Couche application

Couche application

- Couche finale pour la communication
- De très nombreux protocoles
  - HTTP, FTP
  - SMTP, POP, MAP
  - DNS
  - ...
- La plupart des protocoles sont construits au dessus de TCP

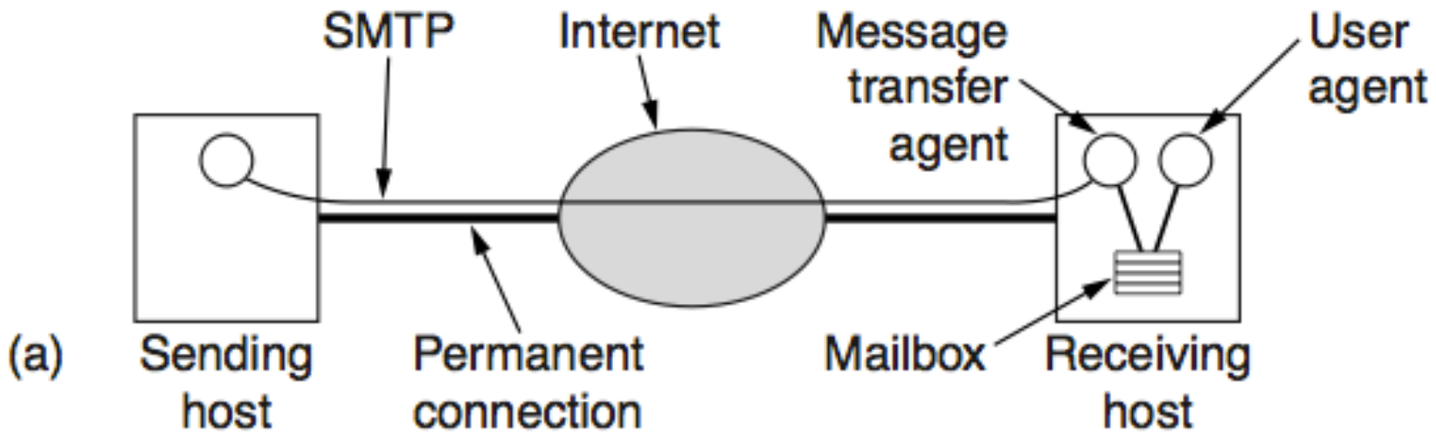
Protocole SMTP

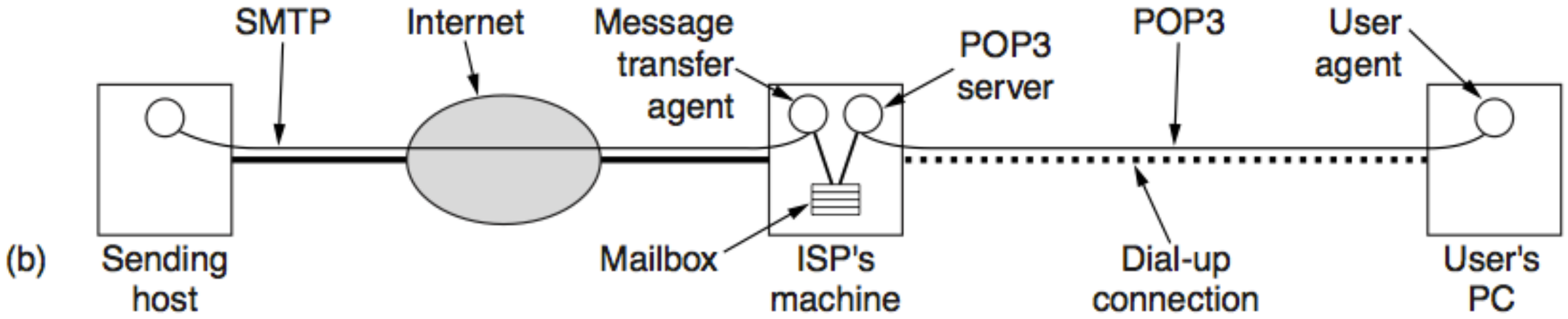
- Simple Mail Transfer Protocol
  - Envoi/transport de courrier électronique
  - RFC 821 (1982)
  - RFC 2821 (2001)
  - TCP - Port 25

Agents du courrier électronique

- MUA (Mail User Agent) : client de messagerie
- MTA (Mail Transfer Agent) : transport des courriers (via des serveurs SMTP en général)
- MDA (Mail Delivery Agent) : remise du courrier au destinataire final

Architecture du courrier électronique





POP (Post Office Protocole) : MDA
ISP (Internet Service Provider)

Exemple de transport de Courrier

- L'utilisateur clique sur «Envoyer»
- Le logiciel de messagerie (MUA) contacte le serveur SMTP local (MTA)
- Ce serveur contacte le serveur SMTP disant (MTA) associé à l'adresse du destinataire
- Celui-ci transmet le courrier au serveur POP (MDA)
- Le destinataire clique sur le bouton «Recevoir» de son logiciel de messagerie (MUA)

POP3 vs. IMAP

Caractéristiques	POP3	IMAP
RFC	1939	2060
Port TCP	110	143
Sauvegarde courriels	Machine hôte	Serveur
Lecture courriels	Off-line	On-line
Temps de connexion	Faible	Important
Usage ressources serveurs	Minimal	Extensive
Plusieurs boites courriels	Non	Oui
utilisation mobile	Non	Oui
Backs up des courriels	Utilisateur	ISP
Récupération partielles des messages	Non	Oui
Problème du quota disque	Non	Possible
Simplicité d'implémentation	Oui	Non

IMAP : Internet Message Access Protocol

Courriels et espace de noms

- Une adresse électronique identifiant@domaine.tld est constitué de :
  - identifiant local du destinataire
  - domaine.ltd
    - Nom de la machine MTA du destinataire
    - ou domaine DNS dont le champ MX (voir partie DNS) indique le MTA

Encodage et extension

- Les caractères transmis doivent être codés sur 7 bits
- Format MIME (Multipurpose Internet Mail Extension)
- Encodage base 64 ou quoted-printable

Entête d'un courrier électronique

- **From** : adresse de l'émetteur
- **Return-Path** : adresse pour la réponse (peut être différent du précédent)
- **To** : adresse(s) du (des) destinataire(s) principal(aux)
- **Cc** : adresse(s) du (des) destinataire(s) secondaire(s)
- **Subject** : sujet
- **Received** : ajouté par chaque MTA
- **MessageId** : identifiant unique
- **Date** : date d'envoi du message (par le MUA)
- **X-...** : champs officieux

Pourriel

- Le courrier électronique non sollicité (spam, pourriel) est un problème important :
  - Achat de liste de millions d'adresse
  - Coût nul de l'envoi, même massif
  - Très faible retour sur un envoi massif reste profitable

Lutte anti-pourriels

- Le MUA peut filtrer le courrier (une fois qu'il est arrivé). Au niveau des serveurs :
  - Certains serveurs refusent systématiquement les connexions en provenance de certains hôtes
    - listes noires/listes blanches
    - listes dynamiques
  - Cela n'est pas prévu dans le protocole
- Enjeu : universalité du courrier électronique

Liste grise

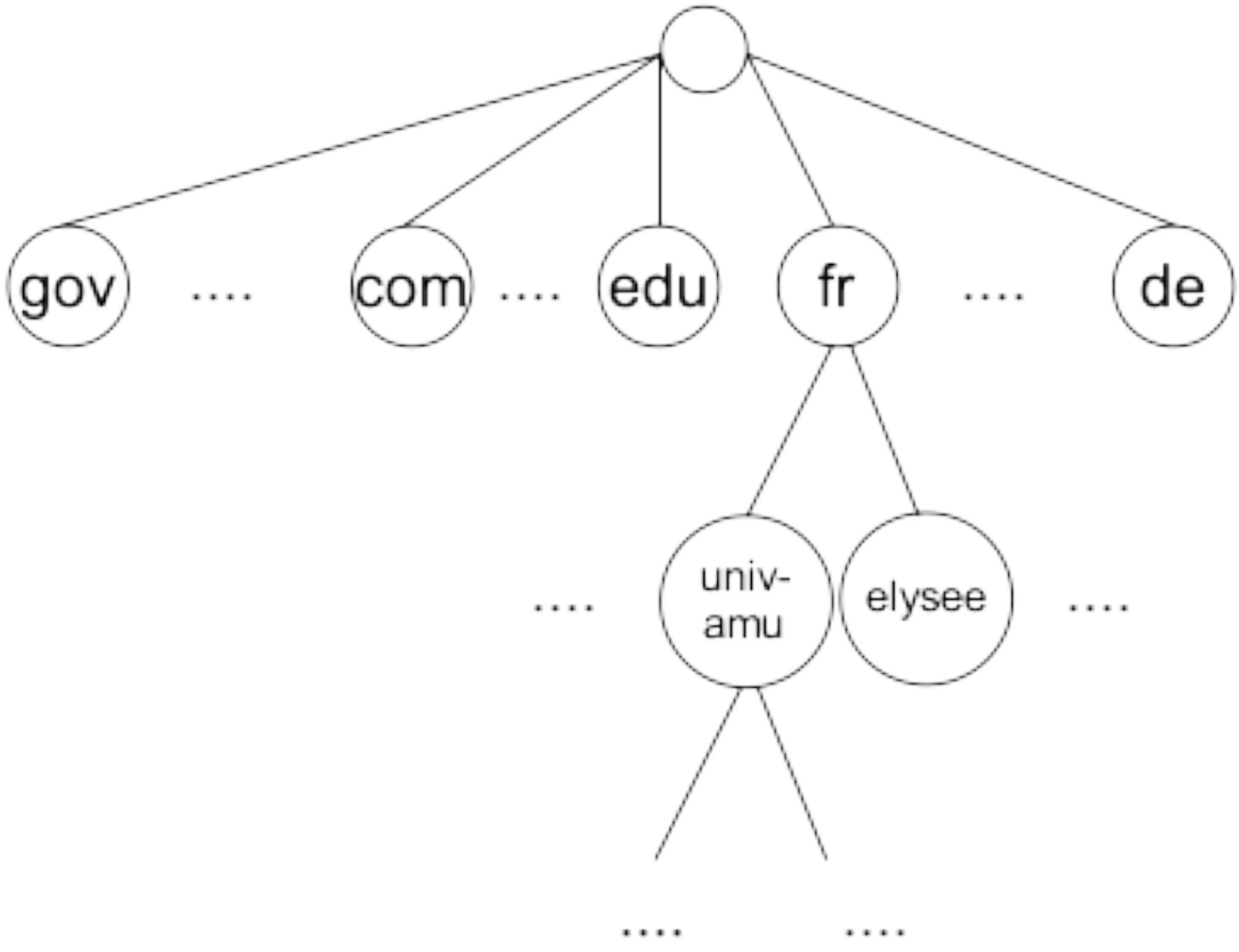
- Le serveur SMTP refuse pendant un certain temps un nouvel expéditeur donné,
- Un spammeur ne réessaie pas sur une erreur
- Un serveur «normal» réessaiera (avec succès) ultérieurement

Domain Name Server (DNS)

- Base de données hiérarchique et distribuée permettant la résolution de noms vers les adresses IPv4 et IPv6
- Hiérarchie : les noms sont structurés et forment une arborescence
- Zones : ce sont des ensembles disjoints de noms formant des sous-arbres. Chaque zone est dotée d'au moins un serveur.
- Structures de données distribuées : pour chaque zone, un ou plusieurs serveurs DNS sont chargés d'effectuer la résolution.

Domain Name Server (DNS)

Vue simplifiée



Domain Name Server (DNS)

- Le mécanisme qui permet la résolution d'un nom en une adresse IP est gérée par des serveurs de noms qui représentent une base de données distribuée des noms de domaine.
- Quand une entité a reçu l'autorité de gérer une zone elle doit maintenir au moins deux serveurs de noms : un primaire et un ou plusieurs secondaires.
- Les secondaires sont des serveurs redondants par rapport au primaire de manière à faire face à une défaillance d'un système.
- Lorsqu'une machine est ajoutée à une zone, l'administrateur de la zone doit ajouter son nom et son numéro IP sur le serveur primaire qui se reconfigure alors en fonction de ces nouvelles données.
- Quant à eux, les serveurs secondaires interrogent régulièrement (toutes les 3 heures) le primaire et font les mises à jour nécessaires en cas d'évolution de la base de données.

Domain Name Server (DNS)

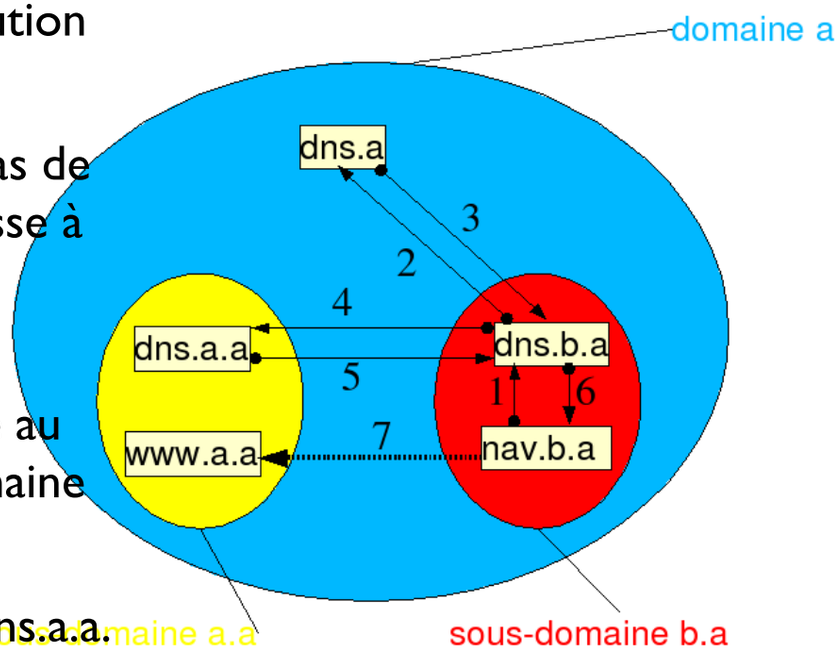
- Les serveurs de noms peuvent fonctionner en mode récursif ou non, mais ils doivent toujours implanter le mode non récursif.
  - Mode non-récursif : le serveur indique au client un autre serveur de noms qui saura lui répondre ou à son tour transmettre la requête à un autre serveur.
  - Mode récursif : c'est le serveur qui se charge de l'interrogation successive des serveurs de noms et qui retourne finalement la réponse au client.
- Lorsqu'un serveur de noms reçoit une demande, il vérifie si le nom appartient à l'un des sous-domaines qu'il gère. Si c'est le cas il traduit le nom en une adresse IP en fonction de sa base de données et renvoie la réponse au demandeur

Domain Name Server (DNS)

- Dans tous les cas, lorsqu'un serveur ne sait pas répondre il utilise l'adresse d'un serveur de nom hiérarchiquement supérieur qui connaît le nom et l'adresse IP de chaque serveur de noms pour les domaines de ses sous-niveaux.
- Ce serveur de nom supérieur renvoie alors l'adresse d'un serveur de noms à contacter.
- Et ainsi de suite, par interrogations successives de serveurs de noms (soit par le client en mode non-récursif soit par le serveur lui-même en mode récursif) le client initial obtiendra l'adresse demandée.
- Pour éviter de faire trop souvent de telles requêtes, tout serveur de noms stocke dans une mémoire cache les correspondances (numéro IP, nom de machine)

Domain Name Server (DNS)

- Résolution (en mode non récursif) du nom du serveur web www.a.a lorsque le navigateur sur la machine nav.b.a cherche à joindre ce site.
- Le navigateur envoie à son DNS dns.b.a une requête de résolution pour le nom www.a.a.
- dns.b.a ne connaissant pas cette adresse, car elle ne dépend pas de sa zone et qu'il ne l'a pas dans son cache, transmet cette adresse à dns.a puisque c'est le DNS d'autorité de niveau supérieur qu'il connaît.
- dns.a ne connaissant pas non plus l'adresse demandée, renvoie au demandeur l'adresse d'un ou plusieurs DNS pour le sous-domaine recherché a.a et auquel il a lui-même délégué son autorité.
- Le serveur dns.b.a réémet sa requête vers ce nouveau DNS dns.a.a.
- Le serveur dns.a.a connaît l'adresse demandée car la machine www.a.a appartient à sa zone et peut donc renvoyer l'adresse IP demandée à dns.b.a.
- Le DNS mémorise dans son cache la réponse et la retourne au demandeur initial : le navigateur.
- Le navigateur peut se connecter au serveur web désiré.



Enregistrements DNS

- A : indique une adresse IPv4 associée à un nom
- AAAA : idem pour IPv6
- CNAME (Cannonical Name) : alias (1 ou plusieurs) vers un autre nom.
- NS (Name Server) : indique un serveur de nom du domaine. Il en faut au moins 2 pour tolérer les défaillances
- PTR (Pointer) : pointeur vers un autre espace du domaine (résolution inverse)
- SOA : serveur principal et administrateur de la zone
- MX : MTA de courrier du domaine
- ...

Interrogation DNS : commande dig

Requête DNS

- Une requête porte un champ particulier concernant un domaine passé en paramètre.
- Le protocole UDP est utilisée, sauf si le message dépasse 512 octets. Dans ce cas, TCP est utilisé.
- Port 53
- Deux modes : récursif et non récursif
- Un champ TTL indique combien de temps la valeur d'un enregistrement peut être gardé en cache : en général de l'ordre de la journée.

Bibliographie

- Emmanuel Godard, Support Cours Réseaux, 2019