Haute Ecole Léonard de Vinci

Synthèse
Introduction aux réseaux

Par Corentin D'haeyere

Année 2022 - 2023

Qu'est-ce qu'un réseau ?

Un **réseau** est un ensemble de machines qui peuvent communiquer ensemble via un support de transmission dans un langage commun.

Une machine peut être :

- Un point de terminaison (PC, smartphone)
- Un équipement réseau (switch, routeur)

Support de transmission :

- Supports guidés (fil de cuivre, fibre optique)
- Supports sans-fil (Wifi,)

Un langage commun (Protocole) :

- Définit des règles de communication (Implémentées par les logiciels selon les RFC)
- Réponds souvent à une problématique précise

  Les protocoles sont spécifiés et documenté par une RFC (Request for Comment)

    - Organisations structurantes
        - IAB (Internet Architecture Board)
        - IETF (Internet Engineering Task Force)
        - IRTF (Internet Research Task Force)
        - ICANN (Assigned Names & Numbers)

Un exemple de protocole : NTP (Network Time Protocol) :

- Permet de synchroniser l'heure des machines
- Problématique : je souhaite obtenir l'heure précise
- Règles définies :
    - Format des messages
    - Interlocuteurs
    - Calcul de l'heure (algorithme)

Différentes distances de reseau:

- LAN (Local Area Network) : Réseau domestique, entreprise
- MAN (Metropolitan Area Network) : Réseau de ville
- WAN (Wide Area Network) : Réseau de pays, Internet

Différentes topologies de reseau:

1. Point à point : Dans une topologie point à point, chaque nœud du réseau est connecté directement à un autre nœud sans avoir à partager la connexion avec d'autres nœuds. Chaque connexion est dédiée exclusivement à la communication entre ces deux nœuds spécifiques.

2. Bus : Dans une topologie en bus, tous les nœuds sont connectés à une seule ligne de communication partagée appelée "bus". Chaque nœud peut envoyer des données sur le bus, mais toutes les autres stations reçoivent ces données. Cependant, seule la station destinataire prévue traite réellement les données, tandis que les autres nœuds les ignorent.
3. Ring : Dans une topologie en anneau, chaque nœud est connecté à exactement deux autres nœuds, formant ainsi une boucle continue. Les données circulent dans l'anneau de nœud en nœud jusqu'à ce qu'elles atteignent leur destination. Chaque nœud dans l'anneau amplifie et régénère le signal avant de le transmettre au nœud suivant.
4. Star : Dans une topologie en étoile, tous les nœuds sont connectés à un hub central ou à un commutateur. Toutes les communications passent par ce hub central, qui agit comme un point de contrôle pour les transferts de données entre les différents nœuds du réseau. Si un nœud veut envoyer des données à un autre nœud, il les envoie d'abord au hub central, qui les transmet ensuite à la destination.
5. Mesh : Dans une topologie maillée, chaque nœud est connecté à plusieurs autres nœuds, créant ainsi un réseau dense de connexions. Chaque nœud peut communiquer directement avec n'importe quel autre nœud du réseau sans passer par un nœud central. Cette topologie offre une redondance élevée et une grande fiabilité, car si une connexion échoue, les données peuvent être acheminées par un chemin alternatif.

Sécurité

Il y a trois piliers dans la sécurité :

- Confidentialité : Seuls les utilisateurs de confiance accèdent au système
- Disponibilité : Le système est disponible pour les utilisateurs
- Intégrité : Les données sur le système ne sont pas compromises

Un système sécurisé garantit la confidentialité, la disponibilité et l'intégrité.

Un peu de vocabulaire :

- Une attaque est exécutée par un attaquant via un vecteur d'attaque (DDOS, phishing, …) sur une surface d'attaque (Ensemble des cibles) en exploitant une vulnérabilité pour accéder à une cible

Encapsulation

Encapsulation : Inclure une donnée ou un protocole dans un autre protocole

- La donnée est encapsulée parmi les informations d'un autre protocole
- Chaque protocole reçoit les informations qu'il ne comprend pas
- Le protocole répond à une problématique
- Délègue les autres problématiques à la couche en dessous

La stack OSI

Open Systems Interconnection

Son but est de standardiser le design d'un système avec des protocoles réseaux, chacun d'entre eux appartient à une couche.

La stack contient 7 couches :

- Application : Interaction machine-humain
- Présentation : Vérification du format et du chiffrement
- Session : Garde une connexion avec la machine
- Transport : Segmente les données et gère les flux
- Network : Définition du parcours à travers le réseau
- Data Link : Gestion des erreurs, vitesse, …
- Physical : Encodage physique des données

Chaque couche contient des protocoles d'une même catégorie, capable de décoder et encoder.

C'est cette stack que nous allons aborder durant ce cours.

La stack TCP/IP

Standardise également un système à couche, mais avec proposition concrète, contrairement à la stack OSI :

- Apparu en même temps que OSI
- Plus simple, 4 couches seulement
- Propose des protocoles de communication standardisés
- Le séquencement des informations est plus élevé

Contient seulement 4 couches :

- Application (http, DNS, FTP)
- Transport (TCP, UDP)
- Internet (IP, IGMP, ARP)
- Network Access Layer (Ethernet, Token Ring)

Stack OSI

1) Couche Physique

1.1) Les supports guidés :

Différents types de support guidés :

- « Type cuivre »

  Il en existe deux catégories :

  - Paire torsadée
    - 2 conducteurs identiques torsadés forment une paire
    - Regroupée par fréquence dans des catégories : Les catégories définissent la bande passante maximum
    - Remarques :
      - Maximum ~100m
      - Eviter les câbles plats
      - Choisir la catégorie 5^{e} au minimum
  - Cable coaxial
    - Deux conducteurs concentriques
    - Débits élevés & peu sensible aux perturbations
    - Cher & contraignant (courbure)
    - Nécessite un modem pour décoder le signal

    Aujourd'hui remplacé par des paires torsadées dans un réseau local et par la fibre optique dans des réseaux longues distances

- Fibre optique
  - Un faisceau de lumière est réfléchi et réfracté, avec comme avantages
    - Faible perte & large bande passante
    - Existe en monomode (+distance) ou multimode (+données)
    - Faible dimensions & poids
    - Pas d'interférences électromagnétique
    - Résiste aux attaques chimiques & variations de température
  - Tout connecteur en fibre optique engendre une atténuation

Un câble a plusieurs caractéristiques :

- Multibrin et Monobrin
- Coefficient électrique du conducteur
- Nombre de paires
- Fréquence de diffusion
- Blindage (Protection contre les perturbations électromagnétiques)
  - 2 composantes de blindage
    - Foiled (Feuille d'aluminium autour du câble)
    - Shielded (Tresse métallique autour du câble)

Ces câbles sont sujet à des perturbations électromagnétiques, ce qui peut réduire la vitesse théorique d'un câble mais est mitigé avec un blindage

RJ45 = réseau de communication, connecteur utilisé

Façons de brancher un cable :

- Crossover : entre 2 équipements identiques
- Straight Through : entre 2 équipements différents

Power over Ethernet :

Un câble peut avoir la capacité de fournir une puissance électrique. Il existe deux types de PoE, l'active (puissance variable) et la passive

Les éléments d'un réseau sont interconnectés via un patch panel (baie de brassage)

1.2) Les supports non-guidés

Informations transmises par le biais d'ondes radioélectriques

- Wi-Fi, Bluetooth, talkie-walkie, satellite, téléphonie mobile, etc.
- Aucun support physique nécessaire entre A – B
- ... avantages & inconvénients (implémentation, sécurité, ...)
- Organisation stricte des bandes fréquences nécessaires

Chaque onde radio possède une fréquence et est catégorisé dans une bande

Emission de signaux avec des ondes focalisées

En plus des différents supports de transmission, il existe plusieurs mécanismes pour échanger des informations

- Simplex : Le mode simplex est un mode de communication unidirectionnel où les données peuvent être transmises dans une seule direction, soit du point A au point B, mais pas dans les deux sens simultanément. Cela signifie qu'une station peut seulement émettre des données, tandis que l'autre station ne peut que recevoir ces données. Par exemple, une radio AM/FM est un exemple de communication simplex, car vous pouvez écouter les informations diffusées, mais vous ne pouvez pas envoyer de signal vers la station de radio.
- Duplex : Le mode duplex est un mode de communication bidirectionnel où les données peuvent être transmises dans les deux sens simultanément. Cela permet une communication en temps réel dans les deux directions, à la fois de A vers B et de B vers A. Il existe deux types de duplex :
    - Full Duplex: Dans ce mode, les deux stations peuvent transmettre et recevoir des données simultanément, comme lors d'une conversation téléphonique bidirectionnelle.
    - Half Duplex : Dans ce mode, les deux stations peuvent transmettre et recevoir des données, mais pas en même temps. Ils doivent alterner entre l'émission et la

réception, comme lors d'une conversation radio entre deux personnes qui appuient sur un bouton pour parler et le relâchent pour écouter.

- Série : Dans une connexion série, les données sont transmises bit par bit, l'un après l'autre, sur une seule ligne de communication. Cela signifie que les bits sont envoyés les uns après les autres en série. Les données sont transmises dans un ordre séquentiel et nécessitent une synchronisation précise entre l'émetteur et le récepteur pour interpréter correctement les données. Les connexions série sont couramment utilisées pour les périphériques tels que les ports série RS-232 ou les connexions USB série.
- Parallèle : Dans une connexion parallèle, les données sont transmises simultanément sur plusieurs lignes de communication. Chaque bit est envoyé sur une ligne distincte, ce qui permet un transfert de données plus rapide. Les connexions parallèles étaient couramment utilisées pour les transferts de données internes, par exemple, entre un ordinateur et une imprimante parallèle. Cependant, les connexions série sont plus courantes de nos jours en raison de leur simplicité et de leur capacité à atteindre des vitesses élevées.Multiplexage : partagée avec plusieurs utilisateurs
- Multiplexage : Support partagé avec plusieurs utilisateurs – réalisé par un multiplexeur
    - Simuler sur une seule ligne n liaisons de point-à-point
    - Technique spatiale : une fibre optique utilise différentes longueurs d'ondes
    - Technique temporelle : les utilisateurs possèdent des espaces de temps

2) Couche Data Link

2.1) Description

Cette deuxième couche est en charge du transfert entre nœuds et doit donc gérer les erreurs. L'unité de transfert de cette couche est la trame « frame ».

Elle a plusieurs responsabilités :

- Transmettre correctement des trames dans un réseau local
- Corriger les erreurs de la couche physique
- Résout uniquement des problématiques entre nœuds connexes
- Eviter les collisions de données au niveau local

⇨ Effectuer une gestion du trafic réseau local

Uniquement utilisée dans un réseau local (LAN)

Chaque machine connectée au réseau possède des interfaces réseau, il est possible de changer cette adresses MAC.

Tous les messages envoyés sur le réseau proviennent d'une adresse MAC.

Ces messages sont envoyés en utilisant différentes techniques de transmission

- Broadcast : d'un point vers tous les clients dans un domaine (broadcast domain)
- Multicast : d'un point vers certains clients

2.2) Quelques concepts

Ethernet

Ensemble de technologies qui implémentent les fonctions essentielles L1/L2

- Couvre L1 Physical et L2 Data Link
- Protocole Ethernet, standards pour câbles, etc.
- Définit le concept de trame (frame)
- Mécanisme de vérification d'erreurs
- Conçu pour les réseaux locaux

		Header Ethernet (14 bytes)				
7 bytes	1 byte	6 bytes	6 bytes	2 bytes	46 – 1500 bytes	4 bytes
Préambule	Délimiteur	MAC destination	MAC source	Longueur	Données …	CRC

CRC : Cyclic redundancy check, détecte les erreurs de transmissions. Toutes les erreurs ne sont pas forcément détectées.

Ethernet II

Les 2 bytes sont maintenant dédiées au « EtherType » : le protocole encapsulé

Quelques Ethertypes standardisés :
• 0x0800 IPv4
• 0x0806 ARP
• 0X86DD IPv6

Equipements réseaux

- Hub
  - Equipement réseau basique, basé sur un « repeater »
    - Reçoit un signal sur un port et la répète sur tous les ports
    - Façon minimaliste de créer un réseau
    - Avantage économique par rapport à des équipements complexes
    - Inconvénients : aucune gestion de la charge, sécurité faible, collisions, ...
    - Transmet les données en half-duplex

- Bridge
  - Equipement réseau plus avancé qu'un hub, analyse les trames
    - Analyse des trames Ethernet de la couche Data Link
    - Extrait l'adresse MAC source et destination
    - Possède 2 « ports » (cartes réseau)
    - Transfère les trames d'un port vers un autre... si la trame de destination est sur l'autre port

- Switch
  - Un switch est un bridge avec plusieurs ports
    - Analyse les trames et extrait les adresses MAC
    - Transfère seulement un message vers le port de destination
    - Gestion du trafic avancé, partage de la bande passante, segmentation, ...
    - Transmet les données en full-duplex

  - Le switch a besoin de connaitre l'adresse MAC connectée sur un port
    - Essentiel pour rediriger les trames Ethernet vers le bon port
    - Le switch est capable d'effectuer un apprentissage
    - Opération automatique, pas de configuration
    - Sur base de l'adresse MAC source dans le header Ethernet
  - Le switch maintient une table (forwarding database) avec les adresses MAC connectées à ses ports

Port	Adresse MAC connectée
1	AA:AA:AA:AA:AA:AA
2	?
3	?
4	DD:DD:DD:DD:DD:DD

    - En cas d'absence de l'adresse MAC dans la table, le switch transfère sur tous les ports – sauf le port d'origine
    - Si une adresse MAC n'a pas été aperçue en source depuis un port pendant une durée (5 minutes par exemple), l'adresse est purgée

  - Le switch permet une gestion de trafic optimale dans un réseau
    - Capable d'apprendre automatiquement
    - Si une adresse MAC est dans la table... alors seul l'adresse recevra la trame
    - Si un port est occupé, le switch est capable de mettre la trame en attente
    - Le switch ne modifie pas par défaut la trame Ethernet

Il est donc très facile d'attaquer un switch réseau : (MAC flooding)

- Un switch possède une capacité mémoire limitée
    - C'est également le cas de la forwarding database
    - Un attaquant effectue des envois de trames
    - ... avec une adresse source différente
    - Objectif : remplir la table d'adressage
    - ... et remplacer des adresses légitimes ou autre

Broadcast storm

Souvent déclenché par une trame broadcast avec une boucle réseau

- Chaque switch diffuse la trame sur tous ses ports
- Pas d'expiration (TTL) sur une trame
- ... et donc le message reste indéfiniment dans le réseau local
- Montée en charge jusqu'à arriver à la saturation des équipements (DOS)

C'est là qu'intervient le protocole STP (Spanning Tree Protocol) qui permet d'éviter ces boucles réseaux. Son fonctionnement est très simple :

- Le protocole STP est supporté par tous les switchs modernes
- Uniquement pour switchs, vos équipements ne l'ont pas
- Election d'un root bridge et fermeture de ports sur les autres switchs
    - Je suis le switch avec le bridge ID le plus faible, je deviens le root bridge du réseau

3) Couche Network

3.1) Description

Cette couche contient très peu de protocoles, ne gère pas les réseaux locaux (L2 Data Link), ne gère pas l'aspect physique (L1 Physical) et s'occupe exclusivement du parcours à travers le réseau.

Une adresse MAC est gravée dans une carte réseau... et donc physique

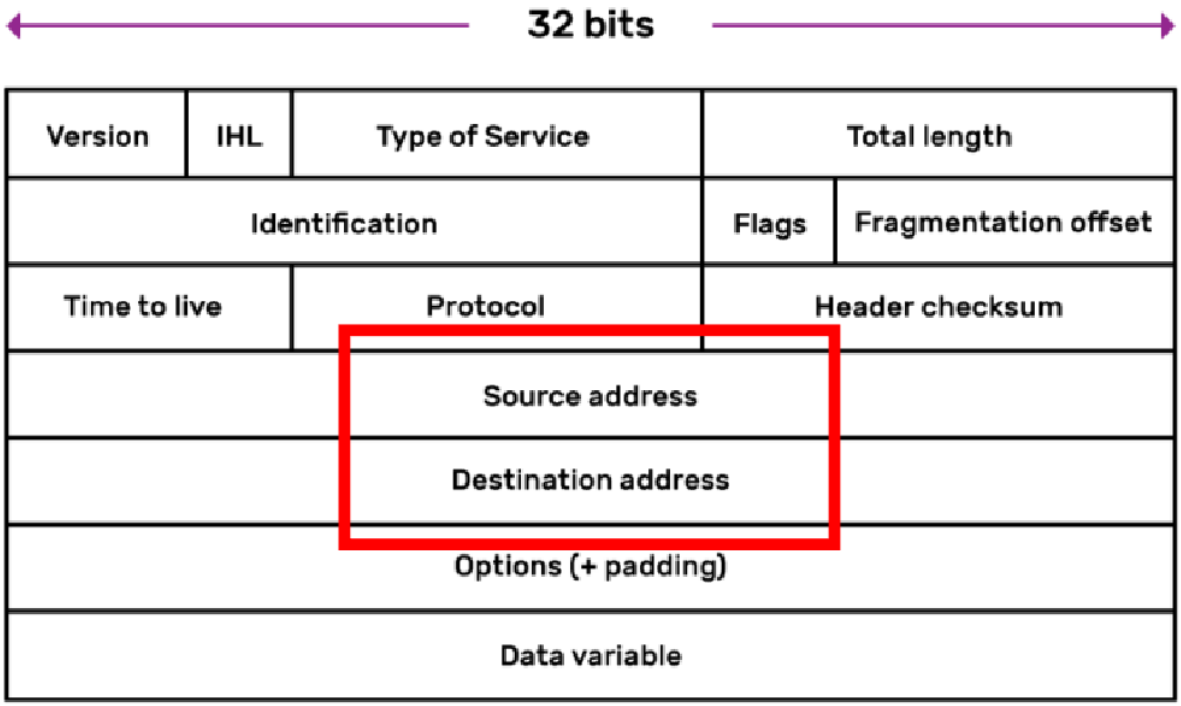
- Elle ne change « techniquement » pas – pas facile d'organiser un réseau
- Nous avons besoin d'autres adresses pour s'adapter au contexte
- Contexte étant : l'emplacement des machines, la taille du réseau, ...

Ce nouvel adressage est géré par la couche Network à l'aide de deux protocoles très connus :

- IPv4, le protocole omniprésent actuellement (192.168.1.1)
- IPv6, l'évolution de l'IPv4 (2001:db8:0:85a3:0:0:ac1f:8001)

Les responsabilités de la couche Network :

- Transfert de données entre réseaux
- Définition d'un adressage logique
- Routage (création d'un chemin de communication « optimal »
- Elle transfert ces données via des paquets



L'adressage IPv4

- Une adresse logique constituée de 4 bytes (32 bits) selon une notation décimale avec points
- Chaque adresse contient une partie dédiée (masque réseau) à identifier le réseau.
- Ce masque réseau détermine les bits alloués au réseau

La classe (historique) définit le nombre de bytes alloués à l'identifiant réseau

Classe A	255.0.0.0	1.0.0.0 - 126.255.255.255
Classe B	255.255.0.0	128.0.0.0 - 191.255.255.255
Classe C	255.255.255.0	192.0.0.0 - 223.255.255.255
Classe D	240.0.0.0	224.0.0.0 - 239.255.255.255

Les classes d'adresses IP prévues initialement ne conviennent plus

3.2) Quelques concepts

Adresses IP privées

Certaines ranges d'IP sont assignés à des réseaux privés

- Réseaux locaux d'entreprise & domestiques
- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

Les adresses non-assignables

Certaines IP ne peuvent pas être assignées à une machine

- 127.0.0.1 : adresse locale, la machine elle-même (localhost)
- 0.0.0.0 : destination inconnue (route par défaut)
- X.X.0.0 : adresse qui identifie le réseau (bits host à 0)
- X.X.255.255 : broadcast, toutes les machines (bits host à 1)

Le Routeur.

- Equipement réseau qui fait transiter les paquets (OSI L3)
    - Transit = acheminer les données (paquets)
    - ... d'une source vers une destination
    - Sur base d'une logique (mécanisme de routage) il transfère les paquets
    - ... d'une interface vers une autre interface réseau

Il existe différentes métriques de distance comme :

- Longueur du lien
- Nombre de sauts
- Bande passante
- Charge
- Délais
- Fiabilité
- Perte de paquets
- … ;

Le routeur définit une table de routage (routing table)

Base de données contenant les informations pour router des paquets

- Présent sur les routeurs
- Présent également sur vos machines ou tout équipement L3
- Contient à minima le réseau à atteindre, une métrique de distance et next hop
- Le « next hop » est le prochain nœud à contacter ~ gateway

Réseau	Masque réseau	Next hop (gateway)	Métrique	Interface
40.0.1.0	255.255.255.0	*Directly connected*	10	Eth0
40.0.2.0	255.255.255.0	50.0.0.2	5	Eth1
40.0.3.0	255.255.255.0	50.0.0.5	10	Eth2

Autonomous System (AS)

Un Autonomous System est un réseau géré par une entité et identifié par ASN

- Chaque numéro d'AS est unique (ASN)
- Chaque AS possède des réseaux (IP ranges) qui lui appartiennent
- Un AS est géré par une entité ou organisation (pays, société, ...)
- L'Internet est composé une multitude d'AS

Il existe différents types de protocoles de routage :

- Statique

Déclaration d'une table de routage manuellement dans chaque routeur

  - N'est pas exclusif avec du routage dynamique
  - Par exemple : un routeur dynamique peut avoir une default route statique
  - Adapté aux petits réseaux
  - Avantages : peu d'impact CPU, pas complexe
  - Désavantages : aucune adaptation (taille, échecs, ...) et probabilité d'erreurs
- Dynamique

Routeur transmet des données vers d'autres routeurs et s'adapte au réseau

  - Les routeurs échangent des informations sur l'état du réseau (tables)
  - Protocoles distance/path vector : les routeurs n'ont pas de vision complète
    - RIP
      - Routing Internet Protocol

        - Interior Gateway Protocol (IGP), utilisé dans un AS
        - Chaque routeur communique avec ses voisins
        - Métrique de routage est le nombre de « hops »
    - BGP
        - Border Gateway Protocol
        - Exterior Gateway Protocol (EGP), utilisé entre les AS
        - Le protocole qui porte Internet
        - Echange des information de routage entre AS
- Protocoles link state : les routeurs connaissent la topologie réseau
    - Via l'algorithme de Dijkstra
    - OSPF
        - Open Shortest Path First
        - Interior Gateway Protocol (IGP), utilisé dans un AS
        - Remplaçant du RIP
        - Plus complexe (notion d'aires, ...)
        - Peut aller au delà de 15 sauts (hops)
        - Prends en compte les liaisons et l'état de la bande passante

Intervient alors un probleme :

Si je souhaite envoyer un message, je possède toutes les informations pour le faire, sauf une très importante. Quel est l'adresse MAC de destination de mon message ?

Une solution : le protocole ARP (Address Resolution Protocol)

- Permet d'associer une adresse IPv4 à une adresse MAC
- Indispensable dans les réseaux locaux
- Le protocole se situe à la couche OSI L3, mais travaille avec OSI L2
- Chaque machine possède un cache ARP (base de données IPv4 – MAC)
- Aucune sécurité, très vulnérable aux attaques

4) Couche Transport

La couche L3 présente des limites

- Pas de rattachement entre les paquets
- Pas de réaction en cas de perte
- Pas de réaction en cas d'ordre différent

Couche du modèle OSI en charge de la gestion de flux avancée

- Au dessus de la couche L3 Network (bénéficie d'adresses, de routage, ...)
- Peut effectue de la gestion d'erreurs (mais pas obligatoirement)
- Rassemble les paquets pour former une communication entre processus

Cette communication entre processus est permise par le concept de ports

Une « boite aux lettres » virtuelle pour contacter un processus

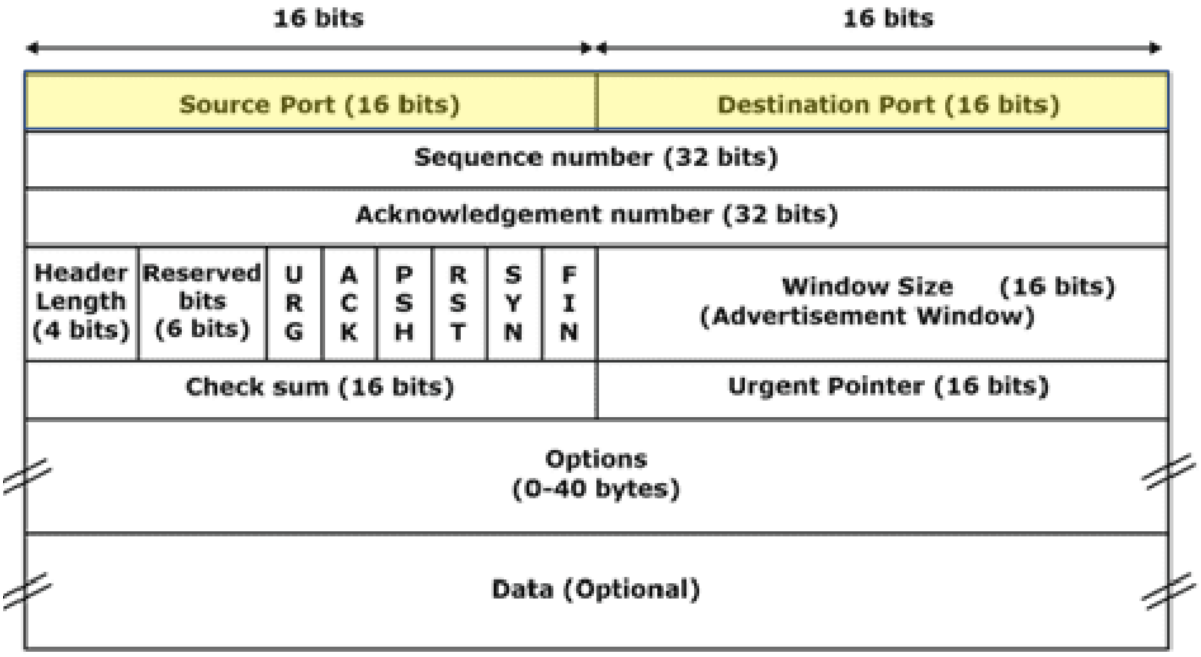
- Chaque paquet dans un segment de la couche OSI L4
- ... contient un port source & destination
- Un processus peut écouter sur le réseau via un port
- Les ports entre 0 et 1023 sont réservés (besoin d'un droit admin)

Avec ce nouveau concept, apparait deux protocoles de transmission de données :

- UDP (User Datagram Protocol)
    - Pas de connexion préalable (protocole connectionless)
    - Aucune fiabilité en cas de perte
    - L'ordre d'arrivée n'est pas garanti
    - Utilisé pour sa rapidité

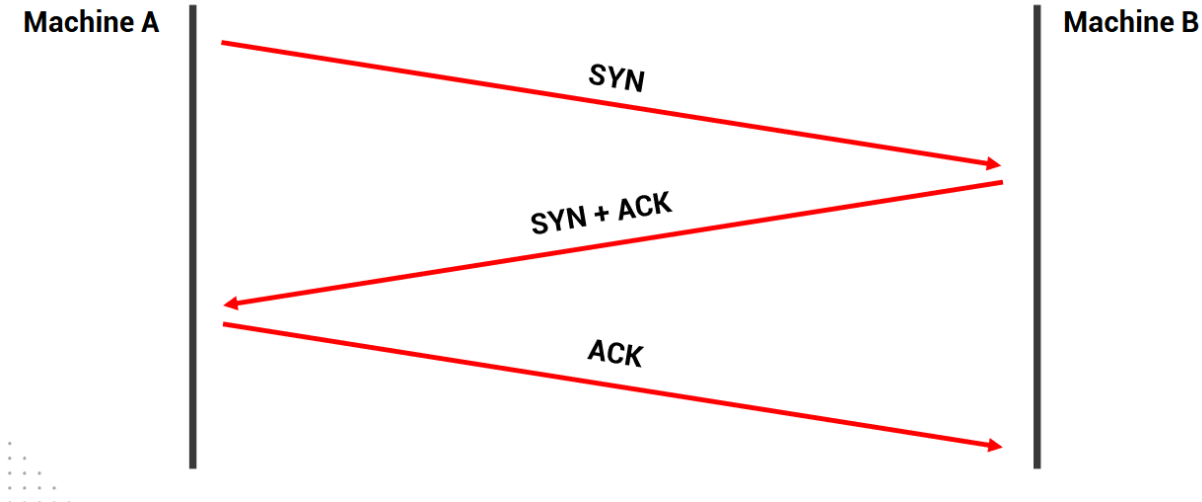
Header UDP (8 bytes)			
2 bytes	2 bytes	2 bytes	2 bytes
Port source	Port destination	Longueur	Checksum UDP
Données (payload) ...			

- TCP (Transmission Control Protocol)
  - Connexion préalable (handshaking)
  - Gestion des erreurs (perte de paquets, ...)
  - Gestion de la congestion
  - Gestion de l'ordre des communications



Concept de « 3-way-handshake »

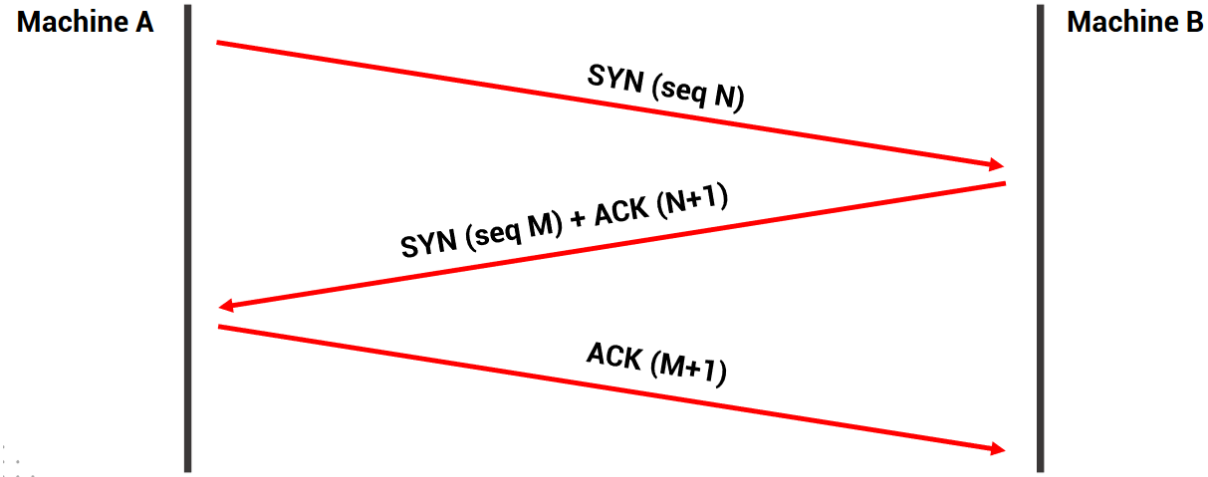
Permet d'établir une connexion entre 2 machines (client-serveur)



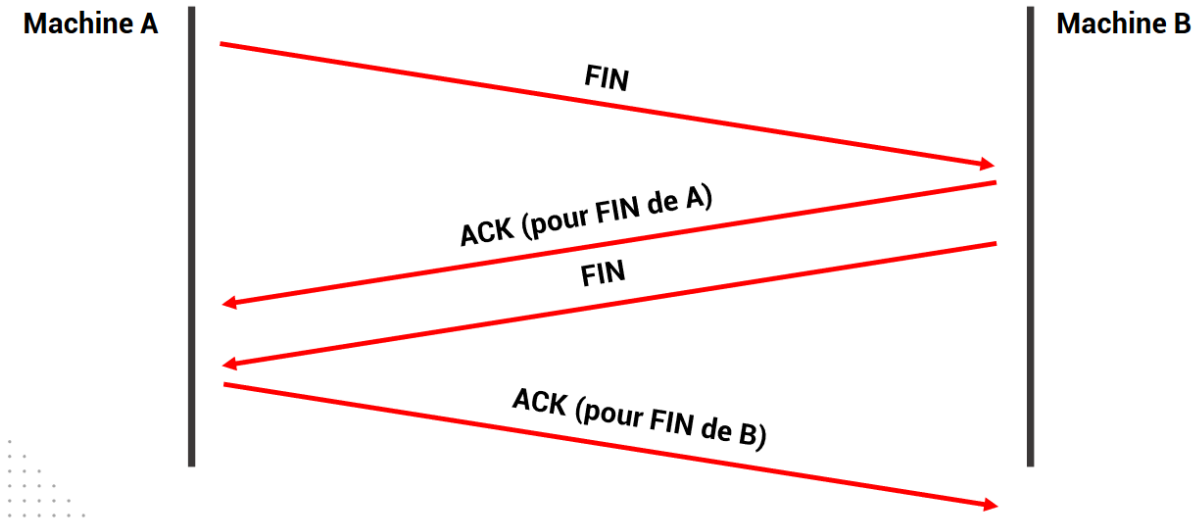
Numéro de séquence TCP

Un numéro sur 32 bits (4 bytes) pour identifier et rassembler les données

- Chaque byte possède un numéro de séquence
- Initialisé aléatoirement au début de chaque échange
- Chaque parti TCP génère un Initial Sequence Number (ISN)
- Permet également de tracer le nombre de données envoyées



Une connexion TCP se cloture mutuellement avec le flag FIN



Différences entre UDP et TCP

	Protocole TCP	**Protocole UDP**
Connexion	*3-way handshake*	Sans connexion
Fiabilité de livraison	Très fiable	Non-fiable
Gestion des erreurs	Complète (garantie d'intégrité, ...)	Minime (checksum basique, ...)
Vitesse	Lent	Rapide
Ordre	Garanti	Non-garanti

5) Couche Application

Toute machine possède une adresse IPv4 privée pour communiquer en interne et une adresse IPv4 publique pour communiquer au dela. Les adresses privées ne sortent pas du réseau local.

Pour communiquer avec le monde extérieur et recevoir une adresse publique, on fait appel au protocole NAT (Network Address Translation)

Le routeur remplace l'adresse IP privée par une adresse IP publique

- Conçu – entre autres – pour apporter une réponse au manque d'IPv4
- Plusieurs appareils partagent la même adresse IP4
- 3 catégories
    - NAT statique (Chaque adresse IP privée est reliée à une adresse IP publique statique)
    - NAT dynamique (Chaque connexion sortante est associée dynamiquement à une IP publique)
    - NAT overlay (Utilise les ports (TCP/UDP) pour partager une même adresse IPv4)

Ayant ca dans notre réseau, on peut aussi introduire le port forwarding, il permet de définir une règle NAT statique. Ce qui revient à autoriser du trafic entrant vers une machine.

Liste de ports TCP & UDP (bases)

Port	Protocole	TCP	UDP	Description
21	FTP	■		Transfert de fichiers (non-sécurisé)
22	SSH	■		Secure Shell & transfert de fichiers (sécurisé)
23	Telnet	■		Communications textuelles (non-sécurisé)
25	SMTP	■		Protocole d'envoi email (non-sécurisé)
53	DNS	■	■	Domain Name System
67/68	DHCP		■	Configuration de réseau dynamique
80	HTTP	■		Hypertext Transfer Protocol (non-sécurisé)
110	POP3	■		Protocole de réception email (non-sécurisé)

Liste de ports TCP & UDP (bases)

Port	Protocole	TCP	UDP	Description
123	NTP		■	Network Time Protocol, synchronisation du temps
143	IMAP	■		Protocole de réception email (non-sécurisé)
443	HTTPS	■		Hypertext Transfer Protocol (sécurisé, TLS/SSL)
465	SMTP (s)	■		Protocole d'envoi email (sécurisé, TLS/SSL)
993	IMAP (s)	■		Protocole de réception email (sécurisé, TLS/SSL)
995	POP3 (s)	■	■	Protocole de réception email (sécurisé, TLS/SSL)
3306	MySQL	■		Base de données MySQL
5432	PostgreSQL	■		Base de données PostgreSQL

Explications de certains protocoles présents :

1) Le protocole http (Hypertext Transfert Protocol)
   - Développé par Tim Berners-Lee
   - A servi aux fondations du World Wide Web avec HTML & URL
   - Protocole de communication pour pages web
   - Utilise le port 80 en TCP
   - Protocole non-sécurisé
   - Un client HTTP peut demander une page web (document)
   - ... et recevoir une réponse d'un serveur http

   Ce protocol a besoin d'une structure pour fonctionner, c'est la qu'interviennent les URL (Uniform Resource Locator)

   Elles permettent de demander une ressource (document) de façon structurée.

Elles sont composées de :

- Du protocol
- Un nom d'utilisateur suivi de son mot de passe
- Le nom de domaine
- Le port de connexion
- Le document demandé
- Des paramètres

```
http://john:secret123@www.google.be:80/index.html?lang=fr
```

Quelques remarque la dessus :

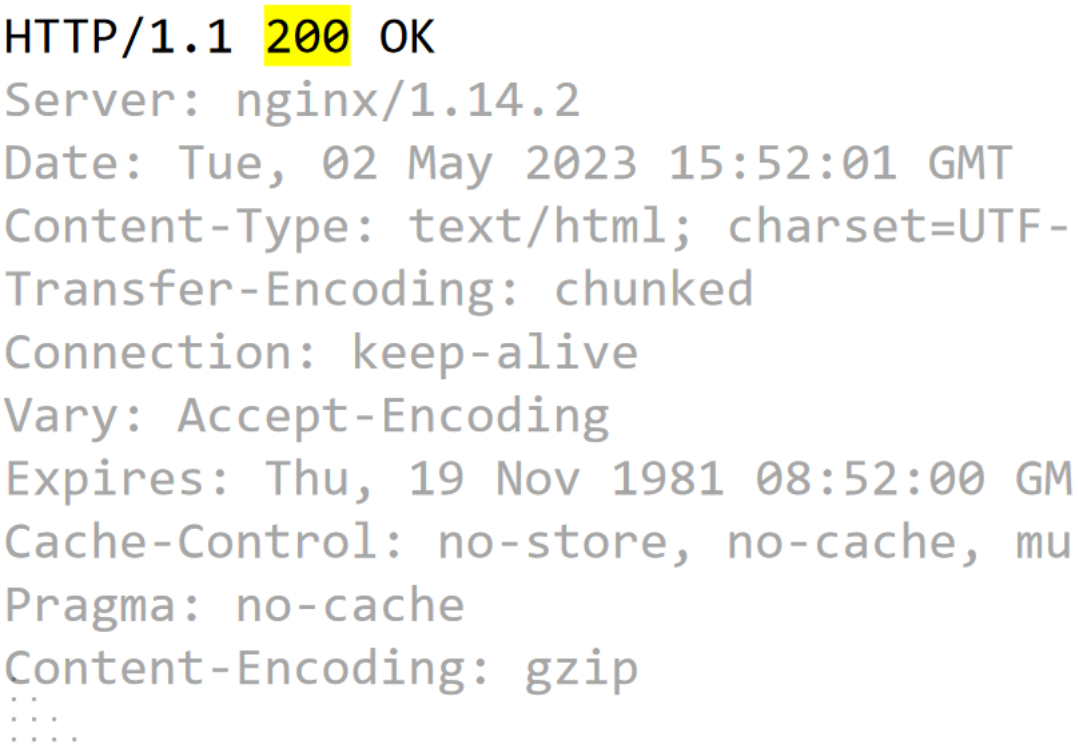
- Protocole HTTP - complété par la navigateur
- Utilisateur/Mot de passe - rarement utilisé sur les sites publics
- Domaine – le seul paramètre indispensable
- Port TCP 80- complété par la navigateur
- Document – par défaut, « index.html » est demandé
- Paramètres (Query) – optionnel, souvent défini par les applications web

Il existe pour le protocol http, différentes actions que l'on appelle méthodes

Méthode	**Signification**
GET (défaut)	Récupérer une ressource (*download*)
POST	Envoyer une ressource (*upload*)
PUT	Remplacer intégralement une ressource
PATCH	Modifier partiellement une ressource
DELETE	Supprimer une ressource

Exemple d'une requête http, avec comme premier parametre, la méthode utilisée. Ensuite la ressource demandée. La version d'http et enfin les headers

Même chose pour la réponse :



La version d'http, le status de la réponse. Le message lié à ce status puis les headers.

Code	Signification
200	OK, tout s'est bien déroulé
201	La ressource a été créé
301	URL changée de façon permanente
400	*Bad request*, requête malformée par le client
401	*Unauthorized*, vous n'êtes pas authentifié
403	*Forbidden*, vous n'avez pas les droits nécessaires
404	*Not found*, ressource introuvable
500	Erreur côté serveur (crash système, ...)

2) FTP (File Transfer Protocol)

- Permet le partage de fichiers
- Utilise une connexion de « contrôle » (TCP, port 21)
- Utilise une connexion de « données » (TCP, port 20)
- Protocole non-sécurisé – préférez le FTPS
- Fonctionne avec un système de
    - Commandes

Commande	Signification
HELP	Affiche les commandes disponibles
STATUS	Donne l'état de la connexion
USER	Spécifie l'utilisateur pour une connexion
PASS	Spécifie le mot de passe
STOR	Envoyer des données vers le serveur
PORT	Spécifie une adresse & port de connexion
QUIT	Fermeture de connexion

- Réponses numériques

Mode active : Le client détermine un port de son côté pour échanger les données, le serveur FTP s'y connecte pour le transfert

Mode passif : Le serveur FTP détermine un port de son côté pour échanger les données, le client s'y connecte pour le transfert

3) Telnet

Permet d'établir une connexion TCP interactive avec des services distants

- TErminaL NETwork
- Historiquement, un serveur telnet utilisait le port 23 (TCP)
- Un serveur telnet donne accès à une machine distante
- Le client telnet permet de s'y connecter... ou d'établir une connexion TCP

4) SSH

Permet d'établir une session à distance sécurisée (chiffrement des données)

- Secure Shell
- Successeur de Telnet
- Utilise le port 22 (TCP)
- Permet à un utilisateur de se connecter sur une machine distante
  - Pour administrer la machine
  - Pour utiliser les services présents
  - Pour établir un tunnel SSH
  - (...)

5) SFTP

Protocole de transfert de fichiers sécurisé, basé sur SSH

- Secure File Transfer Protocol
- Successeur du FTP
- Utilise le port 22 (TCP)
- N'utilisez plus FTP – risque d'interception des communications

6) SMTP

Protocole de communication pour l'envoi des emails

- Simple Mail Transfer Protocol
- Utilise le port 25 (TCP)
- Prends en charge le transfert des emails vers des serveurs de messagerie
- Un « serveur SMTP » prends en charge le transfert des emails
- Protocole non-sécurisé

7) IMAP & POP3

Protocoles de communication pour la réception des emails

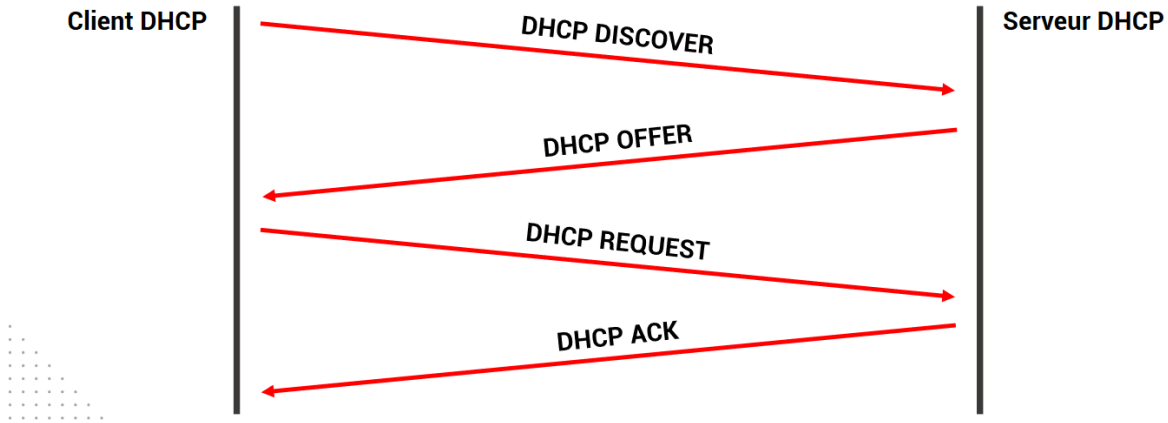
- POP3 utilise le port 110 (TCP)
- IMAP utilise le port 143 (TCP)
- POP3 supprime les messages après lecture sur le serveur
- IMAP permet de lire les messages sur le serveur sans destruction
- Protocoles non-sécurisés

Une question que l'on peut se poser : Comment les machines reçoivent une adresse ip privée ?

Solution : DHCP (Dynamic Host Configuration Protocol)

- Fournit automatiquement une adresse IP dans un réseau
- Propose également d'autres informations (network mask, default gateway, ...)
- Serveur DHCP gère un « pool » d'adresses disponibles
- Une adresse « expire » au bout d'un certain délais (bail)
- Permet de faire une attribution statique pour certains clients

L'obtention d'une adresse IP se déroule en 4 phases



DHCP fournit – en plus d'une IPv4 - aux clients également des options

- Masque réseau
- Route par défaut (router)
- Serveur NTP
- Serveur DNS
- Configuration personnalisée

Finalement, nous avons dans la couche L7, le DNS (Domain Name System)

- Effectue de la résolution de noms en adresses IP
- Permet d'organiser les machines avec une nomenclature logique
- Principalement UDP, fonctionne également en TCP (pour transfert de zone)
- Registre mondial qui peut être requeté

Il existe plusieurs types de serveurs DNS :

- Résolveur récursif : premier point de contact, gère appels DNS & cache
- Root server : 13 serveurs, connu de tous résolveurs – redirigent vers TLD
- TLD server : contient toutes les informations des top-level domains
- Authoritative server : contient informations spécifiques au nom de domaine

Type	Signification
A	Adresse IPv4
AAAA	Adresse IPv6
CNAME	Alias de domaine
NS	Serveur DNS (enfant, backup, ...)
MX	Serveur mail relié au domaine
TXT	Informations textuelles

Load balancing DNS

Le load balancing est une technique de répartition de charge

- L'objectif est d'offrir de la résilience et de soulager l'infrastructure
- Le DNS peut servir de load balancer
- Via l'assignation de plusieurs cibles A/AAAA sur un même domaine
- Attention à la mise en cache DNS