Réseaux Applicatifs - Théorie

Grégoire Roumache

Janvier 2020

1 Introduction

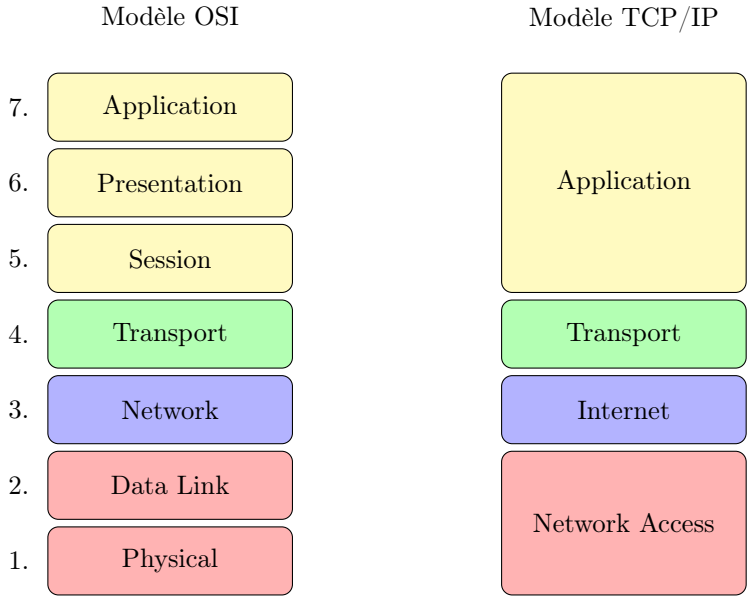
- Caractéristiques des architectures de réseaux:
  - fault tolerance (= tolérance aux pannes),
  - scalability (= capable de grandir),
  - quality of service,
  - security.
- Types de réseaux:
  - Local Area Networks (**LAN**)

    > L'appareil représentatif du LAN est le **switch** qui connecte les appareils entre eux.

  - Wide Area Networks (**WAN**)

    > L'appareil représentatif du WAN est le **routeur** qui connecte les réseaux entre eux.

  - Internet (interconnected networks) est un ensemble de réseaux interconnectés au niveau mondial.
  - Metropolitan Area Network (MAN) est un réseau de la taille d'une ville.
- Modèles OSI et TCP/IP:



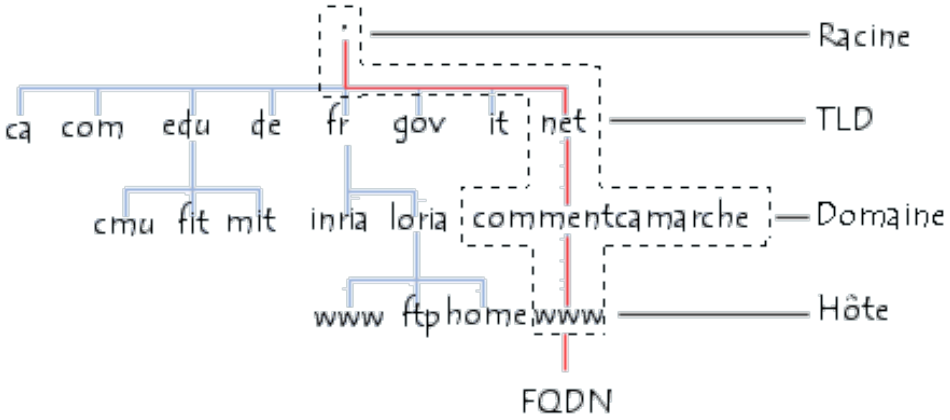
- Avantages liés à l'utilisation d'un modèle en couches:

- aide à la conception de protocole,
- favorise la concurrence,
- les changements dans une couche n'affectent pas les autres couches,
- fournit un langage commun.

2 Couche Applicative

- La couche application fournit l'interface entre les applications/utilisateurs et le réseau.
- Protocoles de résolution des noms:
  - NetBIOS (= nom d'hôte dans les réseaux Microsoft),
  - DNS (= Domain Name Service).

  Objectif = résoudre des noms de domaines en IP (et inversement).
- Structure du système DNS:



  - Le système DNS s'appuie sur une structure arborescente.
  - Chaque noeud est un domaine et possède une étiquette (label).
  - Chaque feuille (extrémité d'une branche) est un hôte.
  - Le nom correspondant au chemin d'un hôte jusqu'à la racine est l'**adresse FQDN**.
  - Chaque domaine possède un serveur DNS.
  - Chaque serveur DNS est déclaré dans un DNS de niveau directement supérieur.
  - Chaque entité est responsable de la gestion de son nom de domaine.

  Remarque: TLD = Top Level Domain.
- Types d'enregistrements DNS:

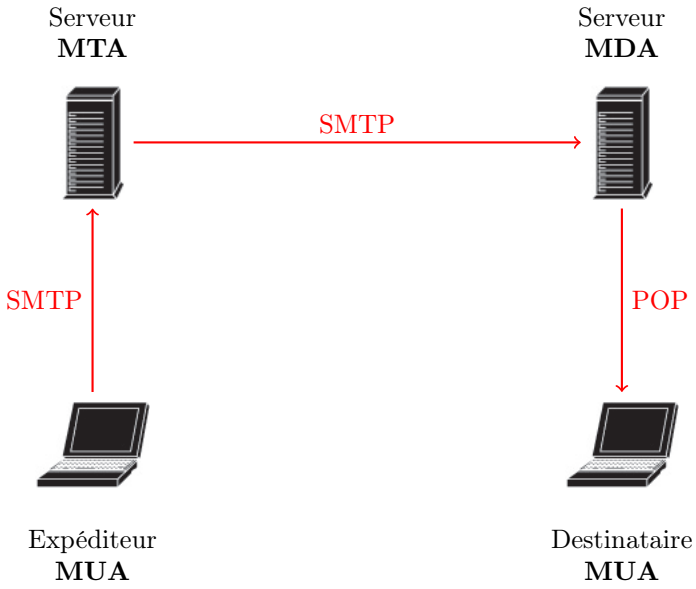
Enregistrement	Signification du nom	Fonction
A	Adresse IPv4	nom de domaine $\Longrightarrow$ IPv4
AAAA	Adresse IPv6 (4× la taille d'une IPv4)	nom de domaine $\Longrightarrow$ IPv6
CNAME	Nom Canonique	nom de domaine $\Longrightarrow$ nom de domaine
MX	Mail Exchanger	nom de domaine $\Longrightarrow$ liste de serveurs (= hôtes)
NS	Name Server	délègue la gestion d'une zone à un autre serveur DNS

- Types de zones & serveurs DNS:
  - zone maître (Master ou Primary),
  - zone esclave (Slave ou Secondary),
  - zone cache (caching),
  - zone inverse (Reverse),
  - serveur forwarder.
- Le DNS utilise le port 53 et les protocoles TCP et UDP:
  - UDP pour les requêtes,
  - TCP pour la synchronisation entre zones.
- 3 types de requêtes DNS: itératives, récursives, inverses.
  - itérative = demande la meilleure réponse possible (y compris partielle) – typique d'un serveur
  - récursive = réponse obligatoire soit correcte et complète, soit négative – typique d'un client
- Types de réponses DNS:
  - autoritative: réponse d'un serveur qui gère la zone concernant la requête.
  - non-autoritative: réponse d'un serveur qui connaît la réponse via le mécanisme de cache.
- Fonctionnement protocole HTTP (port 80, https = port 443):
  1. le client effectue une requête http,
  2. le serveur répond avec le code html demandé,
  3. le client interprète le code html et formate/affche la page,
  4. la session est terminée.
- DHCP est un protocole qui assure la configuration automatique des paramètres IP. Avantages:
  - gestion des IP centralisée et simplifiée,
  - partage optimisé des adresses disponibles,
  - évite les conflits IP,
  - portable et universel: idéal pour assigner des paramètres aux clients mobiles.
- Étapes du cycle de vie DHCP:
  1. affectation: acquisition des paramètres par le client,
  2. réallocation: le client redemande au serveur ses paramètres toujours valides,
  3. opérations "normales": utilisation des paramètres fournis,
  4. renouvellement: le client tente de renouveler son bail,
  5. réafectation: le client tente de renouveler son bail auprès d'un autre serveur si l'ancien est injoignable,
  6. libération: le client libère le bail.
- Les messages DHCP:
  - DHCP DISCOVER = diffusion du client pour localiser les serveurs disponibles.
  - DHCP OFFER = réponse du serveur avec les paramètres de configuration.
  - DHCP REQUEST = message client (3 possibilités):
    1. qui demande les paramètres à un serveur.
    2. qui confirme la validité des adresses précédemment allouées.
    3. qui étend le bail sur une adresse réseau en particulier.

- DHCP ACK = message du serveur avec les paramètres de configuration.
- DHCP NACK = message du serveur indiquant que le bail a expiré.
- DHCP DECLINE = message du client indiquant que l'adresse réseau est déjà utilisée.
- DHCP RELEASE = message du client libérant l'adresse réseau et annulant le bail.

Remarque: DHCP REQUEST est utilisé lors de l'affectation, du renouvèlement et de la réaffectation.

- Les protocoles mail:
  - SMTP (= Simple Mail Transfer Protocol), port = 25
  - POP3 (= Post Office Protocol), port = 110
  - IMAP (= Internet Message Access Protocol), port = 143
  - SMTPS, POPS, IMAPS
- Agents de messagerie:
  - MDA = Mail Delivery Agent
  - MUA = Mail User Agent
  - MTA = Mail Transfer Agent
- Envoi d'un email:



- Fonctionnement de POP3:
  1. connexion au serveur,
  2. téléchargement des fichiers,
  3. effacement des fichiers sur le serveur.
- Autre protocole de réception de mail, **IMAP**:
  - les dossiers manipulés (contenant les mails) ne sont pas locaux mais sur le serveur,
  - les manipulation (ex: suppression de mail) sont donc répercutées sur le serveur,
  - des copies locales sont toujours possibles.
- Protocole de transfert de fichier, **FTP** (= File Transfer Protocol):
  - fiable,

  - performant,
  - versions sécurisées: SFTP, FTPS,
  - port 21 = commande et réponses,
  - port 20 = transfert de fichiers.
- Protocole TFTP (= Trivial File Transfer Protocol):
  - port 69,
  - version simplifiée de FTP:
    * UDP au lieu TCP,
    * pas de listing de fichier ou dossiers,
    * pas d'authentification,
    * pas de chiffrement,

3 Couche Réseaux

- Caractéristiques du protocole IP (= Internet Protocol):
  1. sans connection,
  2. au mieux (non fiable),
  3. indépendant du média.

  Remarque: le protocole IP n'est pas fiable, mais d'autres protocoles gèrent le processus de suivi des paquets (ex: TCP).
- Avantages de créer des sous-réseaux:
  1. plus facile à administrer,
  2. plus performant,
  3. augmente la sécurité,
  4. l'adressage est hiérarchisé: réseau – sous-réseau – hôte.
- Routeur v.s. Switch:

	Routeur	Switch
vitesse	lent	rapide
couche OSI	couche 3	couche 2
adressage utilisé	IP	MAC
broadcast	bloqués	transmis
sécurité	élevée	faible

- Une **route** a 3 composants:
  - le réseau de destination,
  - le masque,
  - le gateway.

  Notation d'une route: `<réseau>/<masque> via <ip_gateway>`.

4 Couche Transport

- Quand un serveur exécute plusieurs services (ex: mail & www), il sait quels paquets sont destinés à quels services grâce aux numéros de port.
- Quand un client ouvre plusieurs sessions sur un même serveur, le serveur distingue les sessions en attribuant à chacune un numéro de port différent.
- Fonctionnalités communes TCP/UDP:
  - segmentation,
  - multiplexage,
  - contrôle d'erreur.
- Fonctionnalités de TCP:
  - fiabilité
    - accusés de réception
    - retransmission des segments perdus
  - délivre les données dans le bon ordre
    - segmente
    - numérote
    - réassemble
  - orienté connexion
    - session TCP (3-way handshake)
  - contrôle de flux
    - fenêtre glissante
    - garde une trace de la connexion
- Étapes d'une session TCP:
  1. établissement de la session,
  2. session,
  3. fin de la session.
- Les flags TCP:
  - SYN = ouverture de session,
  - ACK = accusé de réception,
  - FIN = fermeture de session.
- Autres éléments importants du header TCP:
  - sequence number = le numéro du premier octet de données du segment,
  - acknowledgement number = le numéro du prochain octet (segment) attendu par le récepteur.
- Remarques:
  - Full duplex $\implies$ périphérique = émetteur & récepteur.
  - Si un segment envoyé ne reçoit pas d'acknowledgement après un certain temps, il est renvoyé.
  - Ni TCP, ni UDP ne sont sécurisés.
  - **TCP** est **fiable**.
  - **UDP** est **rapide**.