Notes réseaux

**10/02/2025**

Quel est le numéro du port associé au service Intel ? 🡪 question qui tombera à l’examen 100%

Examen : ~70% théorie ; ~30% pratique

**Un réseau** est un ensemble de machines qui communiquent ensemble via un support de transmission avec un langage commun

Support de transmission : quand on parle, l’air est le support de transmission (vibrations de l’air)

Protocole = langage commun (SL.17) 🡪req, requête 🡨res, réponse

NTP = Network Time Protocol

RFC = « dictionnaire » qui détermine ce qu’est le NTP (Request For Comment)

Une RFC c’est une définition

En sécu : 3 piliers : confidentialité, disponibilité, intégrité (SL.26)

Encapsulation : mettre dans une couche (ici le protocole physique) (SL.35) (def SL.34)

**18/02/2025**

Rappel : L3/4, L7,… -> fait référence à des **couches** de la **stack OSI** (layer)

Encapsulation = inclure une donnée ou un protocole **dans un autre protocole**

Cette séance est focalisée sur la **couche physique** (OSI L1)

« type cuivre »

Support guidé = câble

Cuivre + isolant

Deux catégories : paire torsadée et cable coaxial

Ne jamais passer un câble réseau près d’une machine qui émet des impulsions électromagnétiques 🡪 câble spéciaux blindés ; et ne jamais enrouler un câble en rond

Technologies xDSL : Digital Subscriber Line

Paire torsadée = câble réseau classique (éthernet) -> caractéristiques du câble : voir PPT SL.21

Plusieurs catégories de câbles : définissant la bande passante (vitesse) maximum : SL.22

SL.23 : important (+SL.24 : exemples de SL.23)

SL.25 : RJ45 : le seul qu’on utilise vrmt dans le monde pro

PoE = Power over Ethernet : on met dans un même câble un câble électrique et un câble réseau

Principe de la fibre optique : on ne transporte pas l’info avec des décharges électriques, mais avec de la **lumière**

(infos manquantes : voir PPT)

Liaisons non-guidées (pas de câble)

Liaisons Hertziennes : ondes radioélectriques

Chaque technologie a sa fréquence dédiée

Satellites réseaux 🡪 presque tjrs en orbite géostationnaire.

**25-02-2025**

Rappel cables blindés (catégorie 7) : le blindage capte les perturbations et les envoient à la terre -> un cable de catégorie 7 doit être relié à la terre !!

PoE = mécanisme pour faire en sorte que le courant électrique soit injecté dans le câble réseau

Cette séance est focalisée sur la **couche datalink** (OSI L2)

Simplex : source 🡪récepteur

Half Duplex : source 🡪 récepteur et source 🡨 récepteur MAIS PAS EN MÊME TEMPS

Full Duplex : source 🡪 récepteur et source 🡨 récepteur (possiblement en même temps)

Transmission en parallèle / en série : voir PPT SL.12

Multiplexage = simuler sur une seule ligne plusieurs connections point à point

Multiplexeur : prendre plusieurs sources et le faire passer en une seule

Démultiplexeur : inverse du multiplexeur

Technique spatiale : le démultiplexeur prend les diff longueurs d’ondes (couleurs de la lumière) et envoie chacune à diff machines

Technique temporelle : allouer à chaque appareil une période de temps

Ex : 3 personnes co sur un cable de fibre optique :

Le 1e envoie « Bonjour! »

Le 2e envoie « Hello!=D »

Le 3e envoie « Goeiedag »

Ce qu’enverra le multiplexeur : Bo|He|Go|nj|ll|ei|ou|o!|ed|r!|=D|ag|

Ce que traduira le démultiplexeur : Bonjour!|Hello!=D|Goeiedag

COUCHE DATALINK (OSI L2)

Nœud = machine connectée à une autre (sans fil ou avec fil)

Unité de transfert = enveloppe (trame (frame))

Responsabilités de la couche datalink : faire en sorte que la communication soit propre et bien gérée (pour plus de détails : voir PPT SL.18)

Les protocoles de la couche datalink sont utilisés en LAN

Si une machine a une interface réseau (carte réseau, puce wifi), elle a d’office une adresse MAC

Adresse MAC = chaque constructeur a un préfixe d’adresse MAC unique (asus, TP-Link,…), adresse MAC = identifiant

Broadcast : voir PPT

Broadcast domain : délimite la zone de broadcast

Ethernet : ensemble de technologies qui implémentent les fonctions L1 et L2

L’ethernet est conçu pour les réseaux locaux (LAN)

STRUCTURE D’UN PAQUET ETHERNET (voir PPT SL.31)

Préambule = « attention, je vais émettre qqch !! »

Délimiteur = ??

MAC DESTINATION & MAC SOURCE (adresses MAC des machines qui communiquent entre elles)

Type d’ethernet

Les données

FCS = ??

(j’me suis cassé à la pause)

-VACANCES-

**11-03-2025**

BUT DE LA COUCHE DATALINK : pouvoir lier des appareils entre eux (destinataires, envoyeurs)

Rappel : adresse MAC liée à la CARTE RESEAU

Rappel : les couches sont déterminées dans le **système OSI** (c ça qu’on voit dans ce cours)

FCS = pour voir s’il y a des erreurs

Rappel : paquet = Trame Ethernet

Hub = machine au milieu 🡪 travaille au niveau physique (L1) (PPT3 SL46) (fonctionnement du hub : src : A ; src : B => A envoie🡪Hub reçoit🡪 B reçoit (tlmd reçoit)

Bridge 🡪 travaille au niveau data link (L2) (rappel : L = Layer)

Le Hub est bête et ne comprend pas le message 🡪 il transmet le message à tlmd

Le Bridge et intelligent et comprend le message 🡪 il transmet le message du côté où se trouve le destinataire



🡪Ici , A envoie et le B est destinataire. Le Hub forwarde à tlmd, tandis que le bridge vérifie où est le destinataire

Switch : encore mieux que le Bridge : n’envoie QUE au destinataire

Le routeur WIFI à la maison est un Switch (pas une Switch hein j’te vois v’nir p’tit malin)

**PPT 4 : Le Switch**

Le switch a besoin des adresses MAC

Le switch peut apprendre (!) sur base de l’adresse MAC source

Forwarding database = table d’apprentissage

Flooding : qd je reçois un message de A destinée à une machine inconnue, le switch va Flooder le réseau, càd envoyer sur TOUS les ports (sauf celui de l’envoyeur)

Mais alors est ce que les autres machines peuvent lire le message ?

🡪Oui, mais ils vont l’ignorer car si l’adresse MAC du destinataire ne correspond pas, ils vont refuser de le lire. (sauf en promiscuous mode aka the sneaky sneaky mode où les messages sont écoutés et enregistrés)

File d’attente : le switch est capable de mettre des trames en attente si un port est occupé

IMPORTANT : le switch ne MODIFIE PAS la trame internet !!!

Expiration des adresses mac : si une adresse MAC n’a pas été vue depuis un certain temps (genre 5 min), on efface cette adresse MAC de la table d’apprentissage

Interro surprise : que se passe-t-il si, après suppression de D dans la table, A envoie un message à D ? Réponse  : Le Switch effectue un Flooding !

Dans un datacenter : plusieurs switches

SL28 : A1 veut envoyer un message à A4 : étape 1 : A1 crée une trame réseau ; étape 2 : créer un préambule ; étapes suivantes : créer le reste du paquet ; étape x+1 : A1 envoie au Switch1 ; étape x+2 : le Switch1 va Flooder vers A2, Switch2 et A6 ; étape x+3 : le Switch2 va Flooder vers A3, A4 et A5 🡪 **A4 reçoit le message**. Les Switches écrivent le port de A1 dans leurs tables.  
Maintenant A4 veut répondre à A1 : étape 1 : A4 crée une trame réseau ; étape 2 : créer chaque partie du paquet ; étape 3 : A4 envoie le message à Switch2 ; étape 4 : le Switch ne va PAS Flooder car il connait maintenant l’adresse de A1 : il envoie le message à Switch1 ; étape 5 : Switch 1 forwarde le message à A1 **🡪 A1 reçoit la réponse**

SL30 : exemple de table d’adressage d’un Switch de datacenter

MAC Flooding : attaque des Switch : le Switch a une mémoire limitée (et aussi la forwarding database)  
on attaque en envoyant (spammant) des trames avec des adresses sources différentes  
objectif de l’attaque : remplir la table d’adressage  
(note : ces attaques fonctionnent uniquement sur des vieux switches cisco à quinze balles)

Autre type d’attaque : voir PPT SL 34+

Rappel : message broadcast : on envoie un message à tlmd

Spanning tree protocol : protocole de niveau 2 (voir PPT SL41)

STP : uniquement compris par les Switch

Multicast : enfaite je veux juste envoyer le message aux switches 🡪 suite de l’explication SL43

SL46 : ne pas étudier

-fin de la séance-

**18-03-2025**

Rappels de la semaine passée :

À quoi sert le champ EtherType ?  
il sert à donner le type de données, le type de protocole dans le niveau au dessus

À quoi sert une forwarding database ?  
forwarding database = table d’adressage dans les switches associer un port à une adresse mac, à une destination

Comment attaquer un switch ?  
remplir sa table d’adressage avec des adresses mac SOURCE

Rappel :  
Le switch est bête : il retient l’adresse SOURCE dans la table d’adressage !!! TRES IMPORTANT

**LE SWITCH SERA 100% A L’EXAMENNN !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!**

Comment définir un réseau local techniquement ?  
(voir PPT SL 12)

SL12 : à retenir : un message broadcast passera par toutes les machines dans le bleu pointillé (niveau L2) mais ne passera jamais par du L3

SL.14-15 : voir PPT

SL.21 : adresse logique et physique :

Adresse physique : adresse MAC

Adresses logiques : adresse IPv4 et IPv6 🡪 couche L3 : Network

**PAQUET** : couche L3  
**TRAME**: couche L2

BUT DE LA COUCHE NETWORK : transfert de données ENTRE RESEAUX, définition d’un adressage logique et routage (voir PPT)

IMG paquet : voir PPT SL.26

Orh j’ai la omegaflemme d’ecrire 🡪 tkt frer les slides sont super claires :) ¯\\_(ツ)\_/¯

SL.30 : au dessus : l’adresse réseau (adresse IP); en dessous : le masque réseau

11111111.11111111 🡪 le numéro de réseau  
00000000.00000000 🡪 le numéro de machine

SL.31 : réponse

SL.33 : ***OUTDATED***

SL.35 : A L’EXAM 🡪   
ex : 42.38.200.7/24 : OK ; 42.38.200.**0**/24 : IMPOSSIBLE ; 42.38.200.**255**/24 : IMPOSSIBLE

**25-03-2025**

Rappels de la semaine passée :   
adresse IP : couche L3 Network  
Réseaux  
Switch : couche L2 Datalink -> adresse MAC  
l’adresse MAC ne peut jamais changer, l’adresse IP peut changer

Calculs d’adresses IP : voir slides suppl sur Moodle

SL.40 : adresses IP privées : ces adresses IP sont **privées** à ce réseau, elle ne peuvent pas sortir de leur réseau, et on ne peut rien leur envoyer depuis l’extérieur

SL.43 : réponse : NON.

Protocole ARP : Address Resolution Protocol 🡪 sert à chercher et trouver dans le réseau local l’adresse MAC destination  
-> indispensable dans les réseaux locux

SL.48 : animation

SL suivant

SL.3 : routeur : rôle : amener des paquets d’un point A à un point B  
🡪 sur base d’une logique 🡪 plus intelligent que le switch

SL.4 : les ports en jaune sont un switch 🡪 réseau local  
 arrivée COAX : décodeur

🡪 schéma SL.5

SL.11 : la vitesse peut varier à cause : du type de cable, du blindage du cable, de la longueur du cable, …

SL.13 : les routeurs sont capables de savoir quel sera le « chemin » le plus rapide pour envoyer les données -> la **métrique**.

-jme suis cassé à la pause-

**08/04/2025 (la semaine passée y avait pas cours)**

Rappels semaine passée : (voir PPT pour plus de détails)

AS = ensemble de machines gérée par une entité assez large (Autonomous System) (couche L3)  
(Orange, Proximus, etc)

Utilité de la table de routage : sert à savoir où mener l’information dans le réseau (un peu comme Waze), permet à un routeur de prendre des décisions de routage -> contient le réseau à atteindre, une métrique de distance et le « next hop »

Exemples de métriques de distance : distance en mètre, le type de cable, le blindage du cable, nb sauts (de machines intermédiaires), bande passante, charge, etc

Les adresses privées sont :

* Entre 10.0.0.0 et 10.255.255.255
* Entre 172.16.0.0 et 172.31.255.255
* Entre 192.168.0.0 et 192.168.255.255

Toutes les autres adresses sont des adresses publiques

Entre les AS, on a des BGP. Dans un AS, on a des Statique, des OSPF ou des RIP (protocoles) (le RIP est un vieux protocole qui n’est plus trop utilisé, les gens utilisent l’OSPF mnt)

RIP : ne voit que ses voisins ; alors que OSPF voit tlmd

Le RIP choisit son trajet en fct de son nombre de sauts uniquement et s’en fout du type de câble dcp s’il y a un chemin utilisant moins de sauts avec des cables tout pourris et un autre chemin avec plus de sauts mais des super cables en fibre optique, le RIP choisira le premier chemin.

OSPF = Open Shortest Path First : prend en compte les liaisons et l’état de la bande passante en plus du nombre de sauts (donc mieux que le RIP (R.I.P. le RIP)

On a fini le L3, mnt on passe au L4

Limites de la couche L3 :

* Pas de rattachement entre les paquets
* Pas de réaction en cas de PERTE
* Pas de réaction en cas d’ordre différent

Objectifs de la L4 : considérer les amas de paquets comme un **flux de données** + gestion d’erreur + rassembler les paquets pour former une communication entre processus

(rappel : processus = programme exécuté)

(rappel : le L2 -> trame -> L2  
 L3 -> paquet -> L3)

Pour L4 : L4 -> segment -> L4

Concept de ports : voir PPT

L’adresse IP est comme une boite aux lettres : c cool on sait à quelle boite aux lettres poster le message mais il faudrait savoir à quel habitant de la maison (processus) appartient vrmt le paquet !

Port : boite aux lettres virtuelle pour contacter un processus

L2 : adresse MAC ; L3 : adresse IP ; L4 : Port (source et destination)

Les ports vont de 0 à 65535 (16 bits, 2 bytes)

De 0 à 1023 : ports réservés  
De 1024 à 49151 : assignés officiellement par l’IANA  
De 49152 à 65535 : ports dynamiques

UDP : je prend le message et je l’envoie : aucune fiabilité en cas de perte (bouteille à la mer)

Cas d’usage pour l’UDP (voir PPT SL.35) (des endroits où on a besoin de rapidité)

TCP : on a des ports, mais de manière FIABLE.

ACK pour acknowledge

Numéro de séquence : chaque byte a un numéro de séquence pour identifier et rassembler les données

Ex : H e l l o \_ w o r l d  
H a le num de séq 4000, le e 4001, le l 4002, etc (le 1e num est généré aléatoirement)

3way handshake : établir une connexion (fiable) entre 2 machines

// avec séquences : on incrémente à chaque fois qu’une info est reçue et acknowledged, une valeur est incrémentée pour confirmer que l’info a été reçue. Si une des valeurs n’a pas été incrémentée, c’est que l’info a été perdue.

On utilise le TCP partout où on n’utilise pas l’UTP (là où on préfère la fiabilité à la rapidité)

**15-04-2025**

Rappels semaine passée :

Port = boite aux lettres virtuelle pour contacter un **processus** (machine = immeuble, processus = appart => les deux ont des adresses)

Différence entre TCP et UDP : voir PPT SL.8  
(exemples d’utilisation de l’UDP : jeux vidéo, streaming,…)

**Ce qu’il faut vraiment totalement absolument retenir du cours précédent** :   
**PORTS & TCP/UDP**

Pourquoi deux adresses différentes ?

Chaque machine a une IP privée.  
Les machines peuvent communiquer en interne.  
Les adresses IP privées **ne sortent pas du réseau local !  
Chaque machine a une IPv4 pour communiquer au-delà**

Type NAT (Netork Adress Translation)

->le routeur **remplace l’adresse IP par une adresse IP publique**

3 catégories de NAT (voir PPT SL.15)

NAT Statique : qd tu reçois une IP privée, tu mappes ça dans une table et tu me transformes ça en adresse IP publique (tu = routeur)  
Problème : les adresses IP coutent de l’argent

NAT Dynamique : qd une machine veut sortir du réseau, j’ai dans ma table une liste d’adresses publiques dispo, je prends une de ces adresses pour envoyer les paquets et cette adresse devient occupée. qd l’adresse n’est plus utilisée, je l’indique comme dispo dans ma table.  
Problème : si la machine doit envoyer plein de requêtes en mm temps à plein de machines, elle ne peut utiliser qu’une adresse IP et donc envoyer ses requêtes à une seule machine.

NAT Overlay : le routeur : « la machine [adresse] avec le port [port] veut accéder à [adresse 2], je vais donc lui ouvrir un port [port 2] pour accéder à l’IP [adresse 2]. Pour plus de requêtes, j’ouvrirai d’autres ports. »

Port forwarding : autoriser du trafic entrant via une règle NAT statique

* RISQUE DE SECURITE!!!!!

Pour le reste du cours, on passe en L7 !

Les deux slides suivants sont particulièrement détestées :

SL28 : Liste de ports à connaitre. Liste des ports par défauts attribués à certains protocoles   
***connaitre ce tableau par cœur pour l’examen et savoir le réciter dans les deux sens***

Exemples :

Q : quel est le port 21 ?

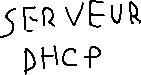
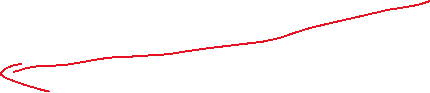
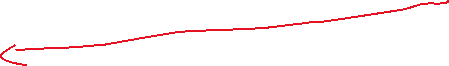
R : Le port 21 est pour le protocole FTP et utilise le TCP

Q : quel est le pot associé au protocole DNS ?

R : Le port 53 et il utilise le TCP et l’UDP.

DHCP : Dynamic Host Configuration Protocol : fournit automatiquement une adresse IP dans un réseau -> gère un « pool » d’adresses disponibles -> une adresse expire au bout d’un moment (parfois : attribution statique (= réservation d’un an par exemple))

4 phases :



(explication SL.suivantes)

(broadcast discover) (discover = broadcast)

Le DHCP est un peu comme le concierge d’un hôtel

DNS = alternative à l’adresse IP pour l’utilisateur  
-> résolution de noms de domaines vers des adresses IP

DNS 🡪 principalement en UDP

Résolution DNS = processus pour accéder à un site via le registre mondial (voir SL.49)  
Client (moi) -> Serveur (Proximus pas ex) -> Root server (connait un peu tout) -> Serveur -> Top-Level Domain server (connait tous les .com) -> Serveur -> etc. …

TOUTE PERSONNE QUI A LA MAIN SUR LE SERVEUR DNS PEUT VOIR OU ON VA !

SL.52 : requête de type A -> Adresse IPv4, etc

Load balancing = technique de répartition de charge

(taper nslookup -type=a <nom\_de\_domaine.com> dans le terminal, c assez sympathique)

**22-04-2025**

PPT de cette séance : L7 Partie 2

À retenir du cours précédent : NAT, DHCP, DNS

QUESTIONS POUR UN CHAMPION :   
nos PCs ont des adresses privées. Grâce au **NAT Overlay,** le routeur transformera l’adresse IP privée en adresse IP publique

Dans l’autre sens, ça s’appelle du **port forwarding**

Différence entre NAT Dynamique et NAT Overlay : l’Overlay utilise des ports, pas le Dynamique (Dynamique et Statique sont des vieux types de NAT)

Rappel : DHCP = le concierge du réseau  
Connaitre et savoir citer les 4 phases d’une requête DHCP  
pk 4 phases ? car il y a plusieurs serv DHCP. Il faut des phases en plus pour avoir le bon serv

Fin des rappels

Qd on fait une recherche google :

1. Le DNS convertit le nom de domaine en adresse IP (ex 20.10.5.10)
   1. Dans le paquet : on met dans le L3 comme IP source l’IP du PC (privée (192.168.10.5)) et comme IP destination l’IP publique (20.10.5.10)  
      (quiz = 0.0.0.0 signifie quoi ? R = 0.0.0.0 = adresse inconnue
   2. Dans la table de routage du PC : Destination : 0.0.0.0, Next Hop : 192.168.0.1 (adresse de la box)
   3. L’IP source du paquet devient l’adresse de la box (192.168.0.1)  
      (le DHCP donne l’adresse de la box au pc)
   * **🡪 Savoir expliquer ça à l’examen !!!**
2. Envoi du paquet à google
3. Connection TCP pour chaque requête/réponse

Protocole HTTP : voir PPT SL.16-17  
http est **stateless** : il ne garde pas de session, il ne sait pas ce qui se passe, juste il transmet les infos et il les envoie  
SL.18 : multiplexage : au lieu de faire « une requête ; une réponse », on fait plusieurs requêtes en mm temps (« images & JS ») et le serveur va renvoyer des bouts d’image et des bouts de JS que le client va reconstituer -> plus efficace que l’HTTP/1.1  
HTTP/1.0 : j’ouvre une connexion, je charge, je ferme, je réouvre une connection,…  
HTTP/1.1 : j’ouvre une connexion, je charge, je garde la connexion ouverte et je continue,…

URL : voir PPT SL.21

Méthodes HTTP : voir PPT SL.25

SL.29 : 1e ligne : requête  
tout le reste : header

Codes SL.31 à évidemment connaitre par cœur

Scaling vertical : augmenter la puissance d’une machine  
Scaling horizontal : augmenter le nombre de machines sans forcément améliorer leur puissance

Ajd : horizontal > vertical

Reverse-proxy : il reçoit la requête et l’envoie vers un backend  
voir PPT SL.37

Partie 2 : FTP

File Transfer Protocol

FTP : non sécurisé -> utiliser le SFTP

2 types de connexion : connexion active ou passive : voir PPT  
passive > active en termes de sécurité

Problème de sécurité : si qqn s’introduit dans ma connexion, il peut lire les mots de passes ! (PASS)