I S C A E

Réseaux et Télécommunications

« Technologies de l'Internet »

Partie 1

2012 - 2013

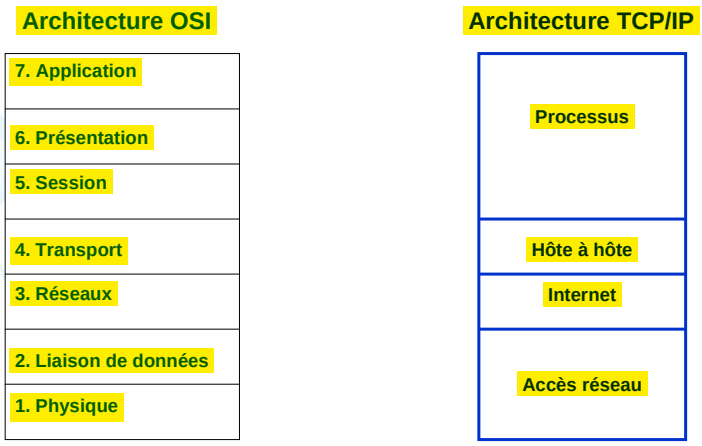
Saadbouh O CHEIKH EL MEHDI

Plan

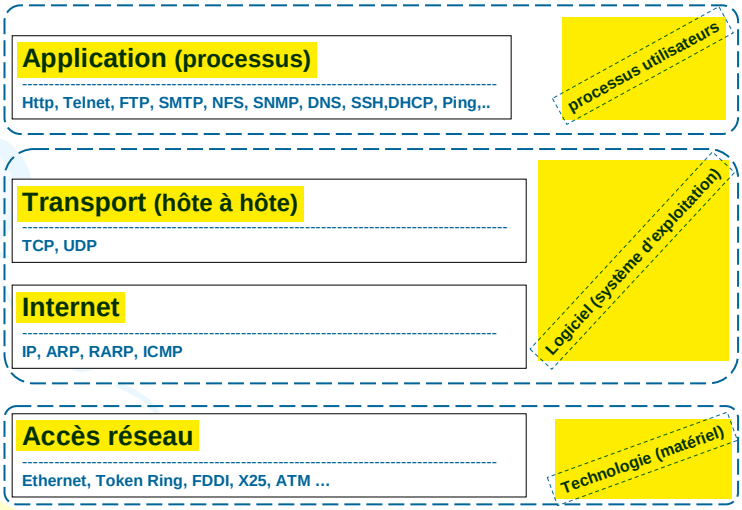
(Première partie du cours)

1- Vue d'ensemble des technologies IPv4

Architecture TCP/IP



Architecture TCP/IP



Couche Internet

IP (Internet Protocole)

- issu des travaux du Department of Defense (DoD) sur ARPANET
- protocole d'interconnexion de réseaux correspondant à la couche 3 (réseau) du modèle OSI
- opère par routage de paquets
- protocole réseau d'Internet, de fait le plus utilisé de la planète
- version actuelle (IPv4) définie dans la RFC 791, publiée en septembre 1981
- IPv4 souffre de limitations que devrait en partie combler IPv6, en cours de déploiement *(IPv6 sera abordé dans le cadre de ce cours très prochainement)*

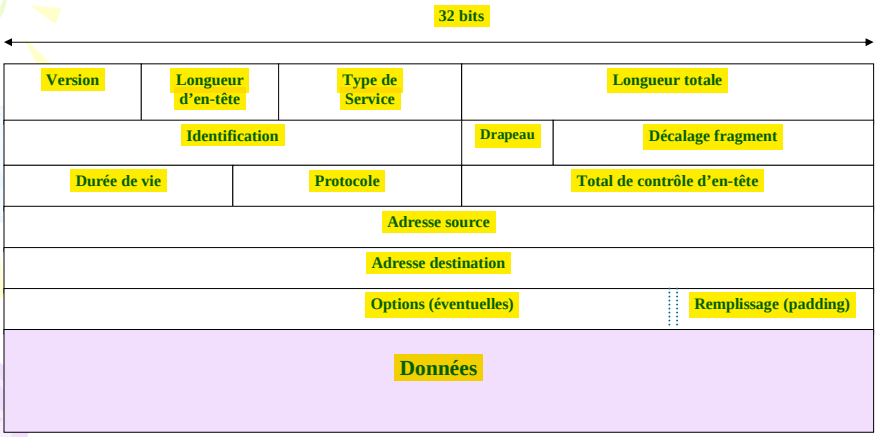
Couche Internet

IP

- rend un service non fiable en mode datagramme
- 3 fonctions élémentaires :
  1. adressage
  2. routage
  3. Fragmentation
- s'adapte aux réseaux physiques sous-jacents (fiables ou non), à leur charge utile
- a pour PDU le datagramme IP
- défini un standard d'ordonnancement des données (NetworkByte Order)

Couche Internet

Structure d'un paquet IP



Couche Internet

Description des champs

Version (4 bits) : numéro de la version du protocole utilisé pour créer le datagramme. L'objet de ce champ est la vérification que l'émetteur et le destinataire des datagrammes sont bien en phases avec la même version. Actuellement c'est la version 4 qui est principalement utilisé sur l'Internet, bien que quelques implémentations de la version 6 existent et soient déjà en expérimentation (Nous verrons un peu plus loin la version 6 d'IP)

Longueur d'en-tête (4 bits) : longueur de l'en-tête exprimée en mots de 32 bits. La taille standard de cette en-tête fait 5 mots

Type de service (8bits): Ce champ donne des indications aux équipements qu'il traverse sur son niveau de priorité et sa classe de service.

Longueur totale (16 bits): donne en octets la longueur totale du datagramme (en-tête plus données). S'il y a fragmentation, il s'agit également de la taille du fragment

Identification, Drapeau et Décalage fragment : *Ces champs sont prévus pour contrôler les fragments de datagrammes. Les données peuvent être fragmentées car les datagrammes peuvent avoir à traverser des réseaux avec des MTU plus petits que celui du premier support physique employé.*

Couche Internet

Description des champs

Identification (16 bits): permet au destinataire de savoir à quel datagramme appartient un fragment ?

Drapeau (3 bits):

- 1er **bit**: inutilisé(=0 toujours)
- 2nd **bit**: **DF** (**D**on't **F**ragment): indique si la fragmentation est autorisée(=0) ou non(=1)
- 3ème **bit**: **MF** (**M**ore **F**ragments) :(=0) il s'agit du dernier fragment, =1 y aura d'autres fragments

Décalage fragment (13 bits): indique la position du 1er octet dans le datagramme total. C'est un multiple de 8 (l'unité du est un groupe de 8 octets).

Durée de vie (8 bits) : compteur utilisé pour limiter la durée de vie des datagrammes (Son objet est d'éviter la présence de paquets fantômes circulant indéfiniment. . .)

- décrémenté à chaque saut
- détruit quand passe à 0

« Si un routeur détruit le paquet, un message d'erreur -ICMP- est renvoyé à l'émetteur avec l'indication du routeur. »

Protocole (8bits): Ce champ codé sur un octet, identifie le protocole de niveau supérieur transporté dans le champ de données du paquet IP (ICMP=1, IGMP=2,TCP=6, UDP=17, OSPF= 89,…etc.).

Couche Internet

Description des champs

Total de contrôle d'en-tête: (16 bits): ce champ contient une valeur codée sur 16 bits qui permet de contrôler l'intégrité de l'en-tête « **uniquement l'en- tête** » afin de déterminer si celui-ci n'a pas été altéré pendant la transmission. La somme de contrôle est le complément à un de tous les mots de 16 bits de l'en-tête (champ *total de contrôle* exclu), doit être recalculé dès qu'une valeur change (Par ex: durée de vie ! Donc dans chaque routeur traversé!)

Options : Ce champ est facultatif et de longueur variable. Les options concernent essentiellement des fonctionnalités de mise au point. Toutes les options sont contrôlées par un octet, généralement divisé en trois champs :un drapeau de **copie** sur un bit, une **classe** d'options sur deux bits et un **numéro d'option** sur cinq bits.

Copie (1)	Classe (2)	Numéro (5)	Paramètres éventuels

copie :

- **0**: l'option doit être copiée sur le premier fragment mais pas sur les suivants.
- **1**: impose à une passerelle de recopier le champ options dans tous les fragments

Classe:

- 0 : datagramme ou supervision réseau
- 2 : mesures et mise au point
- 1, 3 : réservés

Numéro: Signification de l'action. Par exemple, pour la classe 0 :

- **0** : fin de la liste des options, **3** : routage approximatif, **7** : enregistrement de la route **9** : routage exact

Remplissage (padding): rempli de **0** de manière à aligner le début des données sur un multiple de 32 bits

Couche Internet

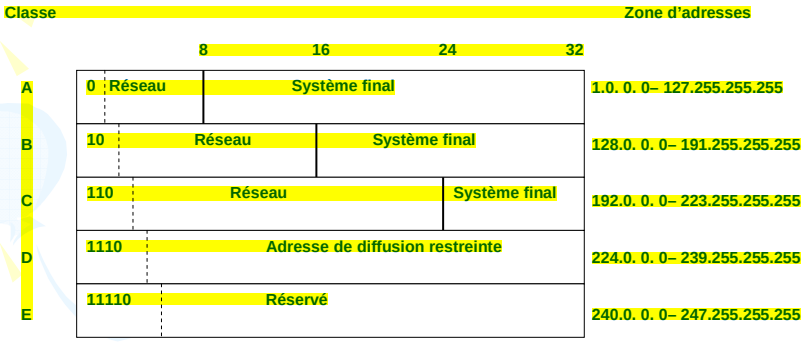
Les adresses IP

- **adresse unique** dans le monde (si elle est publique)
- **4 octets** :
  - représentés en décimal
  - séparés par des points
  - premier(**s**) octet(**s**) : numéro de réseau
  - dernier(**s**) octet(**s**) : adresse locale de l'entité sur le réseau
- **Deux types**:
  - Les adresses privées que tout administrateur de réseau peut s'attribuer librement, mais à condition qu'il ne cherche pas à les router sur l'Internet
  - Les adresses publiques délivrées par une structure mondiale qui en assure l'unicité. Ce dernier point est capital pour assurer l'efficience du routage
  - Les adresses de réseaux privées (RFC 1918)

10.0.0.0 - 10.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 - 192.168.255.255

Couche Internet

Classes d'adresses



Les classes d'adresses **A**, **B** et **C** comprennent une partie réseau respectivement de 7, 14 et 21 bits et un identifiant de système terminal de 24, 16 et 8 bits. L'appartenance à l'une de ces classes est déterminée par les premiers bits (forts) de l'adresse.

Couche Internet

Adresse IP et Masque

- Chaque adresse IP est composée de deux parties:
  - Partie pour identifier le réseau
  - Partie pour identifier la machine sur le réseau
- Dans une adresse, quelle est la partie réseau et quelle est la partie machine **?**
  - On utilise le Masque
- Le Masque (comme l'adresse IP) est une suite de 4 octets (32 bits)
- Pour connaître le numéro du réseau: l'opération logique R= (@IP) AND (Masque)
  - AND étant l'opérateur logique « ET »
- Exemple : @ IP =192.178.16.66, Masque =255.255.255.192
  - Numéro réseau = 64 (l'@ réseau =192.178.16.64)
  - Numéro machine = 2

Couche Internet

Adresse sans classe

- L'utilisation de classes a conduit à un « gaspillage » d'adresses (*notamment avec la forte croissance du nombre de réseaux connectés sur Internet*)
- Des techniques visant à une meilleure utilisation de l'espace d'adressage disponible ont été développées (*En attendant l'achèvement et le déploiement d'IPv6 avec ses adresses sur 16 octets*)
  - L'idée fondamentale est de permettre que la limite entre le préfixe réseau et l'identifiant du système terminal soit placé à n'importe quelle position de bit, au lieu de ne l'autoriser qu'aux trois positions prévues par les classes d'adresses A, B et C.
- On utilise actuellement sur Internet le système **CIDR** (**C**lassless **I**nter- **D**omain **R**outing ou encore routage Internet sans classe) défini dans [RFC 1518] et [RFC 1519].
  - Les préfixes réseau peuvent avoir une longueur quelconque !
  - L'information sur la longueur de l'identifiant du réseau ne peut plus être déterminée à partir des premiers bits de l'adresse
  - Cette information doit être transmise en utilisant une notation spéciale:
    - Le nombre de bits correspondant au préfixe du réseau est indiqué sous forme d'un nombre décimal, séparé de l'adresse par une barre oblique. Ainsi, l'adresse 192.168.152.0/19 désigne un réseau dont le préfixe est représenté par les 19 premiers bits de l'adresse IP.

    (Nous verrons plus tard et en détail le système CIDR)

Couche Internet

Fragmentation IP - MTU

La couche de liaison (Couche 2) impose une taille limite, le "**M**aximum **T**ransfer **U**nit ".

- Par exemple cette valeur est de 1500 pour une trame Ethernet

Si la couche IP doit transmettre un bloc de données de taille supérieure au MTU à employer, il y a fragmentation !

- Par exemple: un bloc de 1481 octets de données sur Ethernet sera décomposé en un datagramme de 1480 (1480+20 =1500) et un datagramme de 1 octet (1+20=21)! (20 étant l'en-tête IP)
- *Attention*: Si le bit DF du champ drapeau (dans l'en-tête du paquet IP)=1, pas de fragmentation ! Dans ce cas, la couche émettrice est tenue au courant par un message ICMP

Quand un datagramme est fragmenté, il n'est réassemblé que par la couche IP destinatrice finale. Cela implique trois remarques :

1. La taille des datagrammes reçus par le destinataire final est directement dépendante du plus petit MTU rencontré.
2. Les fragments deviennent des datagrammes à part entière.
3. Rien ne s'oppose à ce qu'un fragment soit à nouveau fragmenté.

Couche Internet

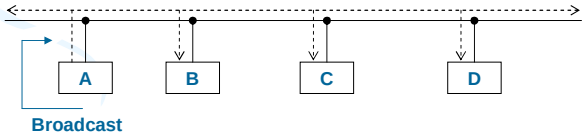
Protocole ARP

ARP " **A**ddress **R**esolution **P**rotocol "**:** définie dans la RFC 826.

Problème à résoudre : Trouver une adresse MAC à partir d'une adresse IP **?**
(l'adresse IP n'a de sens que pour la suite de protocole TCP/IP ; celle-ci étant indépendante de la partie matérielle, il faut avoir donc un moyen d'établir un lien entre ces deux constituants)

Fonctionnement :

A demande à toutes les stations : étant donné l'adresse IP de **C**, que vaut son adresse physique ?

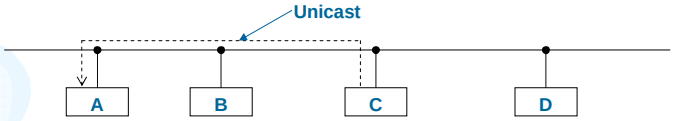


A *diffuse, sur l'ensemble des machines actives, un datagramme de format ARP (une requête ARP)*

Couche Internet

Protocole ARP

C répond directement à **A** en lui communiquant son adresse physique



C *envoie directement à* **A** *, un datagramme de format ARP (une réponse ARP)*

- Si la station **C** ne répond pas, la station **A** continuera à poser la question à intervalles réguliers pendant un temps infini. . .
- Il n'y a pas besoin d'utiliser ARP préalablement à chaque échange, car le résultat est mémorisé (Cache ARP).
- Les datagrammes ARP ne sont pas routables (requêtes et réponses ne traversent pas les routeurs)
- En générale la durée de vie d'une adresse en mémoire est de l'ordre de 20 minutes et chaque utilisation remet à jour ce compteur.

Couche Internet

Format de datagramme ARP

Les requêtes et les réponses ARP ont une structure identique. Elles sont différenciées par le champ opération. Cette structure est la suivante :

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Type de réseau																Type d'adresse de protocole															
Long adr Phys								Long adr Proto								Opération															
Adr Phys Emetteur [octets 0 à 3]																															
Adr Phys Emetteur [octets 4 à 5]																Adr IP Emetteur [octets 0 à 1]															
Adr IP Emetteur [octets 2 à 3]																Adr Phys Récepteur [octets 0 à 1]															
Adr Phys Récepteur [octets 2 à 5]																															
Adr IP Récepteur [octets 0 à 3]																															

Couche Internet

Format de datagramme ARP

Type de réseau: spécifie le protocole de la couche 2 utilisé (réseau physique).
- Par exemple: **1** pour Ethernet.

Type d'adresse de protocole: spécifie le protocole de la couche 3 utilisé,
- Par exemple: **0x08 00** pour IPv4.

Long adr Phys: spécifie la longueur, en octets, de l'adresse de la couche 2 pour le protocole utilisé.
- Par exemple : **6** pour Ethernet .

Long adr Proto :spécifie la longueur, en octets, de l'adresse de la couche 3 pour le protocole utilisé.
- Par exemple : **4** pour IPv4

Opération: indique le type de l'unité de données de protocole ARP :
1 = requête ARP, **2** = réponse ARP
3 = requête RARP, **4** = réponse RARP

Adresse Phys Émetteur
Adresse IP Émetteur
Adresse Phys Récepteur
Adresse IP Récepteur

RARP *(**R**everse **A**ddress **R**esolution **P**rotocol):* fournit l'adresse IP correspondant à une adresse physique donnée. Requête/réponse RARP (même format que ARP)

Couche Internet

Optimisations d'ARP

Cache (mémoire temporaire) ARP :

- contient une liste d'associations « adresse MAC, adresse IP »
- permet d'éviter d'émettre une nouvelle requête lorsque l'association a déjà été obtenue
- chaque association a une durée de vie limitée (environ 20 minutes)
- chaque fois qu'une association est confirmée, sa durée de vie est remise à 20 min
- les associations dont la durée de vie expire sont supprimées

Traitement de la requête :

- les requêtes étant envoyées en broadcast, toutes les stations les traitent
- or elles incluent l'adresse MAC et l'adresse IP de l'émetteur
- en recevant une requête, les stations mettent a jour leur cache avec les infos sur l'émetteur

La commande **arp - a** permet d'avoir le contenu du cache ARP de la machine sur laquelle on se trouve,

Couche Internet

Le protocole ICMP

ICMP " **I**nternet **C**ontrol **M**essage **P**rotocol " : défini dans la RFC 950

Fonctions:

1. Rendre compte des erreurs qui ont pu être détectées pendant les communications de TCP/IP.
   - aussi bien au niveau réseau (IP) qu'au niveau transport (UDP ou TCP)

   La règle générale « en Internet » est qu'en cas d'erreur un message ICMP est envoyé à l'émetteur initial du message.

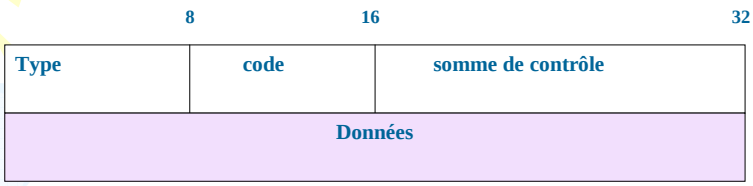
2. Fournir des messages de contrôle du réseau pour
   - tester l'accessibilité à un hôte,
   - des fins de configuration

Remarques:

1. Les messages **ICMP** sont utilisés pour indiquer des erreurs d'un hôte à l'autre ou d'un hôte à une passerelle (de passerelle à passerelle, on utilise un autre protocole :**GGP** pour **G**ateway to **G**ateway **P**rotocol.)
2. **ICMP** utilise **IP** pour transporter ses messages (pourtant **ICMP** fait partie intégrante du module **IP** !)
3. Pour éviter la congestion de l'interconnexion, Un paquet **IP** contenant un message **ICMP** ne peut générer un message d'erreur **ICMP** !

Couche Internet

Format générique des messages ICMP



Description des champs

- **Type** (8 bits) : type du message (spécifie le type de message d'erreur ou de réponse)
- **Code** (8 bits) : information supplémentaire à propos du type
- **Somme de contrôle** (16 bits) : utilisé pour vérifier l'intégrité
  - Fonctionnement similaire à IP
- **Données** : spécifiques au type et au code

Couche Internet

Types des messages ICMP

Type	Message ICMP
0	Réponse à une demande d'écho
3	Destination inaccessible (Échec de connexion…)
4	Extinction de ressources (Plus de ressources suffisantes: mémoire, CPU,)
5	Redirection (Il y a une autre route meilleure pour cette destination …!)
8	Demande d'écho (envoyé par un émetteur à une destination pour tester la connectivité réseau)
11	Temps excédé (TTL) (lorsque la durée de vie d'un paquet est dépassée…!)
12	Problème paramètre paquet (quand un paramètre dans un paquet reçu pose problème …!)
13	Demande horodatage (délai d'acheminement en milliseconde …! Donc plus précision)
14	Réponse horodatage
15	Demande information (Pour découvrir le numéro de réseau sur lequel on se situe. Obsolète !)
16	Réponse information (obsolète)
17	Demande masque adresse (pour connaître le masque du réseau local)
18	Réponse masque adresse

Couche Internet

Requête et réponse d'écho (types 8 et 0)

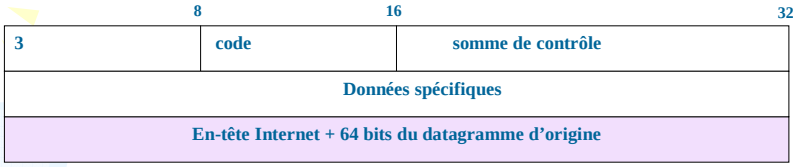
Format

Description

- Demande d'écho (type = 8) et réponse (type = 0)
- Permet à une machine ou une passerelle de déterminer la validité d'un chemin sur le réseau
- Utilisé par les outils applicatifs (utilitaires) comme **ping** ou **traceroute(ou tracert)**
- Identifiant et numéro de séquence : doivent être identiques entre la requête et la réponse (décidés lors de la requête)
- Par défaut le champ des données est vide (mais il peut contenir une quantité spécifiée par l'utilisateur de données aléatoires)

Couche Internet

Destination inaccessible (type =3)



Description

- Type = 3
- Code : indique le code de l'erreur
- Spécifique : données spécifiques au type d'erreur
- En-tête IP + 64 bits données : contient l'en-tête IP du paquet IP et les 64 premiers bits du paquet pour lequel le message est émis

Couche Internet

Codes associés au type 3

Code	Signification
0	le réseau (local du destinataire) n'est pas accessible actuellement
1	le réseau est accessible mais l'hôte n'est pas accessible actuellement
2	le protocole (TCP, UDP, etc.) n'est pas utilisable actuellement
3	le port n'est pas accessible actuellement
4	fragmentation nécessaire mais impossible à cause du flag DF
5	routage a échoué
6	Pas de route vers le réseau indiqué
7	pas de route vers l'hôte indiqué
8	machine non connectée au réseau (inutilisé)
9	communication avec le réseau interdite (le réseau est bloqué à un passerelle.)
10	communication avec la machine interdite (pas accès à l'hôte à cause de l'administration du routage)
11	réseau inaccessible pour ce service
12	machine inaccessible pour ce service
13	communication interdite (filtrage)
…	…..

Couche Internet

Extinction des ressources (types =4)

Problèmes de congestion

- Le protocole IP est un protocole en mode non connecté :
  - Pas de réservation à l'avance de la mémoire nécessaire sur les passerelles pour le routage des paquets
  - En cas de problème de mémoire, des paquets sont détruits
- Les problèmes de congestion se produisent :
  - Lorsqu'une passerelle est connectée à deux réseaux aux débits différents
  - Lorsque de nombreuses machines émettent simultanément des paquets à une passerelle

Résolution avec ICMP

- Envoi d'un message pour demander à l'émetteur de réduire le débit
- Il n'y a pas de message pour demander d'augmenter le débit :
  - La source augmente régulièrement le débit tant qu'elle ne reçoit pas de demande de limitation

Couche Internet

Programmes utilisant ICMP

Il existe différents programmes ou fonctionnalités utilisant le protocole ICMP dont essentiellement les utilitaires **ping** et **traceroute**.

ping

- Permet de vérifier la présence d'un hôte TCP/IP et de calculer le temps moyen de réponse
- Envoi d'un message ICMP d'écho et attente du message de réponse

```
C:\>ping www.google.com
Envoi d'une requête 'ping' sur www.google.com [209.85.129.104] avec 32 octets :

Réponse de 209.85.129.104 : octets=32  temps=15 ms  TTL=50
Réponse de 209.85.129.104 : octets=32  temps=15 ms  TTL=50
Réponse de 209.85.129.104 : octets=32  temps=15 ms  TTL=50
Réponse de 209.85.129.104 : octets=32  temps=15 ms  TTL=50

Statistiques ping pour 209.85.129.104:
Paquets : envoyés = 4,  reçus = 4,  perdus = 0  (perte 0%),
Durée approximative des boucles en millisecondes :
Minimum = 15ms, Maximum = 15ms, Moyenne = 15ms
```

Couche Internet

Programmes utilisant ICMP

tracert ou traceroute

Description

- Permet de calculer la route prise par des paquets IP jusqu'à une destination donnée
- Exploitation conjointe du TTL de IP et de ICMP

Principe

1. Envoyer un message ICMP vers la destination, encapsulé dans un paquet IP dont le TTL est à 1
2. Attendre le message ICMP d'erreur (TTL = 0)
3. On recommence à l'étape 1 avec un TTL + 1
4. Lorsqu'un écho est reçu, le message ICMP est arrivé à destination

Couche Internet

Services et Limitations d'IP

Ce que IP fait :

- interconnexion de réseaux
- remise de datagrammes à des hôtes (adresses IP)
- adaptation aux MTU des réseaux
- durée de vie limitée des datagrammes
- détection des erreurs sur l'en-tête
- signalisation de certaines erreurs via ICMP

Ce que IP ne fait pas (problèmes d'IP) :

- pas d'adressage des applications (client/serveur Web, client/serveur FTP, etc.)
- livraison des datagrammes non garantie
- duplication possible des datagrammes !
- déséquencement possible des datagrammes
- erreurs possibles sur les données
- pas de contrôle de flux

Couche Transport

Rôle de la couche transport

- Aller au-delà des limites d'IP
- Assurer, si possible, la correction d'erreurs :
  - signalées par ICMP
  - non signalées
- 2 protocoles de transport disponibles dans TCP/IP :
  - **UDP** : transport rapide, non connecté, permettant la multi-diffusion
  - **TCP** : transport fiable en mode connecté point-à-point
- Distinguent les applications au sein d'un même hôte
- Garantissent l'indépendance des communications

Couche Transport

Adressage des applications

Plusieurs applications réseaux peuvent s'exécuter simultanément sur la même Machine.

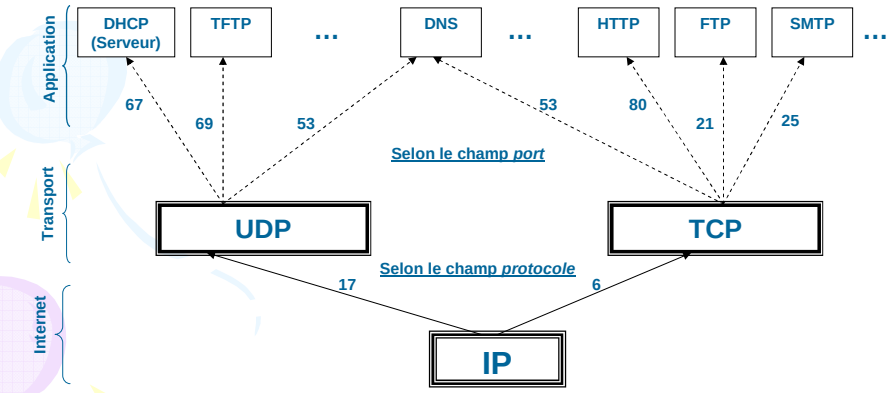
Problème : Comment un émetteur peut-il préciser à quelle application est adressé un message **?**

Solution : utilisation de destinations abstraites : les ports

- Entiers positifs sur 16 bits
- UDP et TCP fournissent chacun un ensemble de ports indépendants : le port ***n*** de UDP est indépendant du port ***n*** de TCP
- Le système permet aux applications de se voir affecter un port UDP et/ou TCP (choisi ou de manière arbitraire)
- Certains numéros de port sont réservés et correspondent à des services particuliers

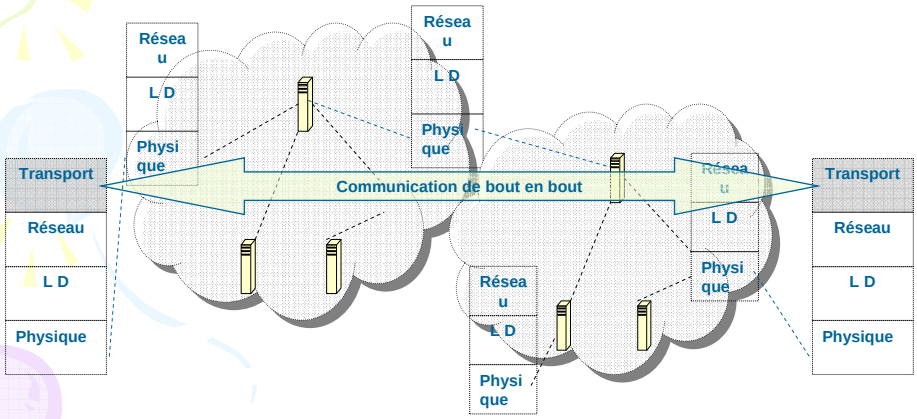
Couche Transport

Démultiplexage des ports



Couche Transport

Communication de bout en bout



La couche transport n'est concernée qu' aux extrémités

Couche Transport

Protocole UDP

« **U**ser **D**atagram **P**rotocol » RFC 768 - août 1980

- Utilise IP pour acheminer les messages d'un ordinateur à un autre
(Se contente des services offerts par la couche inférieure –IP-).

- **Service rendu :**
  - adressage des applications par numéro de port
  - multiplexage/démultiplexage par numéros de port
  - contrôle facultatif de l'intégrité des données
- **Même type de service non fiable, non connecté que IP :**
  - possibilité de perte, duplication, déséquencement de messages
  - pas de régulation de flux

Format des segments UDP

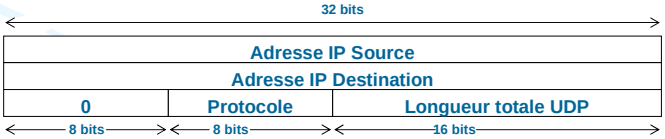
Port source	Port destination
Longueur	Somme de contrôle
Données	

Couche Transport
- En-tête UDP -

Description des champs

Port source: est un champ facultatif contenant le numéro de port de l'expéditeur, compris entre 1 et **65 535**. Si aucun numéro de port n'est spécifié, le champ est mis à 0. Ce champ est par contre nécessaire au destinataire s'il doit renvoyer des données.
Port destination: est le numéro de port sur la machine de destination.

Longueur: est la taille du datagramme, exprimée en nombre d'octets, comprenant en-tête et données. Sa valeur minimum est 8 (taille de l'en-tête UDP) alors que le datagramme UDP le plus long peut transporter **65 535 - 8 = 65 527** octets de données utiles.
Somme de contrôle : est optionnel. S'il est employé, il porte sur un pseudo en-tête constitué de la manière suivante :



Pseudo en-tête UDP

Couche Transport

- En-tête UDP -

Description des champs

Somme de contrôle (suite):

- Vérifie la totalité du datagramme + Pseudo en-tête UDP.
- Permet de s'assurer :
  - que les données sont correctes
  - que les ports sont corrects
  - que les adresses IP sont correctes
- Même calcul que IP sur tout le datagramme UDP (bourrage éventuel 1 octet à 0) + pseudo en-tête UDP
- Pseudo en-tête UDP (interaction avec IP) : (12 octets)

Données: elles sont de longueur variable

Couche Transport

Utilisation d' UDP

Le protocole UDP est utilisé dans:

- Les applications orientées transaction telles que DNS, DHCP, ..
  - Seules une requête et une réponse associée doivent être transmise, de telle sorte qu'il est inutile d'établir une connexion pour cela
- Les contextes où la rapidité de la transmission des données prédomine sur la fiabilité.
  - Les flux d'applications multimédia (flux audio, vidéo)

Couche Transport

Protocole TCP

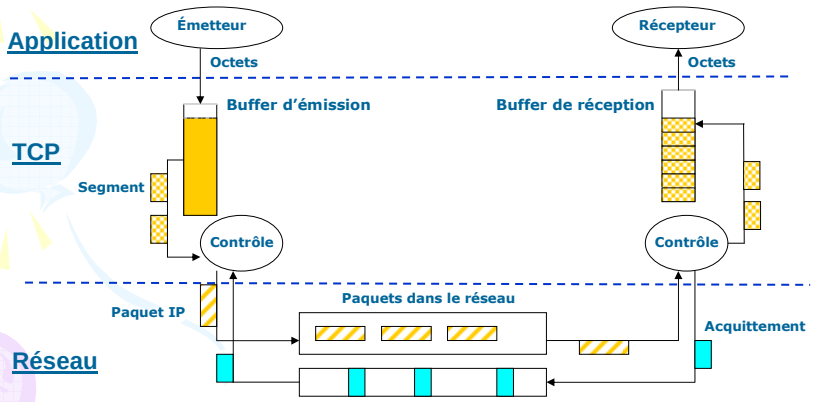
«**T**ransmission **C**ontrol **P**rotocol » RFC 793 - Septembre 1981

Transmission de données :

- Par paquets de tailles variables
- En mode connecté (3 phases:)
  - Établissement de la connexion
  - Transfert de données
  - Libération de la connexion
- Bidirectionnelle (full duplex)
- Flux non structuré de données (suite d'octets "Stream")
  - Il n'y a pas de frontière entre les bits générés par l'application source.
  - La source dépose en 'continu' ou non des flots de bits dans le buffer TCP
  - TCP extrait un certain nombre de bits consécutifs pour former un segment et l'envoie
- Fiable
  - contrôle et récupération des erreurs
  - contrôle de flux et de congestion
  - contrôle de la duplication
  - reséquencement

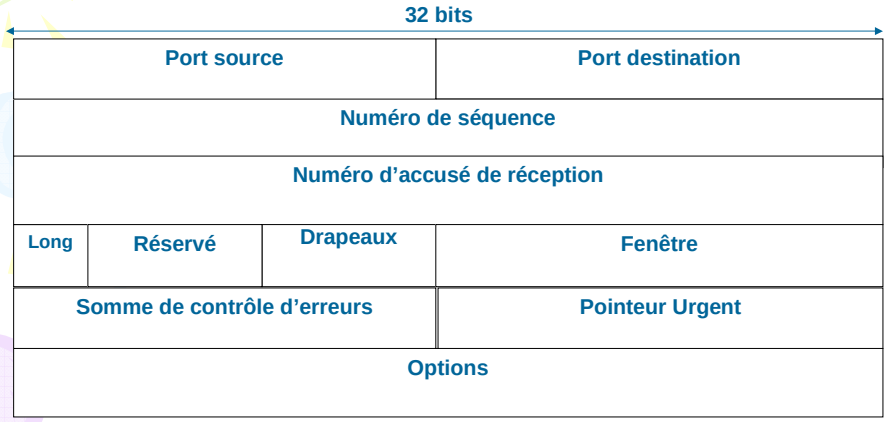
Couche Transport

Buffers de TCP



Couche Transport

Format des segments TCP



Couche Transport

L'en-tête TCP

Port source (16 bits)**:** identifie l'utilisateur TCP local, comme dans le cas UDP.
Port destination (16 bits)**:** identifie l'utilisateur TCP de la machine distante.
Numéro de séquence (32 bits)**:** indique la position du bloc en cours dans l'ensemble du message.
Numéro d'accusé de réception (32 bits)**:** : utilisé par l'expéditeur pour préciser à son correspondant le numéro de séquence qu'il attend dans le segment TCP suivant. (numéro du prochain octet attendu en provenance de l'interlocuteur)
Long (4 bits)**:** indique la longueur de l'en-tête. La valeur de ce champ est importante car le champ **options** a une longueur variable!. Lorsque le champ options est vide Long= 20
Réservé (6 bits)**:** réservé pour des utilisations ultérieures. Les 6 bits doivent être positionnés à 0.
Drapeaux (6 bits) :

- ***URG*****:** Données urgentes *(* le champ "pointeur d 'urgence" doit être exploité*)*
- ***ACK*****:** Acquittement (le champ "numéro d'accusé de réception" doit être exploité)
- ***PSH*****:** Délivrance immédiate « inutilisé»
- Pour la connexion :
  - ***RST*****:** Re-initialisation de la connexion (l'émetteur demande que la connexion TCP redémarre)
  - ***SYN*****:** Le champ « numéro de séquence » contient la valeur de début de connexion
  - ***FIN*****:** L'émetteur du segment a fini d'émettre

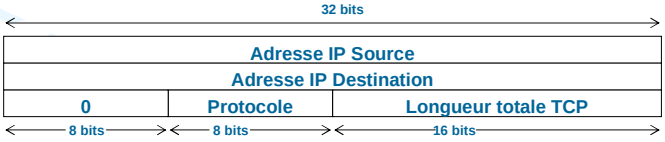
Couche Transport

L'en-tête TCP

Fenêtre (16 bits)**:** indique le nombre d'octets que le destinataire peut recevoir.
Si Fenêtre= **F** et que le segment contient un numéro d'acquittement = **A**, alors le récepteur accepte de recevoir les octets numérotés de A à A + F -1.

Somme de contrôle d'erreurs (16 bits)**:**

- Obligatoire (pas comme en UDP!)
- Vérifie la totalité du segment + Pseudo en-tête TCP.
- Comme pour UDP, permet de s'assurer :
  - que les données sont correctes
  - que les ports sont corrects
  - que les adresses IP sont correctes
- Même calcul que IP/UDP + pseudo en-tête TCP
- Pseudo en-tête TCP (interaction avec IP) : (12 octets)



Pseudo en-tête TCP

Couche Transport

L'en-tête TCP

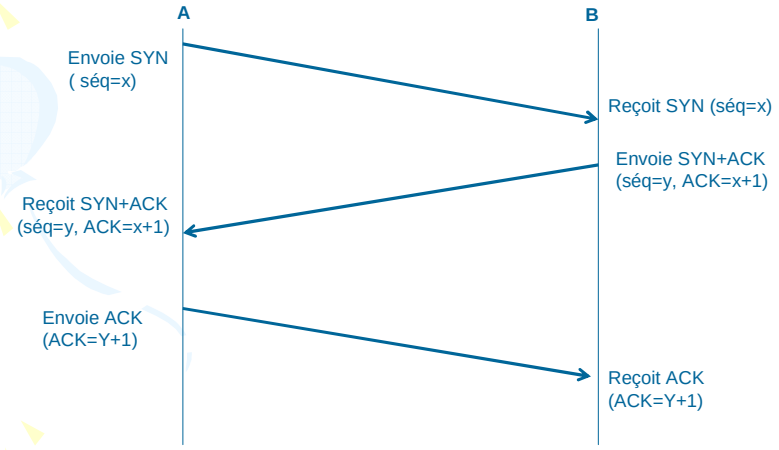
Pointeur urgent (16 bits)**:** un pointeur d'offset vers le N° de séquence marquant le début de toute Information urgente.
On n'a à tenir compte de ce champ que si le drapeau **URG** est activé (**URG =1**).

Options (taille variable) **:** options nécessitant des traitements particuliers.

Couche Transport

Établissement d'une connexion TCP

En 3 temps, avec bits **SYN** et **ACK**



Couche Application

Rôle de la couche Application

- Source et destination finales de toutes les données échangées entre utilisateurs
  - ***raisons d'être des réseaux informatiques –***
- Fournit les interfaces pour la communication entre les utilisateurs
- Spécifie les formats des messages échangées entre processus d'application
- Utilise les services de communication fournis par les protocoles de couche inférieure (TCP, UDP)

Couche Application

Classes d'applications

Grand public

- Web
- E-mail
- Messagerie instantanée
- VoIP (téléphonie)
- Vidéo conférence
- Partage de fichier
- Streaming vidéo
- …

Informatique pour informaticiens

- Utilisation de terminal distant
- Transfert de fichier
- Répertoire réseau
- Gestion de réseau
- …

Spécialisé

- Santé
- Bourse
- Météo
- …

Couche Application

Présentation de DNS

Problématique:

- Pour communiquer avec un hôte TCP/IP, il est nécessaire de connaître son adresse IP
- Comment est-il possible de récupérer l'adresse IP d'un serveur Web à partir de son adresse Web(son nom) ?
- Avant le **DNS**, utilisation d'un fichier HOSTS sur chaque machine :
  - Difficultés de mise à jour
  - Irréaliste à grande échelle

Rôle de DNS:

- Faciliter l'adressage des 'machines' sur un réseau IP
- Faire la correspondance entre un nom logique et une adresse IP

Annuaire Internet : Correspondance adresse IP et nom

Couche Application

Présentation de DNS

DNS ?!?

- **Domain Name System :** Tout un système décentralisé de gestion de noms et d'adresses (l'ensemble des organismes qui gèrent les noms de domaine).
- **Domain Name Service :** le protocole qui permet d'échanger des informations à propos des domaines.
- **Domain Name Server :** un ordinateur sur lequel fonctionne un logiciel serveur qui comprend le protocole DNS et qui peut répondre à des questions concernant un domaine.

Couche Application

Présentation de DNS

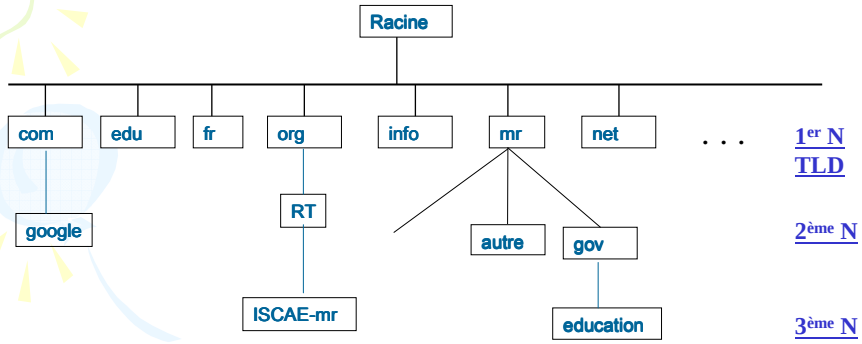
- La difficulté de DNS n'est pas au niveau des concepts qui le définissent mais au niveau de la mise en œuvre :
  - un répertoire mondial
  - des millions d'utilisateurs par jour
  - le temps d'accès doit être aussi court que possible
- Le DNS global est constitué de dizaines de milliers de bases de données (parfois dupliquées)
  - DNS = la base de données la plus répartie au monde

Pourquoi le serveur DNS n'est-il pas centralisé ?

- Maintenance
- Volume du trafic
- Accès distant à une BD centralisée
- Passage à l'échelle

Couche Application

Arborescence des domaines



Couche Application

Composants d'un Nom de Domaine

- Label
  - Chaque noeud est identifié par un label de 1 à 63 octets
    - Sauf la racine qui a un label de 0
- Nom de domaine :
  - Chemin d'un noeud vers la racine
    - Constitué par une succession de labels séparés par un "**.**"
  - Maximum de 255 octets "**.**" compris

TLD : Top- Level Domains

- Noeuds de premier niveau dans l'arbre DNS :
  - Co-supervisés par des organismes :ICANN, INTERNIC,…
- TLD génériques (gTLD) : .com, .edu, .mil, .net, .org
- TLD nationaux (ccTLD) : .mr, .fr, .ma, .it, .us,…

Couche Application

Enregistrements DNS

- La base des données de serveurs de noms est constituée « d'enregistrement de ressources » ou « Ressource Records »(RRs)
- Ces enregistrements sont répartis en classes. La seule classe d'enregistrement usuellement utilisée est la classe Internet (IN)
- A chaque nom de domaine est donc associé un RR
- Les champs d'un RR: { **Nom-Domaine TTL CLASSE TYPE RDATA** }
  - **Nom-Domaine** : nom absolu de l'espace de nommage DNS (FQDN)
  - **TTL** : durée de vie de l'objet dans les caches en secondes
  - **CLASSE** : IN pour Internet
  - **TYPE** : type de données
    - **A** : traduction nom/adresse
    - **PTR** : traduction adresse/nom
    - **CNAME** : nom canonique (nom officiel de l'hôte, des alias peuvent exister)
    - **TXT** : information libre
    - **RP** : personne responsable
    - **MX** : Mail eXchange (email associé à une adresse)
  - **RDATA** : valeur de l'objet (associée au TYPE)

Exemple

www.iscae-mr.org	**3600**	**IN**	**A**	**192.77.93.99**

Couche Application

Requête DNS

- Requête DNS, triplet de la forme : { **Nom-Domain CLASSE QTYPE** }
- QTYPE comprend les valeurs TYPE usuelles d'un RR
- La résolution d'une requête consiste à trouver l'ensemble des RR du DNS qui correspondent aux trois valeurs

Exemple

Requête : { google.com. IN A }

Réponses :

google.com.	389	IN	A	209.85.129.104
google.com.	389	IN	A	209.85.129.105
google.com.	389	IN	A	209.85.129.106

Couche Application

Hiérarchie de serveurs DNS

- Un serveur DNS ne peut avoir dans sa base une infinité d'entrées
- Lorsqu'un serveur DNS ne peut pas répondre, il interroge un autre serveur DNS
- Une requête DNS peut donc être répercutée de manière transparente sur un ensemble de serveurs
- On appelle un serveur racine un serveur qui répond aux requêtes qui concernent les noms de domaine de premier niveau (.com ou .mr)
- Actuellement 13 serveurs racines placés sous l'autorité de l'ICANN (autorité de régulation de l'Internet)
- Certains correspondent maintenant à plusieurs serveurs répartis dans différents lieux géographiques

Couche Application

Cache DNS

- Le serveur DNS garde toujours en mémoire les réponses positives de résolution de nom : l'ensemble de ces réponses est appelé le cache DNS
- Lorsque la réponse à une requête est déjà présente dans le cache, cela évite au serveur d'interroger d'autres serveurs DNS

Remarques

- Les noms de domaine ne sont pas sensibles à la casse:

  GOOGLE.COM = google.com
- Un nom de domaine ne peut être composé que des caractères alphanumérique et de trait d'union

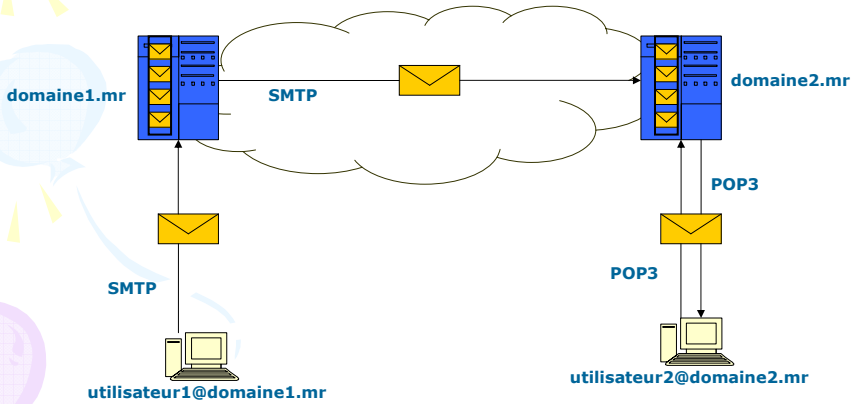
Couche Application

La messagerie

- Plus connu sous le nom Email (Electronic Mail ou Courrier électronique)
- Ce service permet d'échanger des messages et des fichiers.
- La messagerie nécessite:
  - Un serveur de messagerie et un logiciel de serveur ou MTA (Mail Transfer Agent)
  - Des BAL (boîte à lettres) sur le serveur pour chaque client géré
  - Un client de messagerie et un logiciel client ou MUA (Mail User Agent)
  - Des protocoles d'échange (SMTP, POP3, IMAP, …)

Couche Application

Messagerie électronique : Architecture générale



Couche Application

La messagerie

- **MUA** (**M**ail **U**ser **A**gent) est un client de messagerie: Agent utilisateur de messagerie, il permet de:
  - composer, éditer, lire des messages mail
  - soumettre le message mail au serveur MSA
  - Ex: Outlook, Eudora,….
- **MSA** (**M**ail **S**oumission **A**gent) est un serveur de messagerie et relais qui transfère le courrier au MTA
- **MTA** (**M**ail **T**ransfer **A**gent) est un serveur de messagerie et commutateur de courriers; Agent de transfert de courriers au serveur du destinataire MX
  - **MSA** et **MTA** sont souvent intégrés dans un seul serveur.
- **MX** (**M**ail e**X**changer) est un serveur de messagerie du destinataire qui accepte le courrier et le transfère au MDA
- **MDA** (**M**ail **D**elivery **A**gent) est un serveur de messagerie du destinataire qui délivre des messages locaux
  - **MX** et **MDA** sont souvent intégrés dans un seul serveur.

Couche Application

Messagerie - Fonctionnement

MUA : soumet le courrier électronique au serveur MSA en passant par SMTP/TCP port 25

MSA : transfère le courrier au MTA

MTA : recherche d'abord la localisation du destinataire du courrier par la technique DNS (type MX). A l'aide du retour de RR (Registre Record) – nom de hôte, MTA recherche l'adresse IP (type A). Ensuite, MTA connecte au serveur du destinataire étant un client SMTP

MX : accepte le courrier et le transmet à MDA

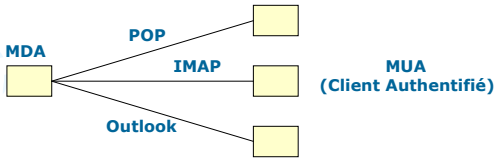
MDA : responsable de courriers locaux

- MDA enregistre les courriers en format mailbox

Couche Application

Messagerie - Fonctionnement

- Une fois un courrier est arrivé au serveur de messagerie du destinataire (serveur local), comment retirer le courrier ?
- Les protocoles de client:
  - POP (Post Office Protocol)
  - IMAP (Internet Message Access Protocol)
  - Systèmes propriétaires tels que Microsoft Exchange – Outlook, …
- Le client (MUA) doit s'authentifier pour retirer ses courriers stockés dans le serveur local. Le relevé de courriers a besoin de primitives spéciales.



Couche Application

Le serveur de messagerie

- Contient la boîte aux lettres (messages entrants de l'utilisateur)
- Contient une file d'attente de mail sortants à envoyer
- Les serveurs mail communiquent entre eux via SMTP :
  - Le serveur mail émetteur joue le rôle de client
  - Le serveur mail récepteur joue le rôle de serveur

SMTP (Simple Mail Transfer Protocol - RFC 821)

- Utilisation de TCP (port 25) (transfert fiable)
- 3 phases de transfert :
  - Établissement de la connexion
  - Transfert des messages
  - Fermeture de la connexion
- Interactions sous la forme de commandes (texte ASCII) et réponses (code d'état + phrase) → Tous les messages sont en ASCII

Couche Application

SMTP (suite)

- SMTP utilise des connexions persistantes
- Les messages SMTP sont en ASCII :
  - Fin de message par un "**.**"
- Certaines chaînes de caractères ne sont pas autorisées :
  - Nécessité de coder les messages (généralement Base64)

Couche Application

Commandes de requêtes de client SMTP

- Chaque requête (un message du protocole SMTP) correspond à une ligne de texte terminée par CRLF
- **HELO** <SP> <domaine> <CRLF>: L'ouverture de session entre le client et le serveur (le message contient le nom de domaine FQDN du client).
- **MAIL** <SP> FROM: <route-retour> <CRLF>: Définit l'adresse mail de l'émetteur (utilisé pour le retour éventuel d'erreurs).
- **RCPT** <SP> TO: <route-aller> <CRLF>: Définit l'adresse d'un destinataire (le routage du courrier est possible en donnant une liste de MTA à visiter : routage par la source @Hote_1,@ Hote_2:usager@ Hote_3)
- **DATA** <CRLF>: Définit l'enveloppe (l'entête) et le corps (le texte) du message.
- **QUIT** <CRLF>: Termine un courrier.

Couche Application

Liste des principales réponses du Serveur SMTP

220 <domaine> Service disponible
221 <domaine> Canal de transmission en cours de fermeture
250 Action de messagerie effectuée, succès
251 Utilisateur non local ; réémission vers <route-directe> (avec relais automatique)
354 Début du corps du message ; arrêt par <CRLF>.<CRLF>
421 <domaine> Service non disponible, canal en fermeture [Réponse à émettre sur tous les canaux lorsque le système exécute une séquence d'arrêt]
450 Action non effectuée : boîte aux lettres non disponible [Ex. : boîte aux lettres occupée]
451 Action arrêtée : erreur de traitement
452 Action non effectuée : manque de ressources système
500 Erreur de syntaxe, commande non reconnue [y compris des erreurs de type "ligne de commande trop longue"]
501 Erreur de syntaxe dans les paramètres ou arguments
502 Commande non implémentée
503 Mauvaise séquence de commandes
504 Paramètre de commande non implémenté
550 Action non effectuée : boîte-aux-lettres non disponible [Ex : boîte aux lettres non trouvée, pas d'accès]
551 Utilisateur non local ; essayer <route-directe> (sans relais automatique)