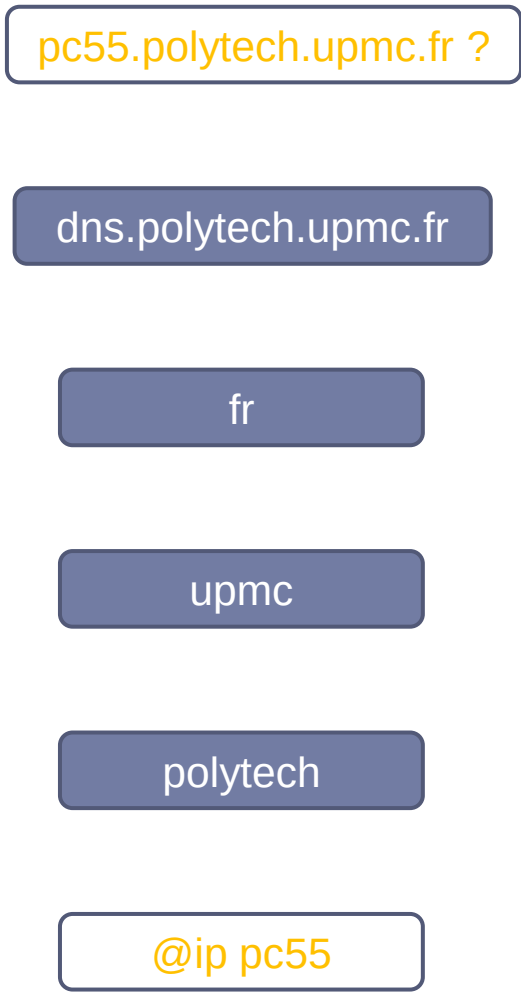
DNS : résolution de nom de domaine



pc55.polytech.upmc.fr ?

DNS : résolution de nom de domaine

1. Une application souhaite se connecter à un hôte connu par son nom de domaine. Elle interroger un serveur de noms (primaire) défini dans sa configuration réseau. En cas de problème elle connait aussi un 2eme serveur de nom primaire (backup)
2. Le serveur de nom primaire répond directement s'il possède la correspondance de nom en cache. Sinon il interroge le serveur de nom racine.
3. Le serveur de nom racine retourne une liste de serveurs de nom ayant autorité dans le domaine.
4. Le serveur de nom primaire interroge l'un de ces serveurs de nom
5. Le serveur lui retourne directement l'@ip de la machine s'il le connait sinon il retourne le ou les serveurs ayant autorité dans le sous-domaine
6. Il interroge enfin le serveur final qui connaît le nom de toutes les machines



DNS : répartition de charge

- Lorsqu'un service génère un trafic important
- Technique du *DNS Round-Robin* (tourniquet)
  - associer plusieurs adresses IP à un nom de domaine.
  - Nous avons vu en TP que www.google.fr renvoyait à différentes @ip
  - L'ordre dans lequel ces adresses sont renvoyées sera modifié d'une requête à la suivante.
  - Une rotation circulaire entre ces différentes adresses permet ainsi de répartir la charge générée par ce trafic important entre les différentes machines ayant ces adresses IP.

À retenir

- Associer des noms de domaines à 1 ou plusieurs @ip
  - FQDN = nom de domaine complet
- Espace de noms de domaine hiérarchisé
  - Organisation internationaux pour les domaines racines
  - Organisme propriétaire pour les sous-domaines
- Résolution du nom de domaine
  - Protocole DNS au-dessus d'UDP/TCP
  - Les différents niveaux de serveurs DNS gérent des caches de correspondance entre FQDN et @ip

Protocoles texte

- Principe
  - Communication en format ASCII (échange de messages texte)
  - Chaque message terminé par <CRLF>
  - Courants car les plus simples à mettre en œuvre et les plus portables.
  - Grammaire pour décrire le format de communication.
  - C'est aux programmes communicants de faire le travail de codage et d'interprétation des chaînes reçues.
- Exemples
  - HTTP
  - SMTP/POP
- Telnet
  - Commande pour contacter un serveur manuellement en mode texte
  - Port 23

SMTP

S: 220 smtp.polytech.upmc.fr SMTP Ready
C: EHLO pc21.polytech.upmc.fr
S: 250 smtp.polytech.upmc.fr
C: MAIL FROM:<webmaster@polytech.upmc.fr>
S: 250 OK
C: RCPT TO:<cecile.lepape@lip6.fr>
S: 250 OK
C: RCPT TO:<toto@gmail.com>
S: 550 No such user here
C: DATA
S: 354 Start mail input; end with <CRLF>.<CRLF>
C: Subject: Bonjour
C: Salut Cecile,
C: comment ca va?
C :
C: A bientot !
C: .
S: 250 OK
C: QUIT
R: 221 smtp.polytech.upmc.fr closing transmission

Ouvre la connexion

Adresse de l'expéditeur

Adresse d'un destinataire

Adresse d'un destinataire

Message terminé par une ligne commençant par un point

Ferme la connexion

POP

```
S:   +OK POP3 server ready
C:   APOP toto c4c9334bac560ecc979e58001b3e22fb
S:   +OK toto's maildrop has 2 messages (320 octets)
C:   STAT
S:   +OK 2 320
C:   LIST
S:   +OK 2 messages (320 octets)
S:   1 120
S:   2 200
S:   .
C:   RETR 1
S:   +OK 120 octets
S:   <the POP3 server sends message 1>
S:   .
C:   DELE 1
S:   +OK message 1 deleted
C:   RETR 2
S:   +OK 200 octets
S:   <the POP3 server sends message 2>
S:   .
C:   DELE 2
S:   +OK message 2 deleted
C:   QUIT
S:   +OK toto POP3 server signing off (maildrop empty)
```

Ouvre la connexion

Statistiques sur le contenu de la boite mail

Récupère un mail par son numéro

Supprime un mail par son numéro

Récupère un mail par son numéro

Supprime un mail par son numéro

Ferme la connexion

HTTP

- Hypertext Transport Protocol\
- Langage du Web
  - Protocole utilisé pour la communication entre les navigateurs et les serveurs web
  - Port 80 (certains sur 8080)
- URL (Uniform Resource Locator)
  - protocole (http, ftp, news)
  - Nom du serveur
  - port
    - Chemin du répertoire de la ressource (fichier, service)
    - Nom de la ressource
  - http://webia.lip6.fr/~lepape/index.html
  - http://localhost:80/cgi-bin/programme.exe

HTTP : méthodes

- GET
  - Accède à une URL sur le serveur web
    - Simple requête pour un fichier (index.html, tp3.pdf)
    - Exécute un programe CGI avec ou sans paramètres dans l'url de la requête
- POST
  - Méthode préférée pour les formulaires web
  - Exécute un programme CGI
  - Paramètres dans le corps de la requête
  - Plus sur
- PUT
  - Pour transférer un fichier du client vers le serveur web
- HEAD
  - Demande les métadonnées des ressources uniquement
  - Utilisé pour améliorer les performances des requêtes
    - Utilisation de date de dernière modification
    - Utilisation de caches

Autres applications réseaux

- FTP (File Transfert Protocol)
  - Transfert de fichiers sur le réseau
- TSL (Transport Layer Security)
  - Sécurisation des échanges internet
- SSH
  - Sécurisation des échanges internet. Repose sur un échange de clés de chiffrement en début de connexion.
- HTTPS
  - HTTP+TSL
- SMTPS
  - SMTP+TLS

Conclusion

- Internet connaît un succès croissant depuis 50 ans
  - Découpage en couches, organisation en pile
  - Supports physiques peu chers
  - Simplicité, efficacité et robustesse d'Ethernet
  - Simplicité, généricité et adaptabilité d'IP
  - Equité de TCP
  - Administration décentralisée
- De nombreux challenges en cours et à venir
  - Réseau mobiles
  - Réseaux autonomes (MANET)
  - Réseaux pair-à-pair
  - Réseau virtuels
  - Cloud
  - Best-effort vs QoS
  - Libre échange Vs Copyright