Introduction aux Réseaux - Partie II

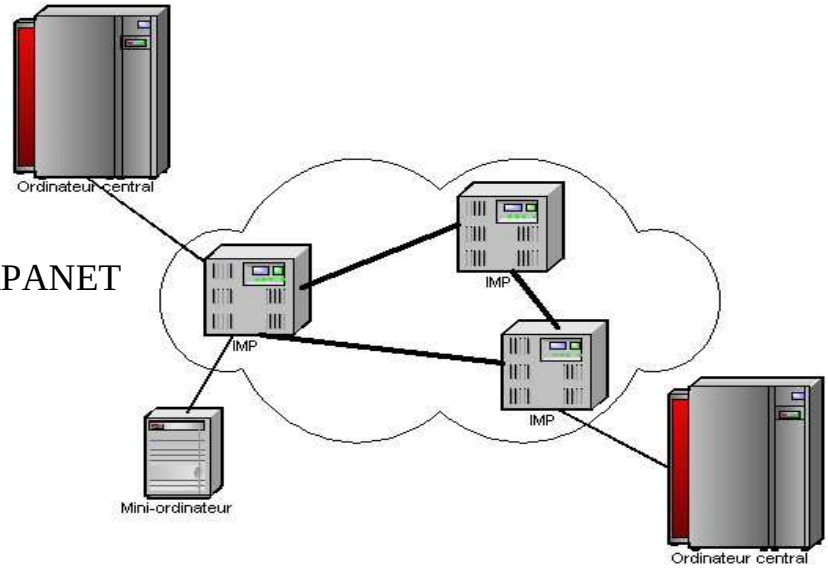
- Dans cette partie, nous allons voir
  - L'architecture TCP/IP
  - Les adresses IP et les masques de réseaux
  - L'utilisation de routeurs
  - Comment se raccorder à Internet
  - L'utilisation de DHCP

Introduction à TCP/IP

1. **Architecture TCP/IP**
2. **Adressage IP**
3. **Routage de base**
4. **Connexion à Internet**
5. **Utilisation de DHCP**

Origines de TCP/IP

- Projet DARPANET du DoD



Projet du DoD financé par DARPA (Defense Advanced Research Project Agency)

- But : interconnecter les ordinateurs militaires américains
- Transfert de fichiers

Première démonstration en 1969

- Architecture : Hôtes, IMPs
- NCP (Network Control Program) : routage et contrôle
- Interconnexion de calculateurs

Deuxième démonstration en 1973

- Grandeur réelle (20 hôtes et 5O IMPs)

Evolution : DARPANET vers ARPANET

- Connexion de sites civils (entreprises, universités, laboratoires)
- Séparation de MILNET : réseau militaire intégré au DDN (Defense Data Network)

Portée internationale

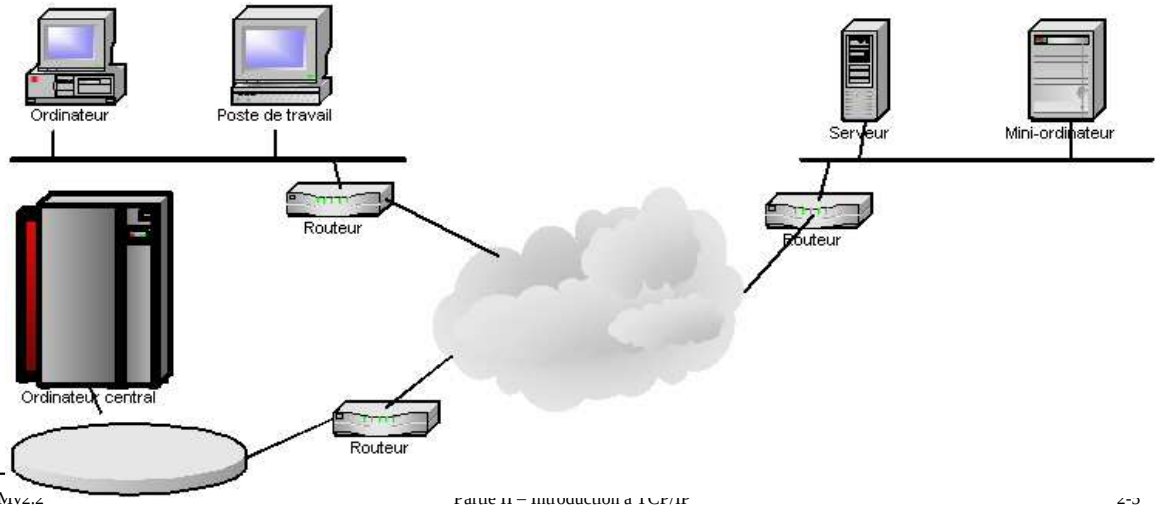
- Pays anglo-saxons
- Pays membres de l'OTAN

Interface Message Processor

Un commutateur de paquets de ARPANet

Interconnexion de réseaux

- Architecture : réseaux, routeurs, hôtes



1983 : remplacement de NCP par TCP/IP

IP : routage inter réseau

TCP et UDP : protocoles de contrôle de niveau Transport

Permet l'interconnexion de réseaux

ArpaNet devient Internet

Années 1990 : remplacement des protocoles et réseaux propriétaires par TCP/IP

Réseaux intra entreprise hétérogènes

Intranets

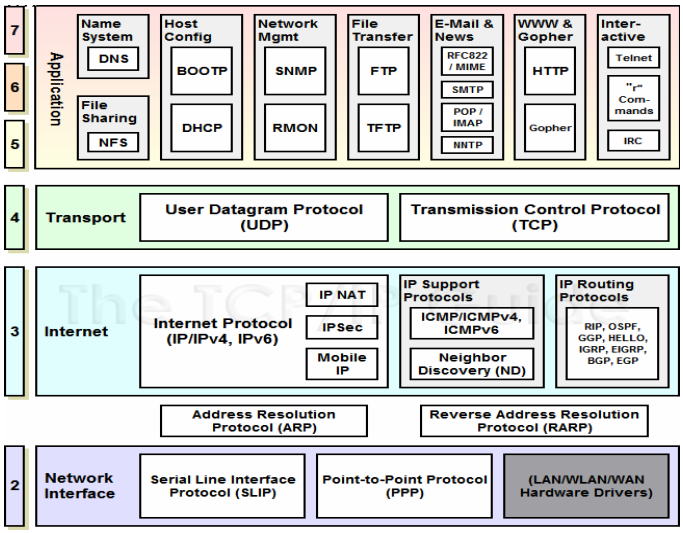
Années 2000 : tout TCP/IP

Internet global

Internet grand public

Architecture globale

- Architecture à trois niveaux



Certaines applications sont directement utilisables par les utilisateurs

FTP, Telnet, rlogin

D'autres sont utilisées par des programmes

SMTP, ESMTP, POP, IMAP

D'autres enfin sont des protocoles applicatifs utilitaires pas forcément directement accessibles

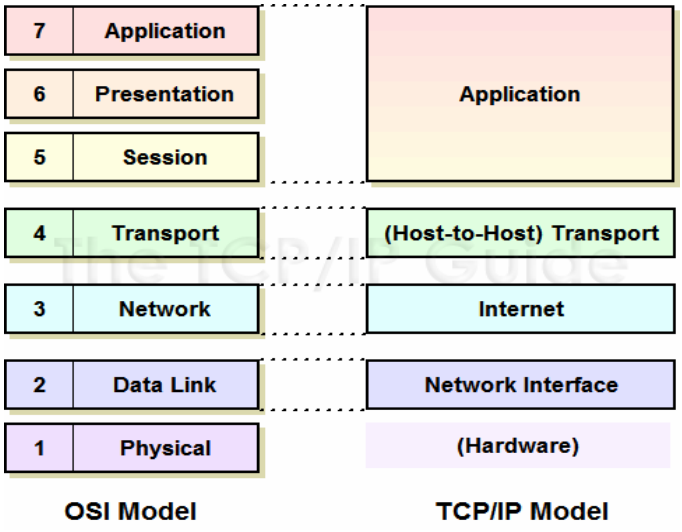
DNS, SNMP

Protocoles de Transport : TCP et UDP

Protocole réseau : IP

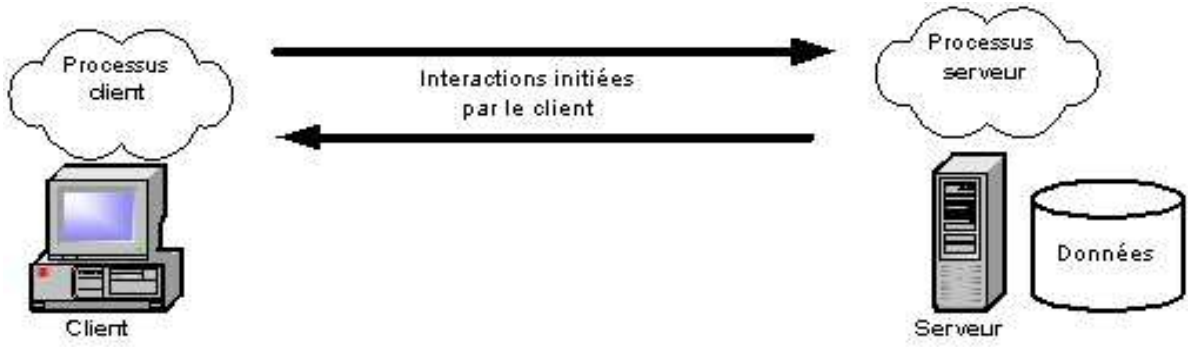
Réseaux de transfert : LANs, WANs

TCP/IP et le modèle OSI



Protocoles Applicatifs

- Modèle client serveur



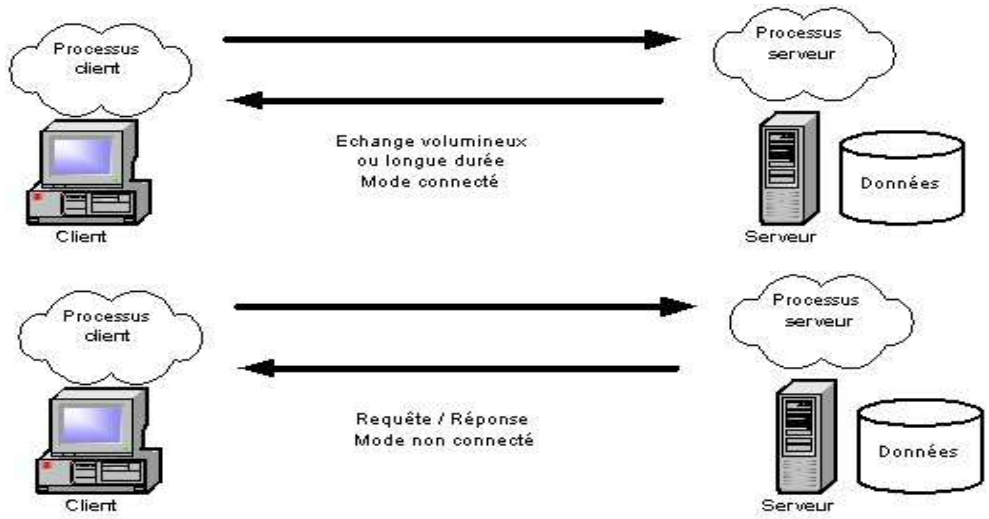
Un protocole applicatif est intrinsèquement dissymétrique

1. Côté serveur
   - ressources (matérielles ou logicielles) spécialisées
   - attente demande des clients distants
1. Côté client
   - initiation des échanges avec le serveur selon les besoins
   - déclenché par un utilisateur ou une application

Protocoles utilisateurs :
- FTP, TFTP, Telnet, HTTP, et d'autres

Protocoles de services :
- Annuaire (DNS)
- Partage de fichier (NFS)
- Gestion de réseau (SNMP)
- …

Mode connecté ou datagramme



Deux façons d'interagir entre un client et un serveur

Mode connecté

- Etablissement d'un dialogue contrôlé
- Utilisation typique de TCP
- Transfert volumineux, où interactions « longue durée »

Mode datagramme

- Dialogue requête – réponse

Quelques services applicatifs

- Transfert de fichiers
  - FTP : File Transfer Protocol
- Accès à distance
  - Telnet, rlogin, commandes r*, ssh
- World Wide Web
  - HTTP : Hyper Text Transfer Protocol
- Courrier électronique
  - SMTP : Simple Mail Transfer Protocol et ESMTP
  - POP : Post Office Protocol
  - IMAP : Internet Mail Access Protocol
- Partage de fichiers en réseau
  - NFS : Network File System
- Annuaire
  - DNS : Domain Name System
  - LDAP : Lightweight Directory Access Protocol
- Gestion de réseau
  - SNMP : Simple Network Management Protocol

Selon vous, lesquels de ces protocoles applicatifs fonctionnent en

mode connecté :

mode datagramme :

Exercice : FTP

- Utilisation du Client FTP
  - Via l'interface de commande
- Capture avec Ethereal
  - Analyse des trames

Activer une capture Ethereal avec le filtre suivant

eth.addr==VotreAdresseEthernet && ftp

Que pensez vous de ce filtre ?

Comment obtenir votre adresse Ethernet ?

Dans une fenêtre de commande Windows :

ftp

help

open AdresseIPduServeur

Au prompt, entrer le nom d'utilisateur suivant :

administrateur

Mot de passe :

administrateur

dir

cd /data

dir

pwd

quit

Arrêter la capture Ethereal et la sauvegarder

Analyser les échanges

Protocoles de Transport

- TCP : mode connecté
  - Fiabilité des échanges
  - Coûteux en ressources
- UDP : mode datagramme
  - Plus simple

TCP : mode connecté, fiabilité des échanges

- Adressage applicatif par numéro de port TCP
- Etablissement de connexion avant échange
- Négociation de paramètres de transfert
- Mémorisation/Acquittement des données échangées
- Numérotation/Séquencement des messages
- Calcul et vérification de checksum
- Terminaison de connexion
- Coûteux en ressources
  - Bande passante
  - Temps CPU
  - Capacité mémoire

UDP : mode datagramme

- Adressage applicatif par numéro de port UDP
- Pas de notion de connexion
- Pas de fiabilisation des échanges
- Pas de garantie de livraison ou de séquencement
- Garantie d'intégrité optionnelle
- Moins coûteux en ressources, plus rapide

Protocole de Réseau

- IP : mode datagramme
  - Le « workhorse » de l'architecture

IP : mode datagramme

Adressage équipement par adresse IP

Identification de la charge (protocole de la couche supérieure)

Routage et relais de proche en proche vers destination

Fragmentation possible en cours de transit, réassemblage à la destination

Pas de garantie de livraison, d'intégrité, ou de séquencement

Protocole de contrôle ICMP

- ICMP : Internet Control Message Protocol
  - Signalisation d'anomalies
  - test du réseau
  - configuration

ICMP est une application qui utilise directement IP

Paquets ICMP directement encapsulés dans IP

ICMP doit être présent sur toute implantation IP

ICMP est utilisé par

les routeurs, pour notifier tout problème lié à un paquet IP

parfois par les équipements pour s'auto-configurer

par vous et moi : commande ping

Interface applicative

- Socket : prise de communication
  - Identification par adresse IP et numéro de port
  - Structures de données et procédures associées
- Type de socket
  - Flux (stream) : TCP
  - Datagramme : UDP
  - Raw : IP

Procédures selon les languages et les environnements de développement

Socket stream (TCP)

Création, attribution numéro de port, préparation, attente, connexion, envoi et réception

Socket dgram (UDP)

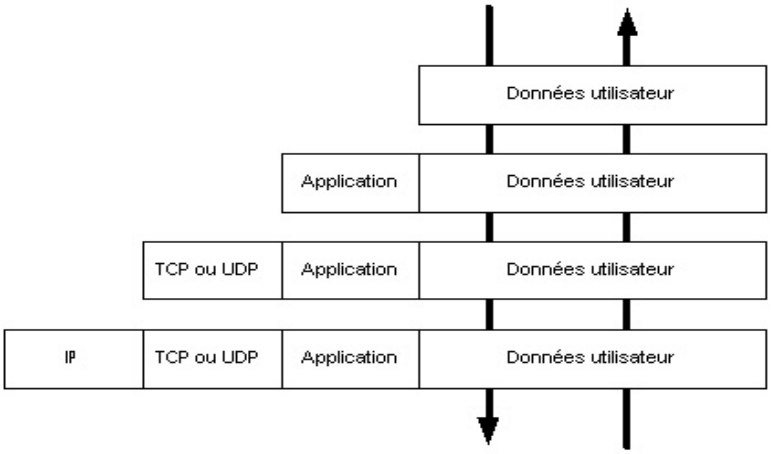
Création, attribution numéro de port, envoi et réception

Socket raw (IP)

Création, attribution numéro de protocole, envoi et réception

Encapsulation

- Insertion des PDUs (Unités de données de protocole) les unes dans les autres



TRMv2.2

2-16

Les données des utilisateurs « passent à travers les couches » jusqu'au support Physique

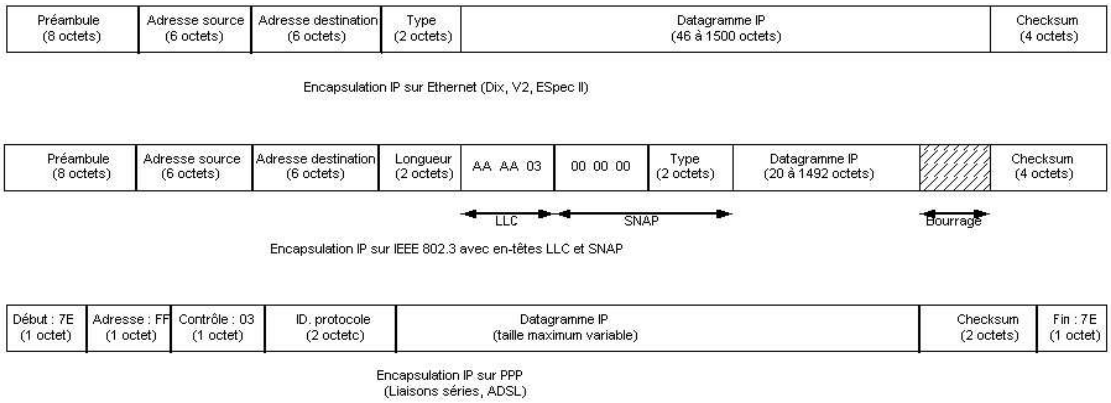
En émission, chaque couche intègre les données reçues de la couche supérieure dans la structure du paquet propre au protocole de cette couche

Elles « remontent à travers les couches » une fois arrivées à destination

En réception, chaque couche analyse le paquet de son protocole et en passe le contenu à la couche supérieure

Certains protocoles d'application, comme ICMP, utilisent directement IP

Tranfert des paquets IP



Un paquet IP (protocole de niveau 3) doit toujours être encapsulé dans un paquet de protocole adapté au transfert sur le réseau physique

Le type de réseau physique impose un choix de trame. Exemples :

- Trame Ethernet sur réseau Ethernet
- Trame IEEE 802.3 (avec encapsulation LLC et SNAP) sur réseau IEEE 802.3
- Trame PPP sur liaison série

Il existe des variantes de ces encapsulations, selon l'environnement

- Par exemple, PPPoA (PPP over ATM) pour ADSL

Exercice : Encapsulation

- Reprendre la capture sauvegardée dans l'exercice FTP
  - Analyser les différents niveaux
- Observer l'établissement des connexions TCP

Lancer Ethereal et charger la capture effectuée durant l'exercice précédant

Configurer le filtre

eth.addr==VotreAdresseEthernet

Que pensez vous de ce filtre ?

Constater que le trafic semble plus volumineux que lors de l'exercice précédant

Analyser l'encapsulation

Commandes et réponses FTP

Paquets TCP

Paquets IP

Trames Ethernet

Observer les connexions TCP vers les ports 21 et 20

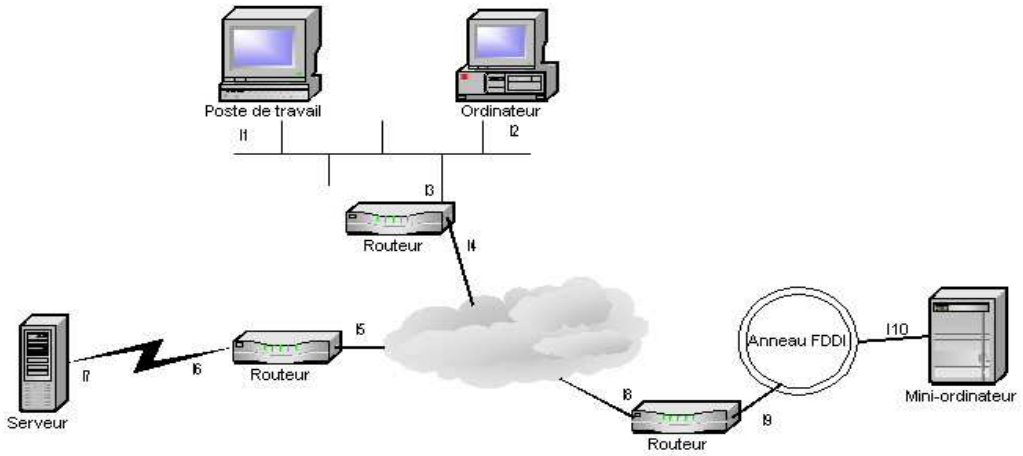
Plus d'explications seront fournies un peu plus tard

Introduction à TCP/IP

1. **Architecture TCP/IP**
2. **Adressage IP**
3. **Routage de base**
4. **Connexion à Internet**
5. **Utilisation de DHCP**

Adressage IP

- Chaque interface réseau sur laquelle on veut utiliser IP doit avoir une adresse IP



Chaque adresse IP doit être globalement unique dans le réseau IP

Adresse IP officielle sur internet

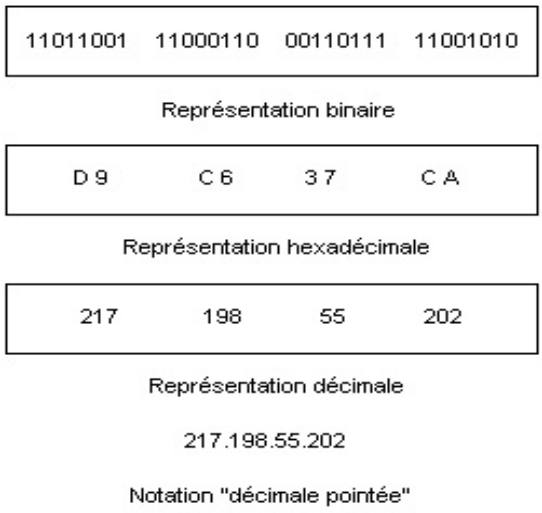
Connue des routeurs d'internet, et unique

Adresse globalement unique dans un réseau IP privé

Une adresse IP est codée sur 32 bits

Capacité théorique d'adressage de 4 294 967 296 adresses

Représentation des adresses IP



Pour connaître son adresse sous Windows

Invite de commande -> **ipconfig**

Interface graphique

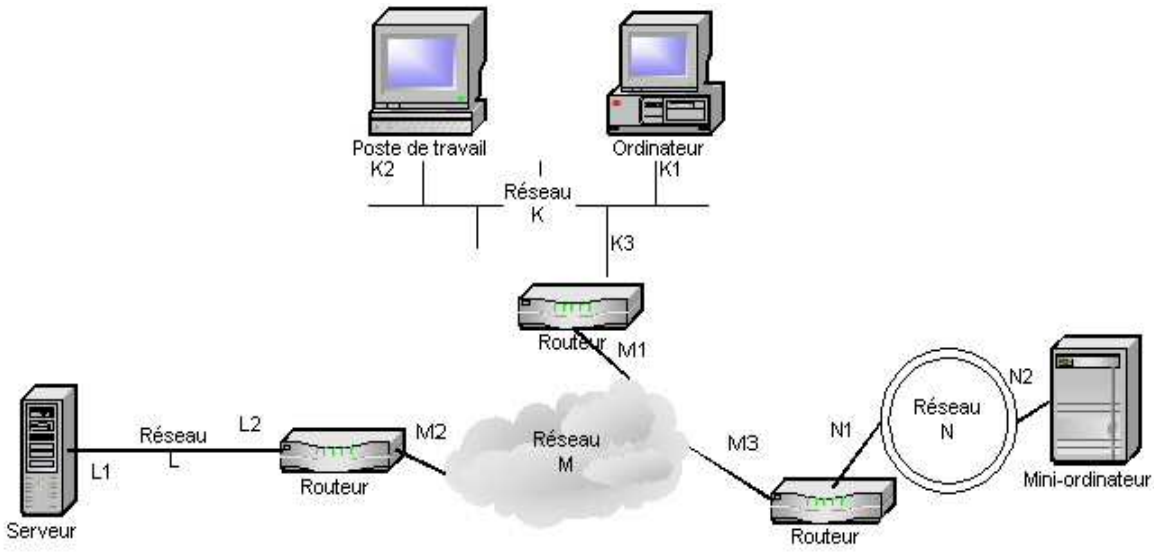
Sous Unix

Fenêtre -> **ifconfig**

Interface graphique

Noter l'adresse IP et masque associé à l'adresse IP

Identification réseau et interface



Une adresse IP identifie deux éléments

- Le réseau sur lequel se trouve l'équipement
- L'interface de l'équipement sur ce réseau

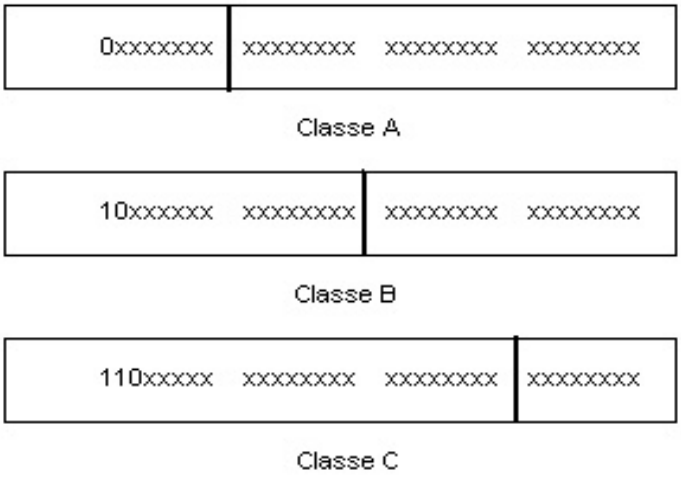
Les adresses sont fondamentales pour le routage

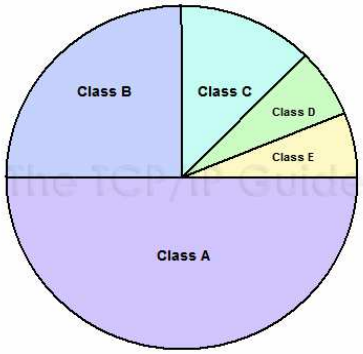
- L'identification du réseau permet d'atteindre celui-ci
- Rôle des routeurs

L'identification de l'interface permet d'atteindre l'interface de l équipement

- Nécessité de « résoudre » l'adresse IP en adresse utilisable par le réseau de transfert

Classes d'adresses





TRMv2.2 Partie II – Introduction à TCP/IP 2-23

Une adresse IP est composée de deux parties

Numéro de réseau ou NetID

Numéro d'interface ou HostID

Initialement, les concepteurs de IP ont défini trois « classes d'adresse IP », identifiées par la valeur des premiers bits de l'adresse

Classe A : très grands réseaux

NetID codé sur les 7 derniers bits du 1er octet, HostID codé sur les trois derniers octets

126 réseaux, contenant chacun 16 777 214 adresses

Classe B : grands réseaux

NetID codé sur les 14 derniers bits des deux premiers octets, HostID codé sur les deux derniers octets

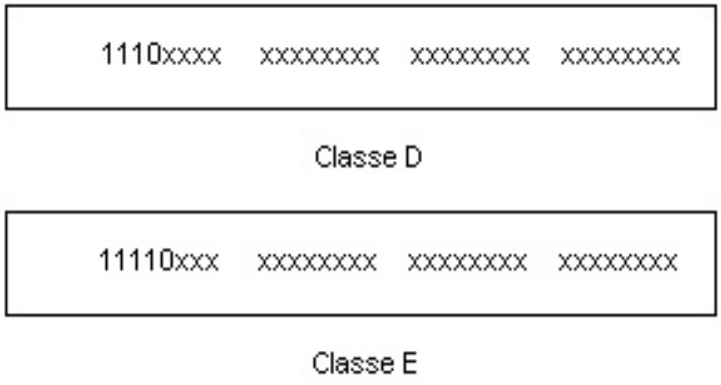
16 384 réseaux, contenant chacun 65 534 adresses

Classe C : petits réseaux

NetID codé sur les 21 derniers bits des trois premiers octets, HostID codé sur le dernier octet

2 097 152 réseaux, contenant chacun 254 adresses

Classes d’adresses



Classe D : adresses IP de « Multicast » où diffusion ; elles identifient des « groupes » de machines

Classe E : adresses IP réservées pour expérimentation

Identification des classes

Classe d'adresse	Valeurs possibles du premier octet
A	1 à 126
B	128 à 191
C	192 à 223
D	224 à 239
E	224 à 239

L'identification de la classe d'une adresse peut se faire simplement par la valeur du premier octet de l'adresse en représentation décimale pointée

Remarques

En classe A, les numéros 0 et 127 ne peuvent pas être utilisés pour identifier un réseau IP

Ces valeurs sont réservées à des utilisations spécifiques

Adresses particulières

- Numéro de réseau
  - Par exemple : 10.0.0.0, 172.16.0.0, 192.168.1.0
- Adresse de diffusion dirigée
  - Par exemple : 10.255.255.255, 172.16.255.255, 192.168.1.255
- Adresse de diffusion restreinte
  - 255.255.255.255

Numéro de réseau : quelle que soit la classe d'une adresse, si la partie HostID n'est composée que de bits à la valeur 0, cette adresse désigne le réseau lui-même et non une machine spécifique

Exemple : 10.0.0.0 (classe A), 139.124.0.0 (classe B), 192.168.1.0 (classe C)

Adresse de diffusion IP « dirigée » : quelle que soit la classe d'une adresse, si la partie HostID n'est composée que de bits à la valeur 1, cette adresse désigne toutes les machines du réseau identifié

Exemple : 10.255.255.255 (classe A), 139.124.255.255 (classe B),
192.168.1.255 (classe C)

Adresse de diffusion « restreinte » : l'adresse 255.255.255.255 désigne, sur un réseau donné et quel que soit le numéro de réseau, l'ensemble des machines connectées à ce réseau. Un tel paquet ne doit jamais sortir du réseau local : il ne franchit pas les routeurs

Adresses particulières

- Adresse non spécifiée
  - 0.0.0.0
- Adresse locale
  - 127.0.0.1

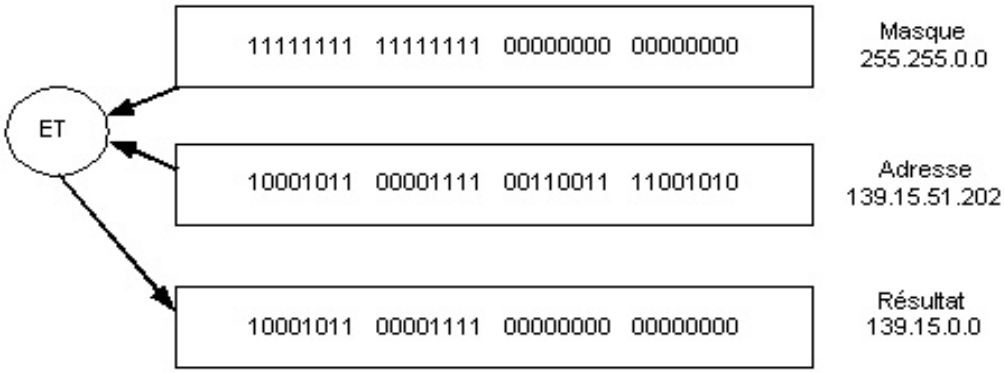
0.0.0.0 : désigne une adresse non connue, non spécifiée

Pour le routage, désigne n'importe quelle adresse

127.0.0.0 : désigne, pour toute implantation IP, les couches supérieures. Une adresse 127.X.Y.Z identifie toujours une interface virtuelle permettant d'atteindre ces couches supérieures. L'adresse 127.0.0.1 est associée au nom « localhost »

Masque de réseau

- Permet de déterminer un numéro du réseau à partir d'une adresse



Un masque de réseau permet de déterminer, à partir d'une adresse IP, le numéro de réseau IP auquel elle appartient

Un masque est une séquence de 32 bits, comme une adresse IP. Un masque est appliqué à une adresse IP par une opération ET logique, bit à bit

Masque naturel de classe : le masque à appliquer à une adresse de classe A, B, ou C pour obtenir le numéro de réseau

A : 255.0.0.0

B : 255.255.0.0

C : 255.255.255.0

Exemples :

10.3.21.34 ET 255.0.0.0 : 10.0.0.0

139.142.76.99 ET 255.255.0.0 : 139.142.0.0

192.168.15.123 ET 255.255.255.0 : 192.168.15.0

Exercice : configuration IP

- Configuration de votre station IP
  - Adresse 10.X.Y.Z
    - X : numéro de salle
    - Y : numéro de groupe
    - Z : numéro de table
  - Masque par défaut 255.0.0.0
  - Pas de routeur par défaut
  - Serveur DNS : 10.X.1.100

Dans invite de commande

taper **ipconfig /all**

Utilisation de l'interface graphique

Démarrer -> Connexions -> Afficher toutes les connexions

Activer votre interface 3Com si elle ne l'est pas

Afficher les propriétés de votre carte 3Com

Cocher la boîte « Afficher l'icône… »

Sélectionner « Protocole Internet (TCP/IP) »

Bouton Propriétés

Editer les paramètres

Fermer les deux panneaux

Dans Invite de commande, taper successivement

ipconfig /all

ping 127.0.0.1

ping 10.X.Y.Z (votre propre adresse)

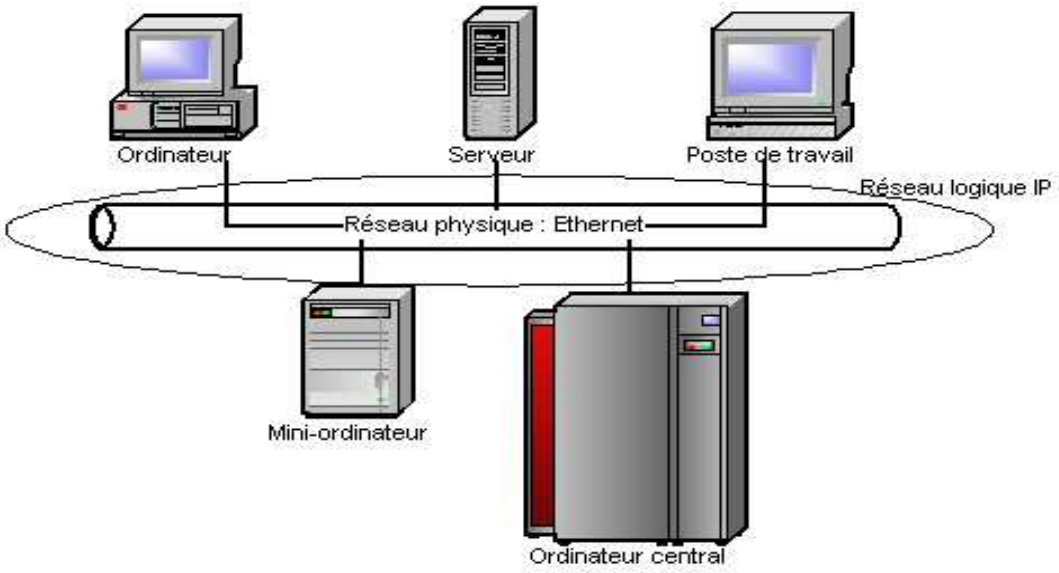
ping 10.X.Y'.Z' (une autre adresse)

ping 10.X.0.100 (serveur DNS)

Introduction à TCP/IP

1. **Architecture TCP/IP**
2. **Adressage IP**
3. **Routage de base**
4. **Connexion à Internet**
5. **Utilisation de DHCP**

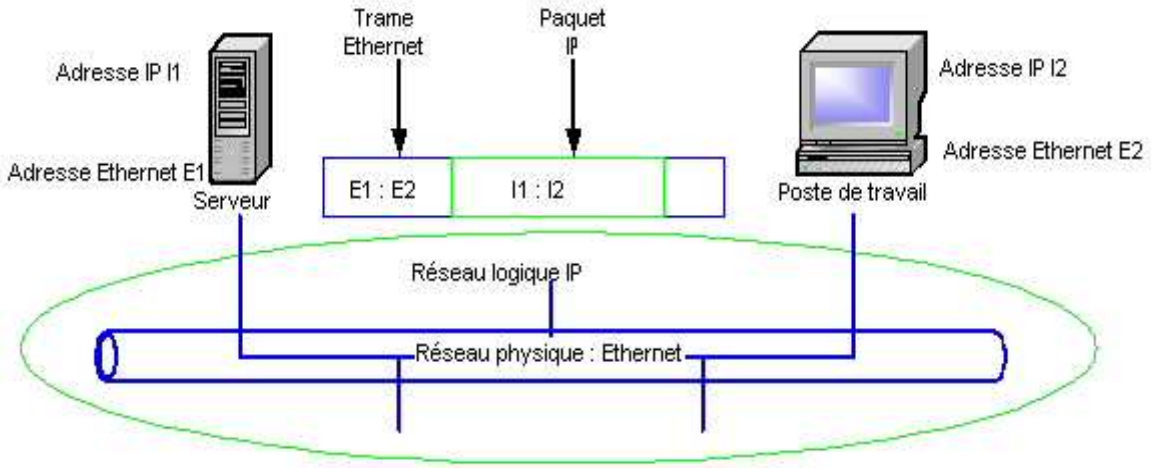
Réseau logique IP et réseau physique



Principe de base : toutes les machines appartenant à un réseau logique IP doivent être connectées au même réseau physique

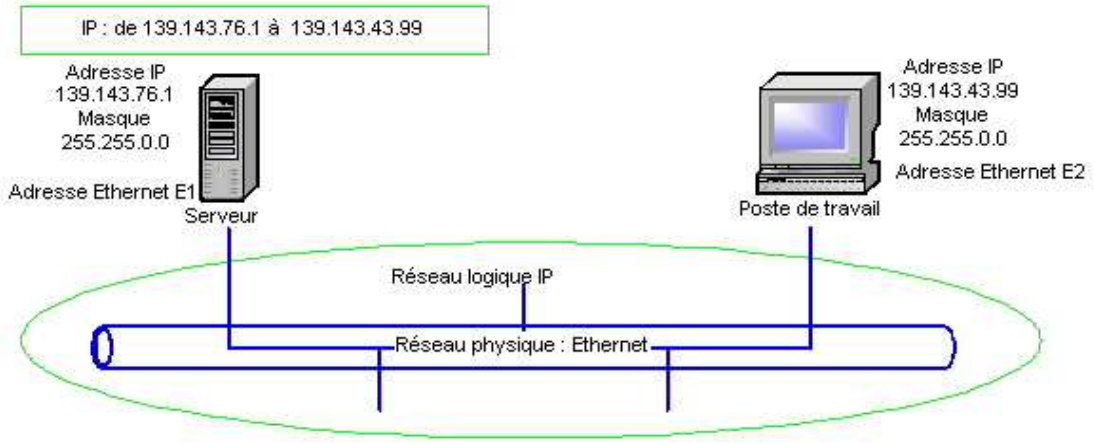
Du point de vue de l'algorithme de routage IP, deux machines sont sur le même réseau physique si leurs adresses possèdent le même identifiant de réseau : elles sont dites « adjacentes »

Transfert entre machines adjacentes



Appartenir au même réseau physique signifie être capable d'échanger directement des paquets IP par le biais du réseau de transfert sous-jacent, sans passer par l'intermédiaire d'un routeur

Test d'adjacence



Le test d'adjacence consiste à déterminer si deux machines appartiennent au même réseau logique IP

Pour déterminer si l'adresse 139.143.43.99 est sur le même réseau :

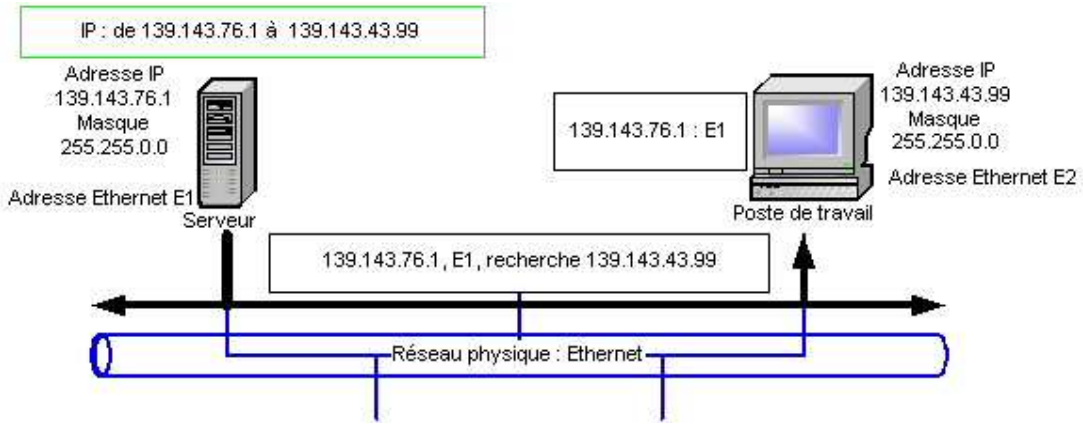
Appliquer mon masque à mon adresse : mon numéro de réseau

Appliquer mon masque à son adresse : son numéro de réseau

Les deux numéros de réseau sont ils identiques ?

Résolution d'adresse

- ARP : Address Resolution Protocol



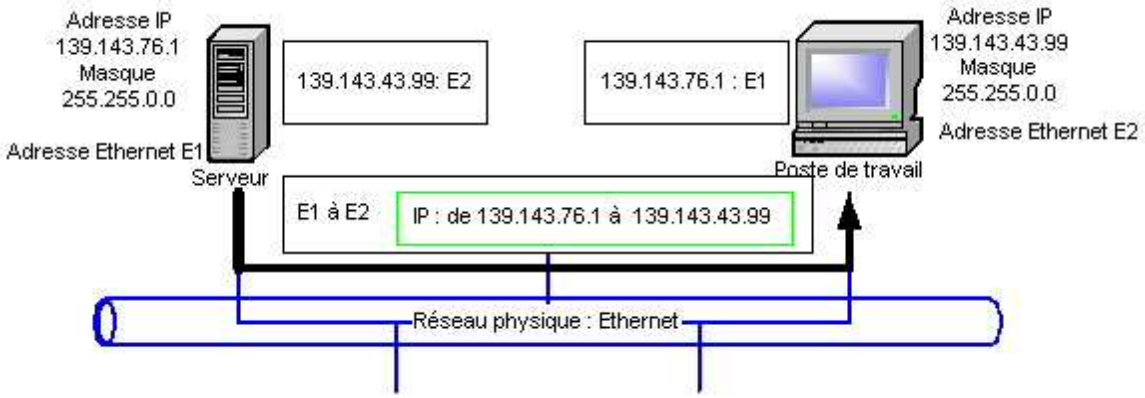
Une fois déterminée l'adjacence, nous savons que l'adresse destination est sur le même réseau

Pour atteindre cette adresse, nous savons que nous pouvons envoyer directement une trame Ethernet

Problème : comment déterminer l'adresse Ethernet correspondant à l'adresse IP destination ?

Solution : une diffusion Ethernet pour demander qui utilise cette adresse IP ; le destinataire sauvegarde en mémoire l'adresse IP et l'adresse Ethernet de la source, puis répond

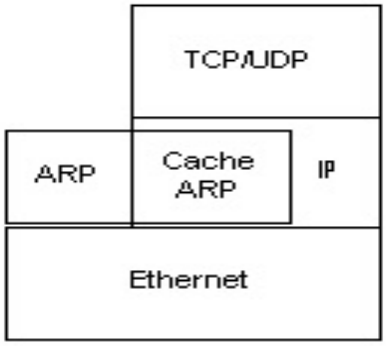
Résolution d'adresse



Une fois les adresses Ethernet associées aux adresses IP connues des deux stations adjacentes, les transferts peuvent avoir lieu

Cache ARP

- Zone mémoire contenant des entrées
  - <Adresse IP : adresse locale>



Architecture : ARP et IP

Le cache ARP est une zone mémoire dynamique

Les informations sont stockées temporairement dans le cache

Plusieurs implantations différentes

Unix : éliminer les informations du cache au bout de quelques minutes

Windows : idem, mais durée plus longue si l'adresse est utilisée

Linux : à échéance de la durée de vie, Requête ARP en mode unicast

Sur la plupart des implantations TCP/IP, des commandes permettent de visualiser ou manipuler le cache ARP

Sous Unix/Windows :

arp –a : visualiser le cache

arp –d @IP : détruire l'entrée associée à @IP

arp –s @IP @Ethernet : insérer une entrée statique liant @IP et @Ethernet

Exercice : Ethereal et ARP

- Visualisation de trames ARP
  - Elaboration d'un filtre Ethereal
  - Analyse d'une requête ARP

Dans une fenêtre de commande, taper

ping 10.X.0.50 (cette adresse IP n'existe pas sur notre réseau)

Observer les réponses au ping

Avec l'outil Ethereal

Observer les traces présentées par Ethereal

Arrêter la capture avec Ethereal

Analyser les messages ARP présentés

Adresse Ethernet Source :

Adresse Ethernet Destination :

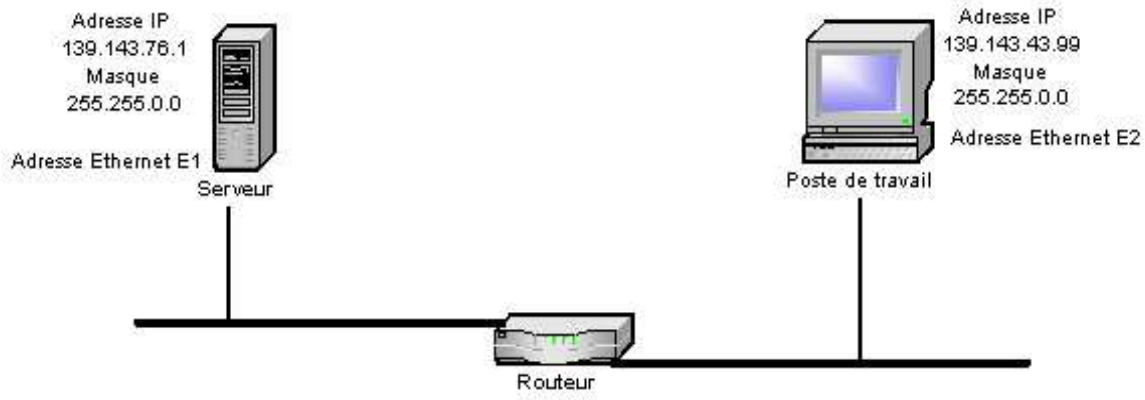
Adresse IP de l'émetteur :

Adresse Ethernet de la cible :

A votre avis, à quoi sert cette Requête ARP ?

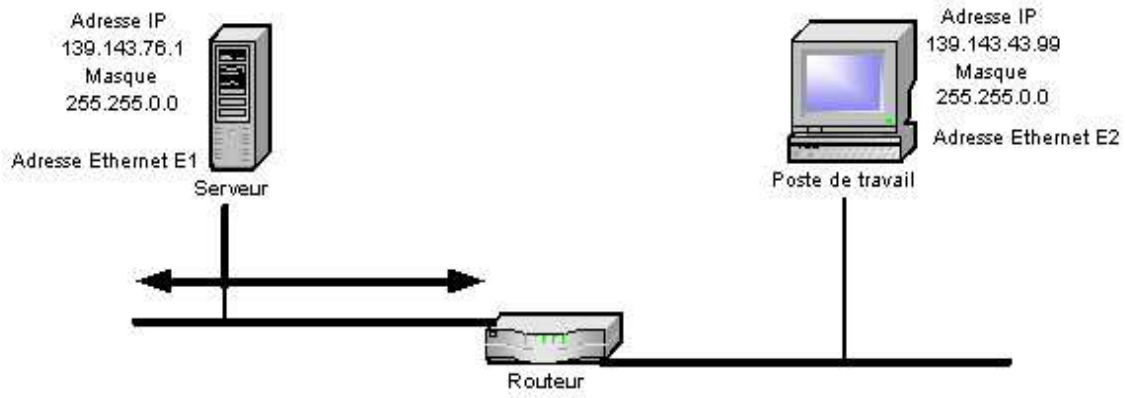
Pourquoi n'y a-t-il pas de réponse ?

Utilisation de routeur



Dans l'exemple suivant, les 2 machines sont sur le même réseau logique IP, mais en réalité sur deux réseaux physiques différents séparés par un routeur

Résolution ARP

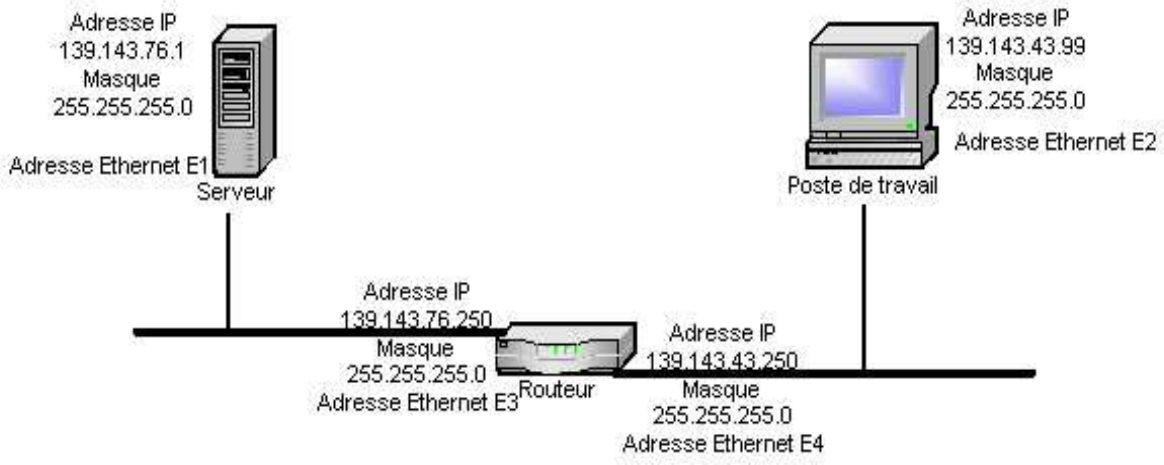


Qu’advient-il de la requête ARP ?

Le routeur ne se reconnaît pas dans l’adresse IP recherchée, et ne répond donc pas

La requête ARP n’atteint pas sa cible. L’émetteur de la requête ne reçoit pas de réponse

Sous réseaux IP



Dans ce cas, il est nécessaire d'établir deux sous réseaux logiques IP différents, et d'assigner au routeur une adresse IP cohérente sur chaque réseau

Ici, les deux sous réseaux logiques IP sont obtenus à partir du réseau 139.143.0.0 masque 255.255.0.0

- Sous réseau 139.143.43.0 masque 255.255.**255**.0
- Sous réseau 139.143.76.0 masque 255.255.**255**.0

L'allongement du masque (8 bits supplémentaires) permet de modifier le test d'adjacence : la destination n'est plus considérée comme étant sur le même réseau, la requête ARP n'est pas émise. L'émetteur va chercher à envoyer son paquet IP via un routeur

Les adresses IP commençant par 139.143

- Seront considérées dans le même réseau si le 3ème octet des deux adresses est identique
- Seront considérées dans des réseaux différents si le 3ème octet des deux adresses est différent

Contraintes

- Définir le masque approprié
- Etablir une topologie réseaux/routeurs appropriée
- Configurer les stations et les routeurs avec les adresses et les masques appropriés
- Indiquer aux stations le(s) routeur(s) permettant d'atteindre les autres réseaux

Sous réseaux IP

- Allonger le masque : 255.255.255.0

Numéro de sous réseau	Adresses	Adresse de diffusion
139.143.0.0	139.143.0.1 – 139.143.0.254	139.143.0.255
139.143.1.0	139.143.1.1 – 139.143.1.254	139.143.1.255
…	…	…
139.143.43.0	139.143.43.1 – 139.143.43.254	139.143.43.255
…	…	…
139.143.76.0	139.143.76.1 – 139.143.76.254	139.143.76.255
…	…	…
139.143.255.0	139.143.255.1 – 139.143.255.254	139.143.255.255

Etant donné une adresse de classe A, B, ou C, l'allongement du masque par défaut permet de définir un nombre particulier de sous réseaux

Les sous réseaux sont identifiés, dans l'adresse, par les bits correspondant à ceux rajoutés au masque naturel de la classe

Le nombre de sous réseaux différenciés par l'allongement du masque est égal à 2 élevé à la puissance N, N étant le nombre de bits supplémentaires dans le nouveau masque (ici, 8 bits supplémentaires font 256 sous-réseaux)

Choix du masque

- Définir le nombre de sous réseaux voulu
  - Arrondir à la puissance de 2 immédiatement supérieure
- Déterminer le nombre de bits supplémentaire dans le masque
  - Calculer le nouveau masque à partir du masque par défaut

A partir de l'adresse IP et du masque d'origine

Exemple : 139.143.0.0 / 255.255.0.0

Déterminer le nombre de sous réseaux nécessaire : arrondir à la puissance de 2 immédiatement supérieure

Exemple : 19 sous réseaux nécessaires, donc choisir 32

Déterminer combien de bits supplémentaires dans le masque sont nécessaires pour identifier ces sous réseaux

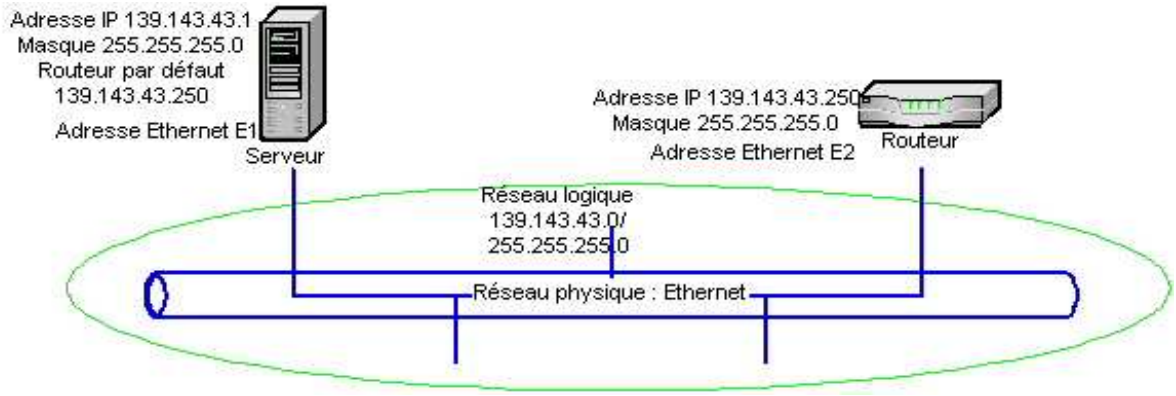
Exemple : pour identifier 32 sous réseaux, il faut 5 bits

Déterminer le nouveau masque approprié

Exemple : 255.255.248.0

Enumérer les sous réseaux, définir les plages d'adresses, et les adresses de diffusion

Routeur par défaut



A partir du moment où on cherche à atteindre une adresse qui n'est pas dans le même réseau IP, il est nécessaire d'utiliser un routeur

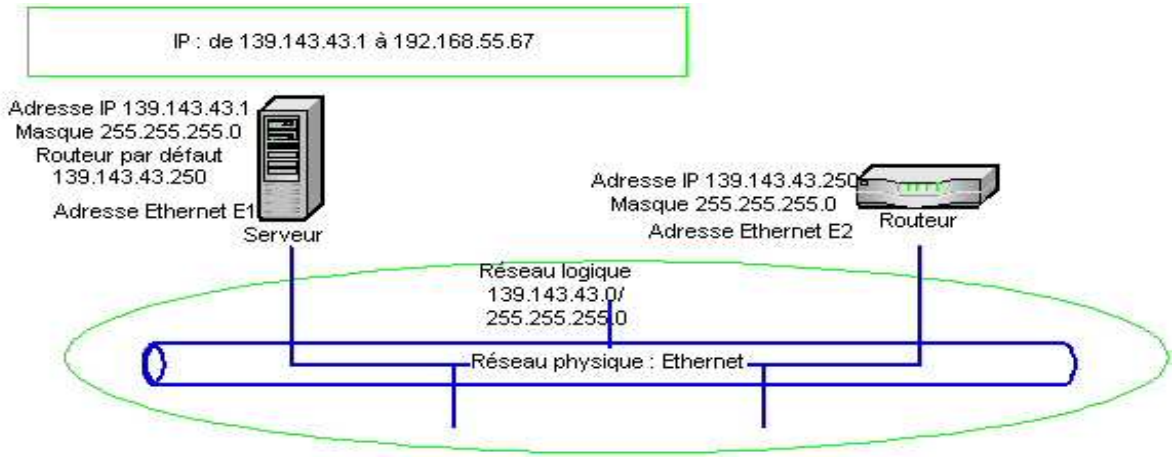
Dans la plupart des cas, sur un réseau local, il y a un seul routeur permettant d'atteindre les destinations hors de ce réseau local

Parfois deux routeurs, selon les besoins de connectivité

Il est nécessaire de configurer les implantations IP avec l'adresse d'un routeur permettant de sortir du réseau local, quelle que soit l'adresse externe : on indique alors l'adresse IP du routeur par défaut

Utilisation du routeur par défaut

- Pour envoyer un paquet IP à une adresse externe au réseau local :



L'adresse IP est elle locale au réseau ?

Test d'adjacence

Mon réseau : 139.143.43.1 ET 255.255.255.0 = 139.143.43.0

Son réseau : 192.168.55.67 ET 255.255.255.0 = 192.168.55.0

Son réseau est différent

Routeur par défaut : 139.143.43.250

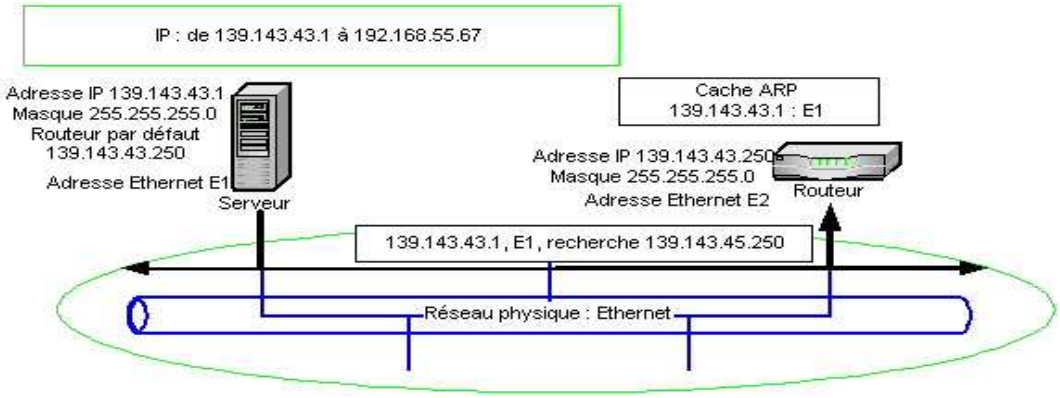
Donc il faut envoyer ce paquet à ce routeur par une trame Ethernet à destination du routeur

Donc il faut connaître l'adresse Ethernet du routeur

Supposons que l'adresse Ethernet du routeur ne soit pas dans le cache ARP

Utilisation du routeur par défaut

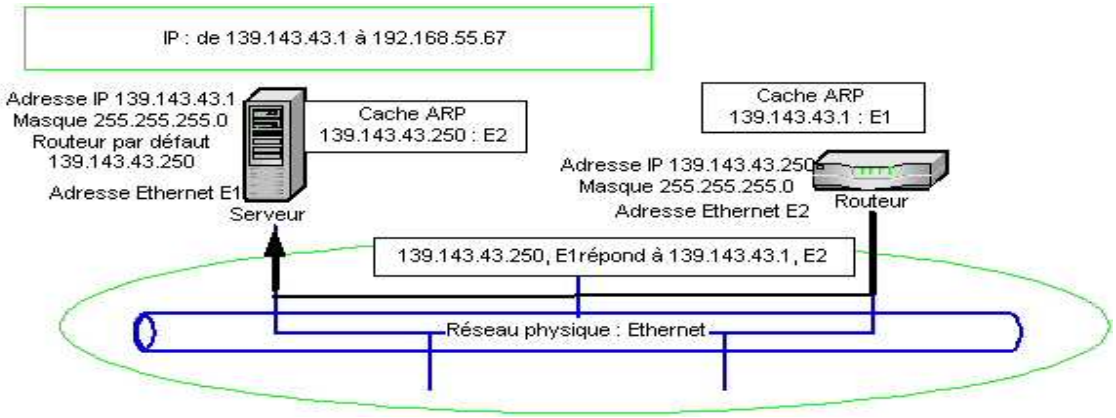
- Utiliser ARP
  - Emission de la requête



Résolution via ARP de l'adresse du routeur par défaut

Utilisation du routeur par défaut

- Transfert de la réponse



Si la résolution est positive, l'émetteur du paquet envoie le paquet IP dans une trame Ethernet adressée au routeur

Exercice : masque

- Modification du masque réseau
  - Choix d'un masque différent
    - 255.255.255.0
- Analyse des effets de ce masque

A l'aide de l'interface graphique, modifier le masque de réseau

255.255.255.0

Lancer Ethereal

Positionner un filtre sur l'adresse Ethernet de votre poste

Activer la capture

Dans une fenêtre de commande

Taper **ping 10.X.Y.Z'** (adresse IP d'une machine de votre groupe)

Observer les réponses et visualiser les trames capturées

Ceci est-il correct?

Lancer une nouvelle capture avec Ethereal

Dans une fenêtre de commande

Taper **ping 10.X.Y'.Z'** (adresse IP d'une machine d'un autre groupe)

Observer les réponses

Y-a-t-il eu des trames capturées ?

Pourquoi ?

Exercice : routeur par défaut

- Modification du routeur par défaut
  - Adresse du routeur : 10.X.Y.250
- Analyse des effets de ce paramètre

A l'aide de l'interface graphique, modifier l'adresse IP du routeur par défaut
10.X.Y.250

Lancer Ethereal avec le filtre **eth.addr==<VotreAdresseEthernet>**
Activer la capture
Dans une fenêtre de commande
Taper **ping 10.X.Y.Z'** (adresse IP d'une machine de votre groupe)
Observer les réponses et visualiser les trames capturées
Cela fonctionne-t-il comme avant?

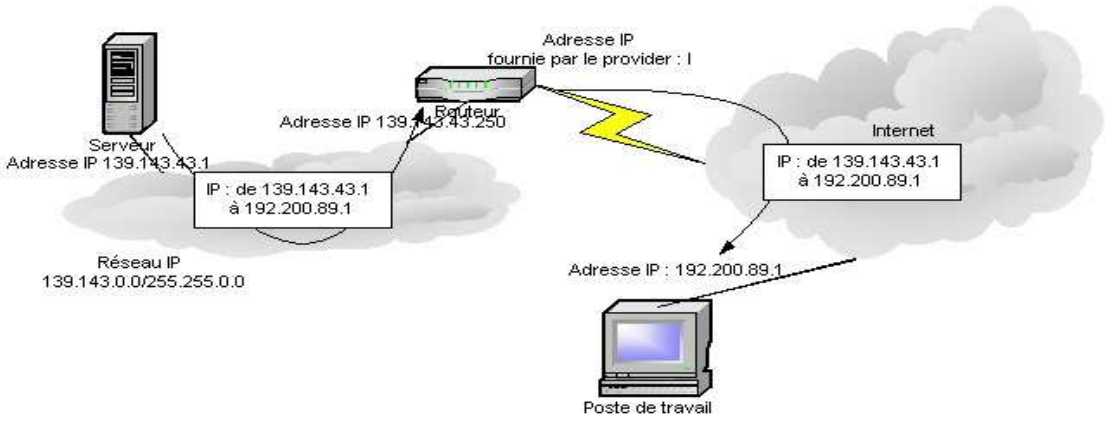
Lancer une nouvelle capture avec Ethereal
Dans une fenêtre de commande
Taper **ping 10.X.Y'.Z'** (adresse IP d'une machine d'un autre groupe)
Observer les réponses
Y-a-t-il eu des trames capturées ?
A quoi servent-elles ?
A votre avis pourquoi le ping n'obtient-il pas de réponse ?

Que faudrait-il faire pour que le ping fonctionne ?

Introduction à TCP/IP

1. **Architecture TCP/IP**
2. **Adressage IP**
3. **Routage de base**
4. **Connexion à Internet**
5. **Utilisation de DHCP**

Adresses Internet



TRMv2.2 Partie II – Introduction à TCP/IP 2-50

Les adresses Internet sont les adresses IP utilisées dans l'espace d'adressage global d'Internet

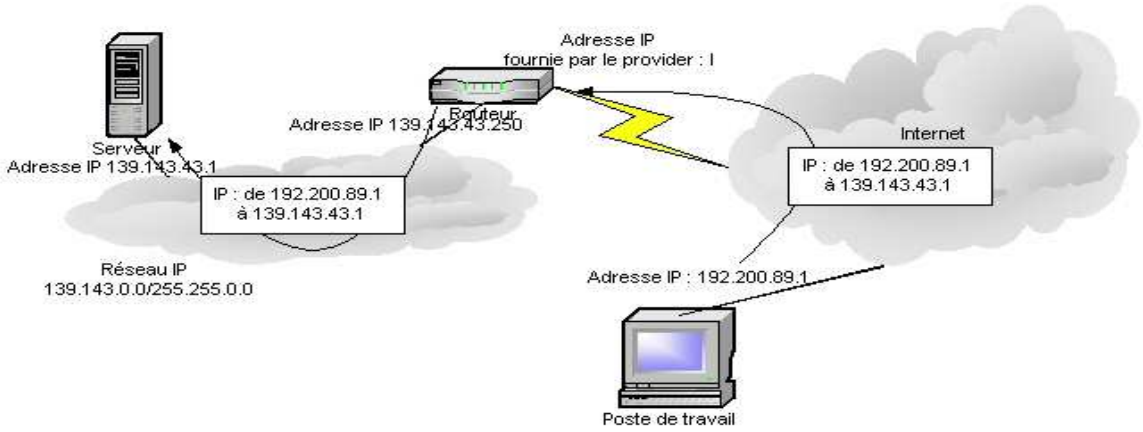
Pour se connecter à Internet, historiquement, il fallait obtenir un numéro de réseau adéquat pour son organisation (Classe A, B, ou C selon les besoins de l'organisation)

> Aujourd'hui, on obtient un « bloc » d'adresses IP défini par un numéro de réseau et un masque

Ce numéro de réseau ou ce bloc d'adresses doit être unique : il ne doit pas être utilisé par une autre organisation

Les routeurs d'Internet doivent être configurés de façon à être capable de router les paquets vers ces adresses

Adresses Internet



Les adresses Internet sont les adresses IP utilisées dans l'espace d'adressage global d'Internet

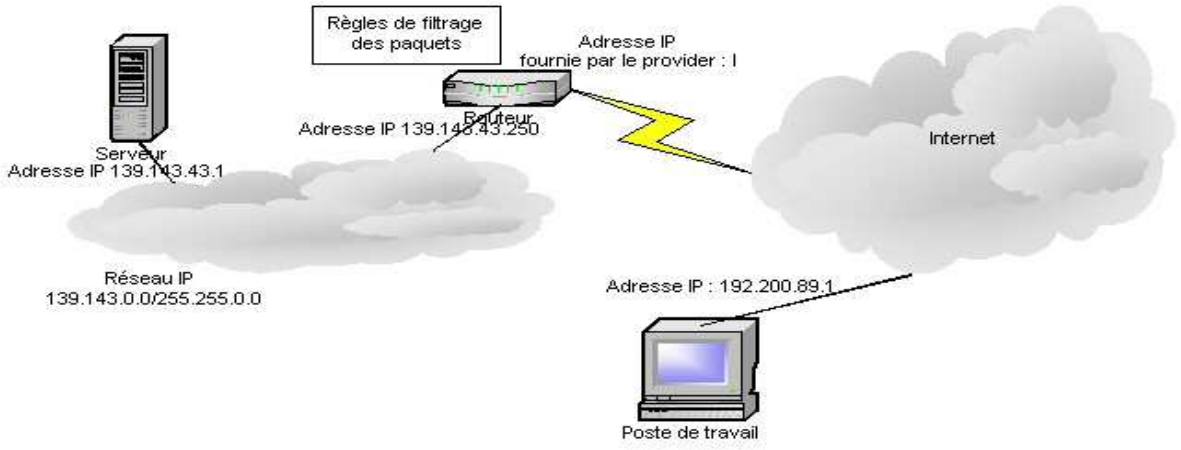
Pour se connecter à Internet, historiquement, il fallait obtenir un numéro de réseau adéquat pour son organisation (Classe A, B, ou C selon les besoins de l'organisation)

> Aujourd'hui, on obtient un « bloc » d'adresses IP défini par un numéro de réseau et un masque

Ce numéro de réseau ou ce bloc d'adresses doit être unique : il ne doit pas être utilisé par une autre organisation

Les routeurs d'Internet doivent être configurés de façon à être capable de router les paquets vers ces adresses

Connexion par un routeur



Le réseau interne doit être organisé de telle façon

- que les trafics internes soient correctement transmis à l'intérieur du réseau d'entreprise
- que les trafics à destination de l'extérieur soient retransmis vers le routeur de sortie

Le routeur externe peut éventuellement implanter des mécanismes de sécurités : filtrage des paquets entrants ou sortants, en fonction des adresses source et destination, des types de trafic (ICMP, UDP, TCP), et des applications visées (types de paquets ICMP, ports UDP et ports TCP)

Adresses privées

Numéros de réseau	Nombre	Classe	Plage d'adresses
10.0.0.0	1	A	10.0.0.1 à 10.255.255.254
172.16.0.0 à 172.31.0.0	16	B	172.16.0.1 à 172.31.255.254
192.168.0.0 à 192.168.255.0	256	C	192.168.0.1 à 192.168.255.254

Les adresses privées sont utilisables en interne, dans une organisation, connectée ou non à Internet (RFC 1918)

Plusieurs organisations peuvent utiliser ces adresses : elles ne sont pas uniques

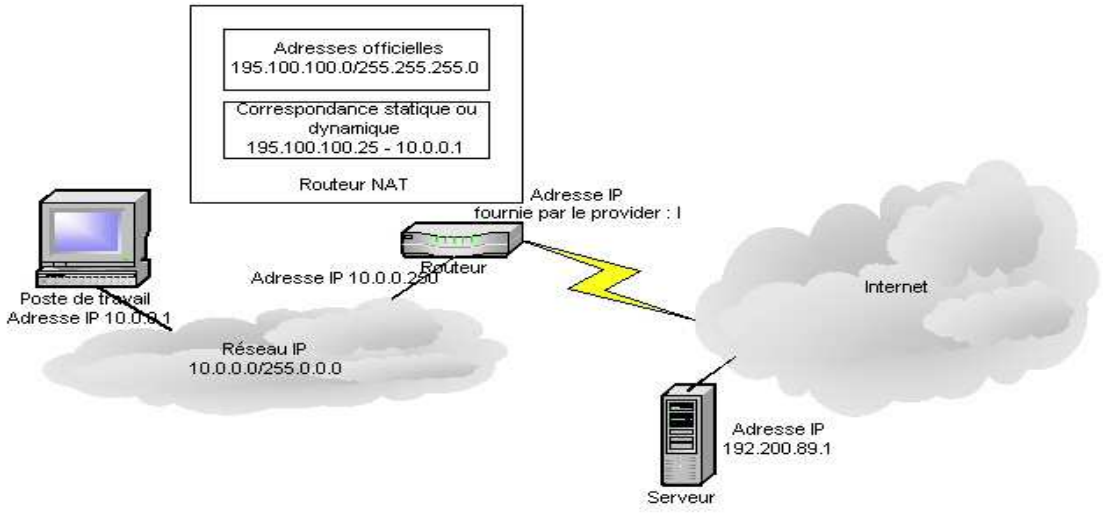
Elles ne sont pas routables dans Internet : les routeurs ne savent pas router les paquets vers ces adresses

Utilisation

- Réseau privé non connecté à Internet
- Réseau privé connecté à Internet par un équipement NAT (Network Address Translation) ou par un proxy (relais applicatif) ou par un pare-feu

Connexion par un NAT

- NAT : Network Address Translation



Considérons une connexion permanente à Internet via un routeur

L'adresse externe de celui-ci est dans l'espace d'adressage du FAI

Routable dans Internet

Le réseau d'entreprise à un numéro IP privé 10.0.0.0 / 255.0.0.0

L'entreprise possède une plage d'adresses officielle 195.100.100.0 / 255.255.255.0

L'adresse IP 10.x.x.x n'est pas routable dans Internet : les paquets IP envoyés par le client ne peuvent atteindre le serveur

Le NAT associe à l'adresse 10.0.0.1 l'adresse officielle, routable, 195.100.100.25

Association fixe : définie par l'administrateur du NAT

Association dynamique

Pour TCP

Association lors de l'établissement de connexion TCP

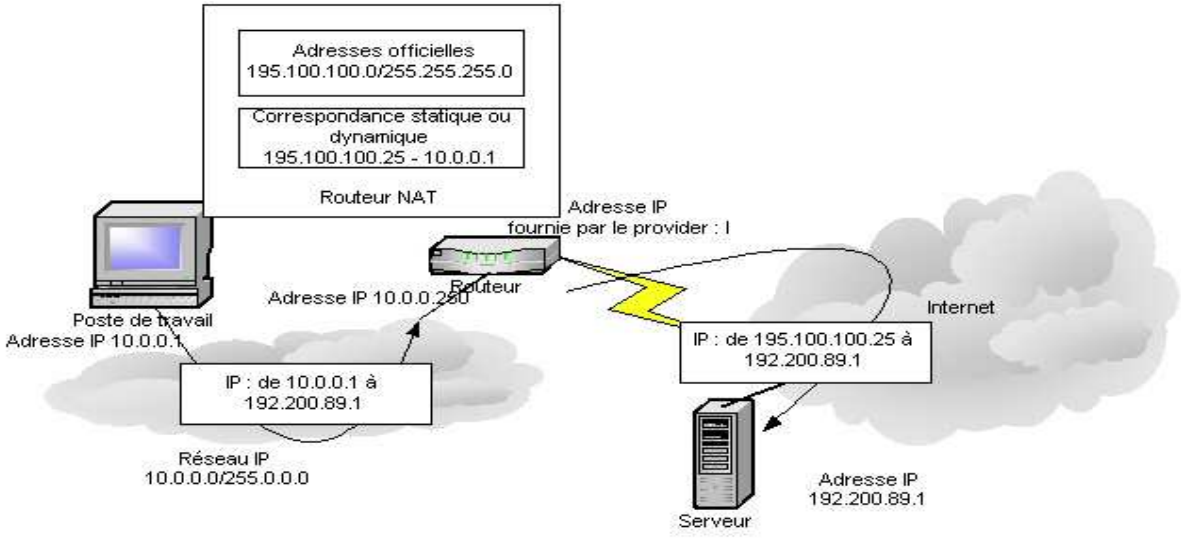
Libération lors de la fin de la connexion TCP

Pour les trafics UDP en mode requête réponse

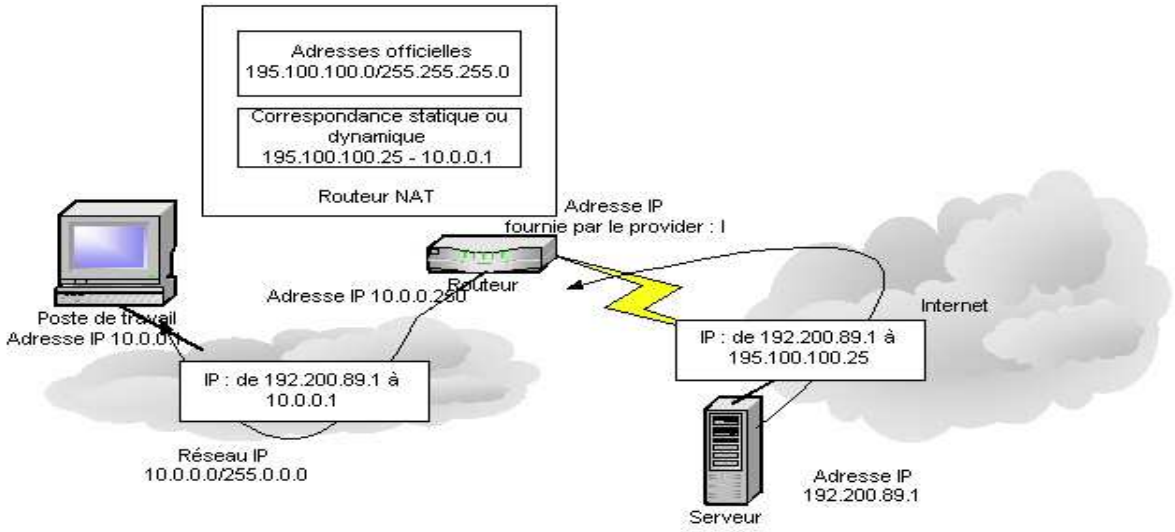
Association lors de la requête

Libération lors de la réponse ou par timeout

Transferts des paquets IP



Transferts des paquets IP



Connexion par un PAT

- PAT : Port and Address Translation
  - Technique utilisée par les routeurs ADSL

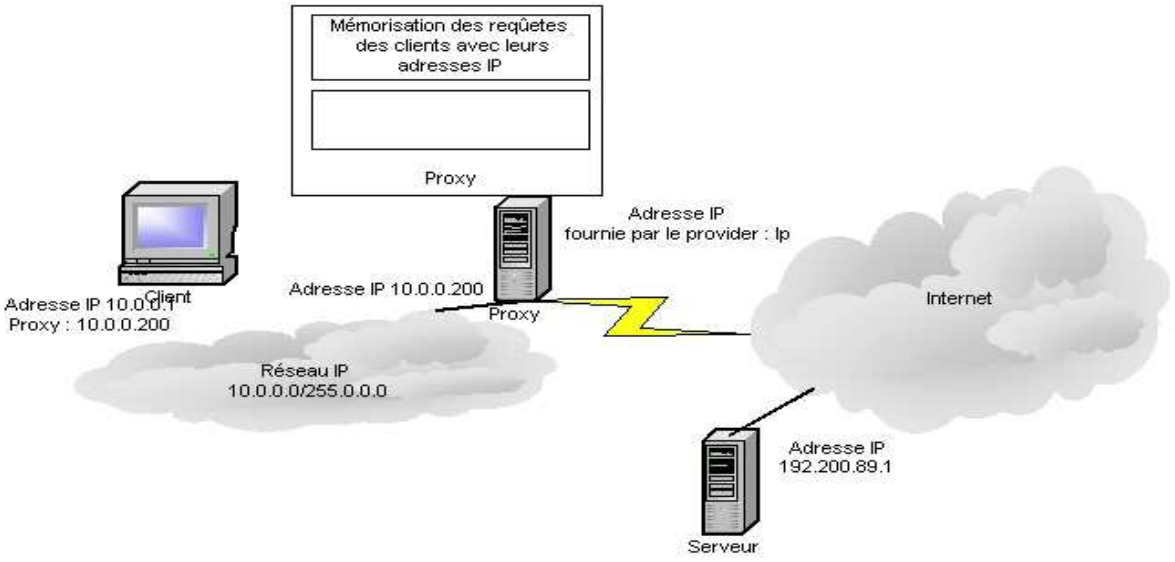
- Le routeur ADSL change le numéro de port utilisé par un autre numéro qui désignera ainsi sans ambiguités l'équipement interne

Une seule adresse utilisée

NAT et PAT

- Quelques points critiques
  - Performance du NAT/PAT
  - Accessibilité depuis l'extérieur
  - Assignation dynamique d'adresses IP
  - Problèmes avec IPsec

Connexion par un Proxy



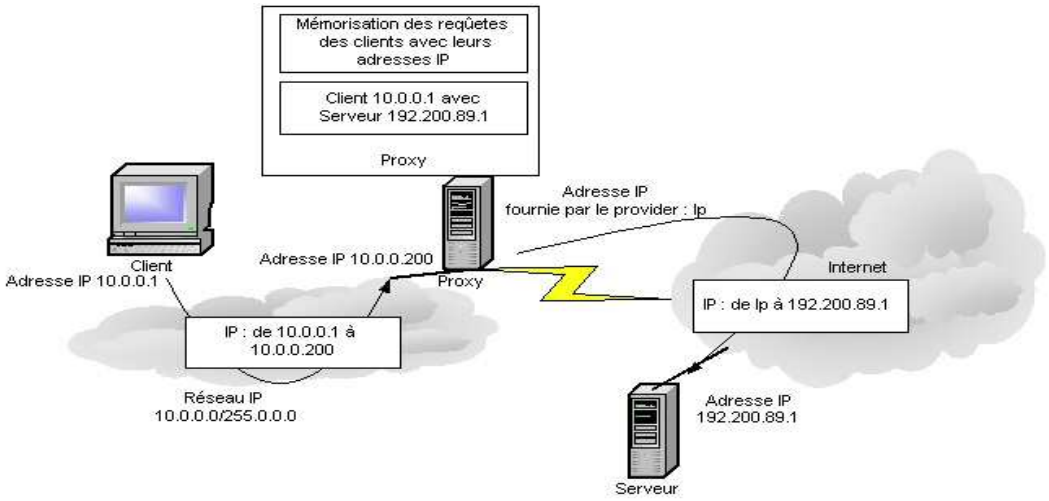
Considérons une connexion permanente à Internet via un proxy

Le réseau d'entreprise à un numéro IP privé 10.0.0.0 / 255.0.0.0

Le proxy à une adresse interne 10.0.0.200, et une adresse externe officielle fournie par le provider : Ip

Les clients internes connaissent l'adresse du proxy

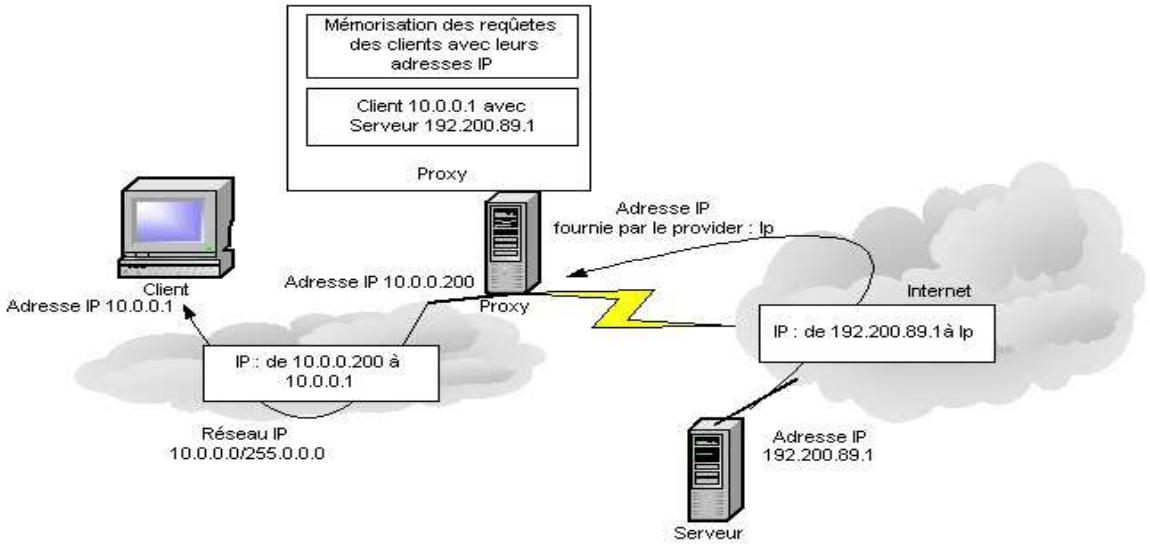
Fonctionnement du proxy



Les clients adressent leurs requêtes applicatives vers l'adresse IP du proxy ; le proxy mémorise la requête et transmet celle-ci au serveur comme si elle émanait de lui-même

Le serveur répond au proxy ; celui-ci retrouve l'origine de la requête et propage la réponse vers le client comme si elle émanait de lui-même

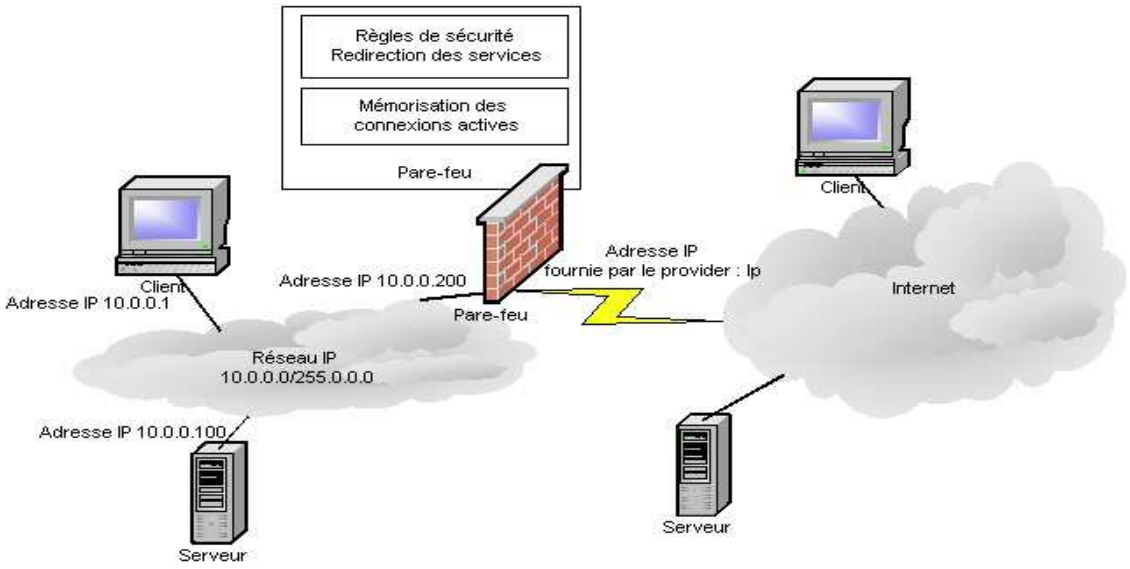
Fonctionnement du proxy



Les clients adressent leurs requêtes applicatives vers l'adresse IP du proxy ; le proxy mémorise la requête et transmet celle-ci au serveur comme si elle émanait de lui-même

Le serveur répond au proxy ; celui-ci retrouve l'origine de la requête et propage la réponse vers le client comme si elle émanait de lui-même

Connexion par un pare-feu



Un pare-feu peut être vu comme un proxy disposant de plus d'intelligence, et notamment de règles de sécurité

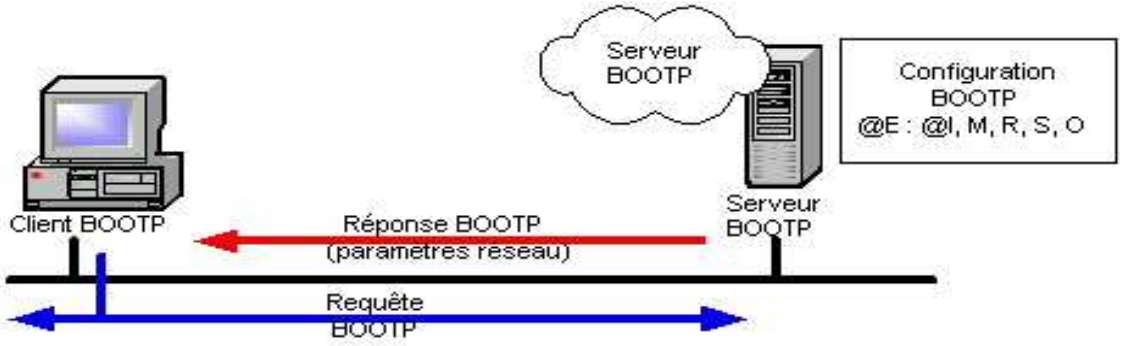
Un pare-feu peut (entre autres)

- Analyser les requêtes et réponses applicatives
- Scanner les contenus transmis
- Interdire certaines transmissions
- Rediriger des requêtes de l'extérieur vers les serveurs appropriés ; par exemple DNS, FTP, http)
- Analyser certaines connexions pour en autoriser d'autres liées

Introduction à TCP/IP

1. **Architecture TCP/IP**
2. **Adressage IP**
3. **Routage de base**
4. **Connexion à Internet**
5. **Utilisation de DHCP**

BOOTP



L'administration d'un nombre important de machines dans un environnement IP est une tâche qui peut être complexe

- Installation des machines
- Configuration des paramètres réseau (adresse IP, masque, routage)
- Définition des paramètres applicatifs (serveurs de courrier, serveurs de noms, etc.)
- Modification des configurations lors des déplacements sur d'autres réseaux

La configuration automatique des machines sous TCP/IP a été envisagée dès le début par les concepteurs de TCP/IP

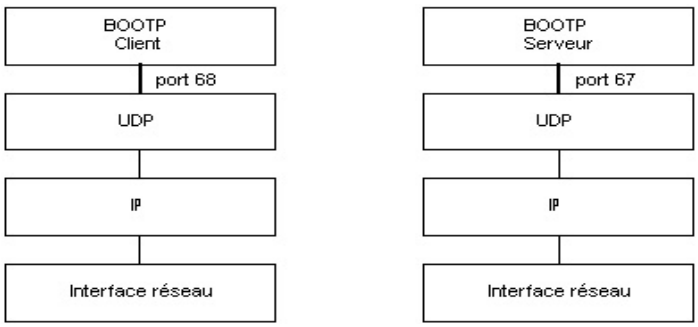
- Utilisation de BOOTP (RFC 951) permettant de récupérer au démarrage les paramètres importants
- adresse IP, masque, routeur par défaut, adresse IP d'un serveur détenant l'OS, nom de l'OS

Fonctionnement

- Un serveur BOOTP, avec un fichier de configuration décrivant pour chaque client, identifié par son adresse Ethernet, l'adresse IP, le masque, le routeur par défaut, le serveur détenant l'OS, et le nom de l'OS

BOOTP

- Architecture du service BOOTP



- Transferts

En-tête Ethernet @Dest : FF FF FF FF FF FF	En-tête IP @Dest : 255.255.255.255	En-têteUDP Port Dest : 67	Requête BOOTP (paramètres)
En-tête Ethernet @Dest : @Client BOOTP	En-tête IP @Dest : @IP proposée	En-têteUDP Port Dest : 68	Réponse BOOTP (paramètres)

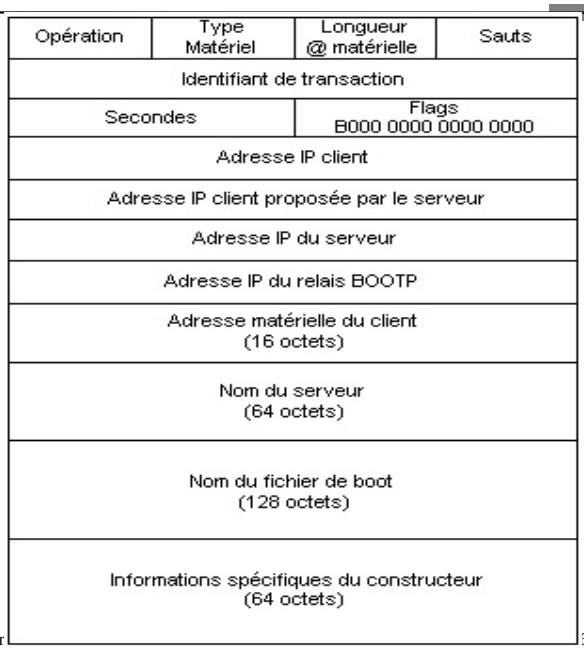
Notes

1. Les paramètres, à part l'adresse IP, sont optionnels

2. Le serveur BOOTP ne fournit pas l'OS, mais l'adresse IP du serveur qui le détient et le nom du fichier le contenant ; le transfert effectif se fait par TFTP

BOOTP

- Format des messages : requête et réponse



Opération : 0 (requête) ou 1 (réponse)

Type de matériel :

- 1: Ethernet 10 Mbps
- 6: Réseaux IEEE 8027ARCNet
- 15: Frame Relay
- 16: ATM
- 17: HDLC
- 18: Fibre Channel
- 19: ATM
- 20: Liaison série

Sauts : en cas de relais BOOTP

Identifiant de transaction : corrèle requête et réponse

Secondes : en cas de relais BOOTP

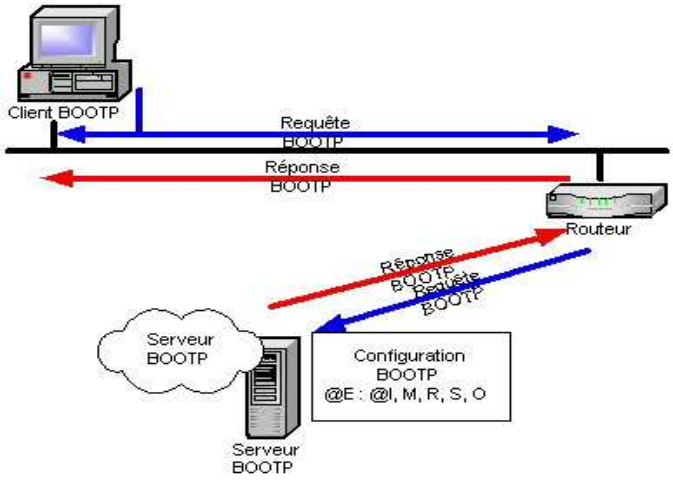
Flags : B=1 implique une réponse en diffusion

Adresse IP client : proposée par le client dans la requête

Adresse IP du relais BOOTP : en cas de relais BOOTP

Utilisation de relais BOOTP

- Messages transmis en diffusion physique
  - Retransmission nécessaire vers serveur distant



TRMv2.2

2-67

La requête BOOTP étant transmises par diffusion, elle ne peut franchir les routeurs

Si un ou plusieurs routeurs séparent le client BOOTP du serveur BOOTP, le système ne fonctionne pas

D'où obligation de disposer d'un serveur BOOTP par réseau !

Un relais BOOTP est une machine IP (généralement un routeur) qui capture les requêtes BOOTP dont le champ Adresse IP du relais BOOTP est à la valeur 0.0.0.0

Ceci indique que cette requête n'a pas été manipulée par un relais BOOTP

Le relais y insère l'adresse IP de l'interface sur laquelle cette requête a été capturée

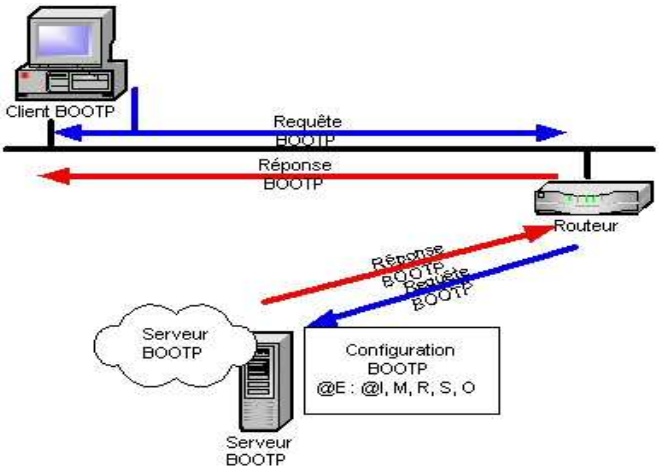
Le relais envoie cette requête à l'adresse IP d'un serveur BOOTP

Il doit connaître au moins une adresse IP de serveur BOOTP

Historiquement, relais par diffusion possible (limitation du nombre de retransmission par le champ Sauts)

Utilisation de relais BOOTP

- Identification du réseau du client par l'adresse IP du relais
  - Transmission de la réponse au relais



TRMv2.2

2-68

Le serveur BOOTP note quelle adresse se trouve dans le champ Adresse IP du relais BOOTP

Si elle est à 0.0.0.0, le client se trouve sur le même réseau et est accessible directement : la réponse est envoyée sur le réseau local

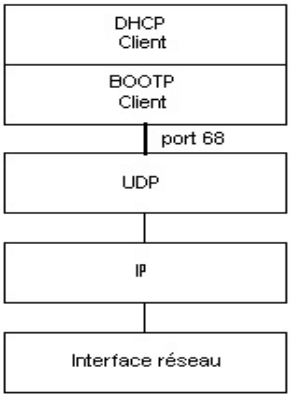
Sinon, la réponse est envoyée à l'adresse du relais BOOTP

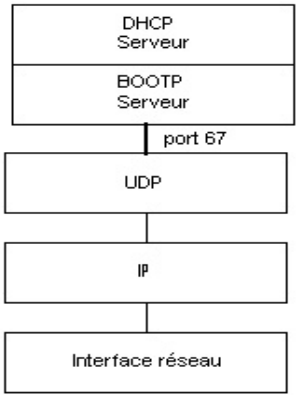
Celui-ci propage la réponse vers le client

La réponse est retardée de la valeur du champ Secondes

DHCP : sur ensemble de BOOTP

- DHCP (RFC 1531) s'appuie sur BOOTP





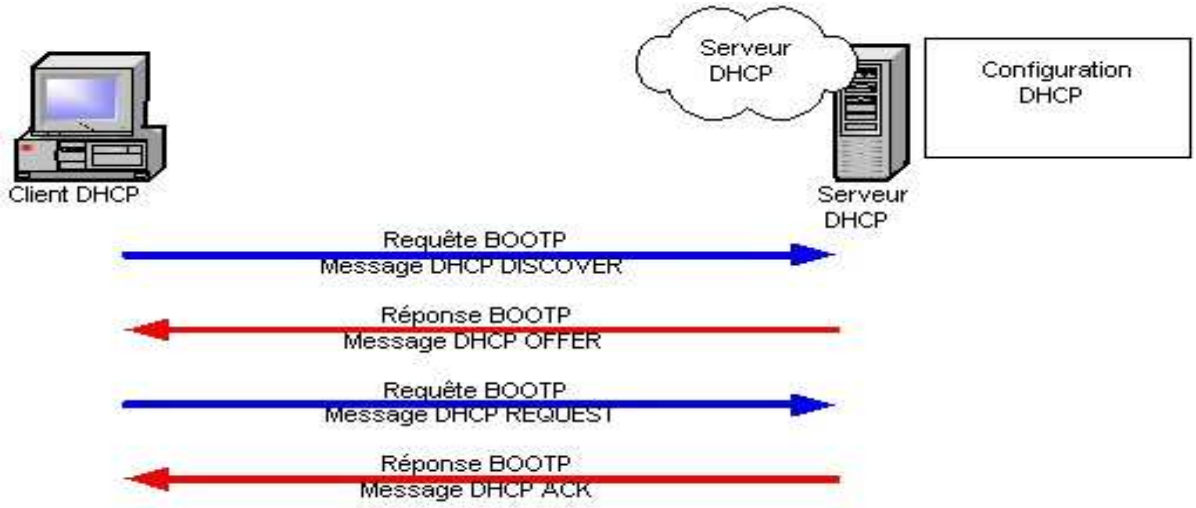
Opération	Type Matériel	Longueur @ matérielle	Sauts
Identifiant de transaction			
Secondes		Flags B000 0000 0000 0000	
Adresse IP client			
Adresse IP client proposée par le serveur			
Adresse IP du serveur			
Adresse IP du relais BOOTP			
Adresse matérielle du client (16 octets)			
Nom du serveur (64 octets)			
Nom du fichier de boot (128 octets)			
Message DHCP (64 octets)			

Utilisation du champ « Informations spécifiques du constructeur » pour contenir des messages DHCP

Utilisation des requêtes et réponses BOOTP pour le dialogue entre client et serveur DHCP

Utilisation implicite des relais BOOTP

DHCP : Fonctionnement



Le message DHCP DISCOVER sert à découvrir le serveur DHCP du réseau

Relais éventuel jusqu'à un ou plusieurs serveurs DHCP

Le serveur choisit une adresse IP et les paramètres associés et offre au client l'utilisation de ces paramètres par le message DHCP OFFER

Si plusieurs serveurs DHCP existent, chacun fait une offre

Le client DHCP sélectionne l'offre la plus adaptée (en général, la première reçue) et accepte l'offre par le message DHCP REQUEST

Optionnellement, il refuse explicitement les autres offres

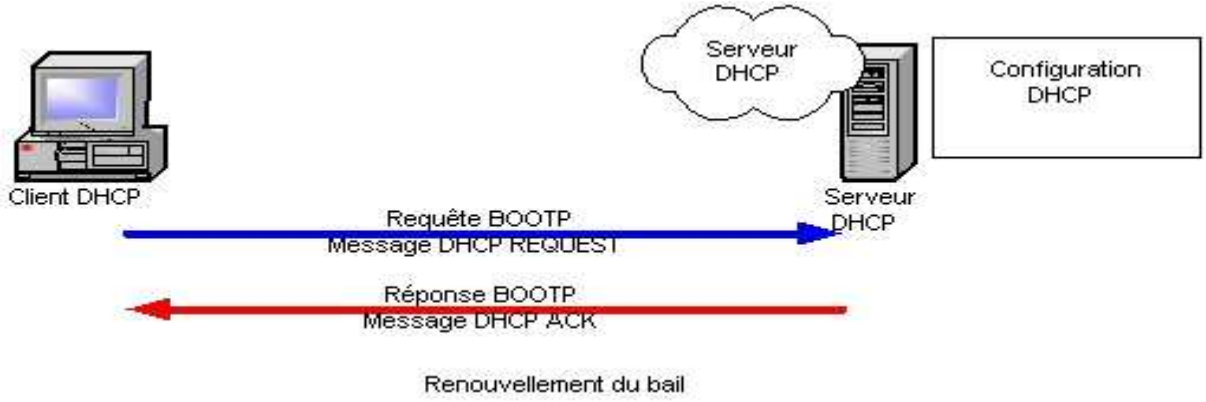
Le serveur DHCP note que l'adresse est à présent « liée » à ce client DHCP (à son adresse Ethernet) et confirme l'offre par un message DHCP ACK

L'adresse IP allouée par le serveur peut être :

Fixe : le serveur est configuré pour n'allouer cette adresse IP qu'à ce client DHCP, identifié sans ambiguïté par son adresse MAC

Dynamique : le serveur alloue cette adresse prise dans un « pool » d'adresses allouables, pour une durée déterminée par le serveur ; cette adresse est allouée pour un bail qui devra éventuellement être renouvelé par le client à échéance

Renouvellement de bail



La durée du bail est déterminée selon les mécanismes suivants

- Le serveur est configuré pour allouer des adresses pour des durées comprises entre Dmin et Dmax, et possède une durée par défaut Ddéf
- Le client propose une durée de bail de son choix
- Le serveur accepte celle-ci si elle se situe dans l'intervalle [Dmin, Dmax] ; sinon, il alloue l'adresse pour la durée Ddéf

Le délai de renouvellement (Renewal Time) est fixé par défaut à la moitié de la durée du bail (Rebind Time) ; à échéance de cette durée, le client DHCP renouvelle son bail.

En cas d'échecs, le client tentera, à 7/8 de la durée du bail, de renouveler le bail avec n'importe quel serveur DHCP (diffusion sur l'adresse IP 255.255.255.255)

En cas d'échecs sur cette tentative, il devra recommencer le cycle complet (DHCP DISCOVER, DHCP OFFER, DHCP REQUEST, et DHCP ACK)

Démonstration : Serveur DHCP

- Création des portées DHCP
  - Une par sous réseau
    - Intervalle d'adresse
    - Masque
    - Routeur par défaut
  - Un paramètre global
    - Nom de domaine
    - Adresse du serveur DNS

Exercice : DHCP

- Configuration du poste en client DHCP
  - Via l'interface graphique
- Capture avec Ethereal de la séquence DHCP
  - Analyse des trames
- Annulation/renouvellement du bail
  - Analyse des trames

Activer une capture Ethereal avec le filtre suivant

eth.addr==AdresseEthernet && bootp

Que pensez vous de ce filtre ?

A l'aide de votre interface graphique de configuration réseau, paramétrer le poste en tant que client DHCP :

Obtenir une adresse IP dynamiquement

Obtenir les adresse de serveurs DNS automatiquement

Dans une fenêtre de commande, taper **ipconfig /all**

Si l'adresse IP est toujours 0.0.0.0, répéter la commande **ipconfig /all**

Si l'adresse n'est plus 0.0.0.0, arrêter et analyser la capture Ethereal

Messages DHCP DISCOVER, OFFER, REQUEST, ACK

Après analyse de la trace, relancer la capture Ethereal

Dans une fenêtre de commande

taper **ipconfig /release**, puis observer la trace Ethereal

taper **ipconfig /renew**, puis observer la trace Ethereal

Revue

- Dans cette partie, nous avons vu
  - L'architecture TCP/IP
  - Les adresses IP et les masques de réseaux
  - L'utilisation de routeurs
  - Comment se raccorder à Internet
  - L'utilisation de DHCP