



1 Utilité du modèle OSI

Le modèle OSI est un modèle en 7 couches qui sert à expliquer comment une communication réseau fonctionne, étape par étape. Il ne sert pas seulement à apprendre des couches par cœur. Il sert surtout à comprendre, diagnostiquer et organiser les communications réseau.

Le modèle OSI est utile parce qu'il permet de :

- réduire la complexité ;
- découper la communication réseau en étapes simples ;
- développer les technologies de manière modulaire ;
- faciliter l'interopérabilité entre constructeurs et protocoles ;
- identifier plus facilement où se situe une panne.

♥ **Phrase prof : le modèle OSI permet de découper une communication réseau en couches afin de réduire la complexité, faciliter l'interopérabilité et aider au diagnostic des pannes.**

2 Exemple de diagnostic

Couche 1	câble débranché, fibre, signal, Wi-Fi physique.
Couche 2	adresse MAC, switch, VLAN, STP, trame.
Couche 3	adresse IP, passerelle, routage, ICMP.
Couche 4	port, TCP, UDP, firewall par ports.
Couche 5	session ouverte, maintenue ou fermée.
Couche 6	format, encodage, compression, chiffrement.
Couche 7	service web, DNS, mail, application.



3 La logique à retenir

Support physique -> MAC -> IP -> Port -> Application

Couche 1	transporte les bits sous forme de signaux.
Couche 2	communique localement avec des trames et des adresses MAC.
Couche 3	achemine des paquets IP entre source et destination au niveau réseau.
Couche 4	transporte les données et identifie les services avec les ports.
Couches 5 à 7	session, format des données et services applicatifs.

♥ Phrase importante : la couche 3 concerne l'acheminement réseau ; la couche 4 concerne le transport et les services avec les ports.

4 Correspondance TCP/IP

Modèle TCP/IP	Couches OSI proches
Application	couches OSI 5, 6 et 7
Transport	couche OSI 4
Internet	couche OSI 3
Accès réseau	couches OSI 1 et 2

TCP/IP est plus proche du fonctionnement réel des réseaux IP. Il regroupe certaines fonctions du modèle OSI.



5 Rôle de la couche 1

La couche 1 est la couche physique. Son rôle est de transporter des bits sous forme de signaux sur un support de transmission. Les bits sont des 0 et des 1. Physiquement, ces 0 et 1 doivent être représentés par un signal.

Câble cuivre	signal électrique.
Fibre optique	signal lumineux.
Wi-Fi	ondes radio.

La couche 1 définit notamment le support de transmission, le type de signal, le connecteur, le débit possible, la distance maximale et les caractéristiques électriques, optiques ou radio.

♥ **Phrase prof : la couche 1 transporte les bits sous forme de signaux sur un support physique comme le cuivre, la fibre ou les ondes radio.**

6 Matériel de couche 1

Exemples : câble RJ45, fibre optique, ondes radio, prise réseau, panneau de brassage, connecteur, répéteur, hub, transceiver SFP, convertisseur de média, modem dans sa partie physique.

Un répéteur est un équipement de couche 1. Il régénère ou répète un signal pour prolonger la distance d'une liaison.

♥ **Un répéteur ne lit pas les adresses MAC, ne lit pas les adresses IP, ne route pas et ne filtre pas.**



7 Rôle de la couche 2

La couche 2 assure la communication locale dans un même réseau local ou entre équipements directement voisins.

- elle organise les bits en trames ;
- elle utilise les adresses MAC source et destination ;
- elle contrôle l'accès au support ;
- elle permet la détection d'erreurs au niveau de la trame.

PDU couche 2	trame.
---------------------	--------

Adresse couche 2	adresse MAC.
-------------------------	--------------

Équipement typique	switch de couche 2.
---------------------------	---------------------

8 LLC et MAC

LLC (Logical Link Control) est la sous-couche supérieure de la couche 2.

Elle fait l'interface entre la couche liaison de données et la couche réseau. Elle permet notamment d'identifier le protocole de couche 3 transporté dans la trame et de fournir un contrôle logique de liaison selon le service utilisé.

MAC (Media Access Control) est la sous-couche inférieure. Elle gère l'accès au média, les adresses MAC, le format des trames et les mécanismes liés aux collisions.

♥ **Phrase courte : LLC = contrôle logique de liaison et lien avec la couche 3 ; MAC = accès au support, adresses MAC et trames.**



9 Collisions et méthodes d'accès

Les collisions sont liées à la sous-couche MAC. Une collision peut se produire lorsque plusieurs équipements transmettent en même temps sur un support partagé.

CSMA/CD (Carrier Sense Multiple Access with Collision Detection) est une méthode utilisée historiquement par Ethernet en half-duplex pour détecter les collisions.

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) est utilisée notamment par le Wi-Fi pour éviter les collisions avant l'émission, car les collisions radio sont difficiles à détecter proprement.

♥ Avec les switches modernes en full-duplex, les collisions Ethernet sont normalement évitées.

10 Commutation / Switching

La commutation consiste à faire progresser une trame ou une information réseau vers la bonne sortie.

En couche 2, le switch lit l'adresse MAC de destination, consulte sa table MAC, puis transmet la trame vers le port correspondant.

Store and forward	le switch reçoit toute la trame, la vérifie, puis la retransmet.
Cut-through	le switch commence à retransmettre dès qu'il a lu l'adresse de destination.



11 VLAN, IEEE 802.1Q et normes importantes

Un VLAN signifie Virtual Local Area Network. Il sert à découper logiquement un même réseau local commuté en plusieurs réseaux locaux virtuels.

Concrètement, sur un même switch physique, on peut séparer les machines en plusieurs groupes réseau.

Un VLAN sépare surtout des domaines de broadcast : une trame de broadcast envoyée dans le VLAN 10 ne va pas automatiquement dans le VLAN 20.

Port access	port associé généralement à un seul VLAN.
Port trunk	port qui transporte plusieurs VLAN.
IEEE 802.1Q	standard qui ajoute un tag VLAN dans les trames Ethernet.

Normes IEEE importantes

Notion	Norme
Ethernet	IEEE 802.3
Wi-Fi	IEEE 802.11
VLAN	IEEE 802.1Q
STP	IEEE 802.1D

♥ **À retenir : VLAN = séparation logique d'un réseau local commuté en domaines de broadcast ; IEEE 802.1Q = tag VLAN sur les trunks.**

12 STP - Spanning Tree Protocol

STP est un protocole de couche 2 utilisé sur les switches pour éviter les boucles réseau.

Quand plusieurs chemins existent entre switches, STP construit une topologie logique sans boucle. Il garde certains liens actifs et bloque certains liens redondants.

Sans STP, une boucle de couche 2 peut provoquer une tempête de broadcast, des trames qui tournent en boucle, une instabilité des tables MAC et une saturation du réseau.

♥ **Phrase prof : STP évite les boucles entre switches en bloquant certains chemins redondants.**



13 Rôle de la couche 3

La couche 3 est la couche réseau. Son rôle n'est pas seulement l'adressage IP : l'adressage IP est une information importante, mais le rôle de la couche 3 est plus large.

La couche 3 assure l'acheminement des paquets IP entre une source et une destination au niveau réseau, à travers un ou plusieurs réseaux.

- adressage logique ;
- routage ;
- choix du chemin ;
- communication entre réseaux.

PDU couche 3	paquet IP.
---------------------	------------

Adresses couche 3	IP source et IP destination.
--------------------------	------------------------------

♥ **Correction prof : ici, on parle de source et destination au niveau réseau. La notion de service ou de processus appartient plutôt à la couche 4.**

14 Routage / Routing

Le routage est le processus qui consiste à choisir le chemin qu'un paquet IP doit emprunter pour atteindre sa destination.

Un routeur consulte sa table de routage pour choisir l'interface de sortie ou le prochain saut.

Route	indication pour atteindre un réseau.
--------------	--------------------------------------

Route par défaut	route utilisée si aucune route plus précise ne correspond.
-------------------------	--

Prochain saut / Next hop	équipement suivant vers la destination.
---------------------------------	---

Préfixe le plus long	règle qui choisit la route la plus spécifique.
-----------------------------	--



15 Routeur et passerelle

Un routeur est un équipement de couche 3 qui relie plusieurs réseaux IP. Il utilise une table de routage pour savoir où envoyer les paquets.

Une passerelle est une fonction de routage utilisée pour sortir d'un réseau local. La passerelle par défaut d'une machine est souvent l'adresse IP du routeur vers lequel elle envoie les paquets destinés à d'autres réseaux.

♥ Une passerelle est souvent un routeur utilisé comme sortie du réseau. Mais un routeur n'est pas forcément la passerelle par défaut de toutes les machines.

16 ARP, ICMP et firewall

ARP associe une adresse IPv4 à une adresse MAC sur le réseau local.

ICMP est un protocole de contrôle de la couche réseau, utilisé par IP pour signaler des erreurs ou donner des informations sur la communication réseau. Il est notamment utilisé par ping avec les messages Echo Request / Echo Reply, mais sert aussi à signaler une destination inaccessible, un délai dépassé ou un problème d'acheminement.

Un firewall peut travailler à plusieurs couches : couche 3 avec les adresses IP, couche 4 avec TCP/UDP et les ports, et parfois couche 7 avec les informations applicatives.

♥ Firewall L3 = IP ; firewall L4 = TCP/UDP et ports ; firewall L7 = informations applicatives.

Page 9 - Couche 4 : Transport

TCP, UDP, ports et sockets



Page 9 / 15

17 Définition corrigée de la couche 4

La couche 4 assure le transport des données entre deux extrémités de communication.

Elle utilise TCP ou UDP et des numéros de ports pour identifier les services concernés sur les machines source et destination.

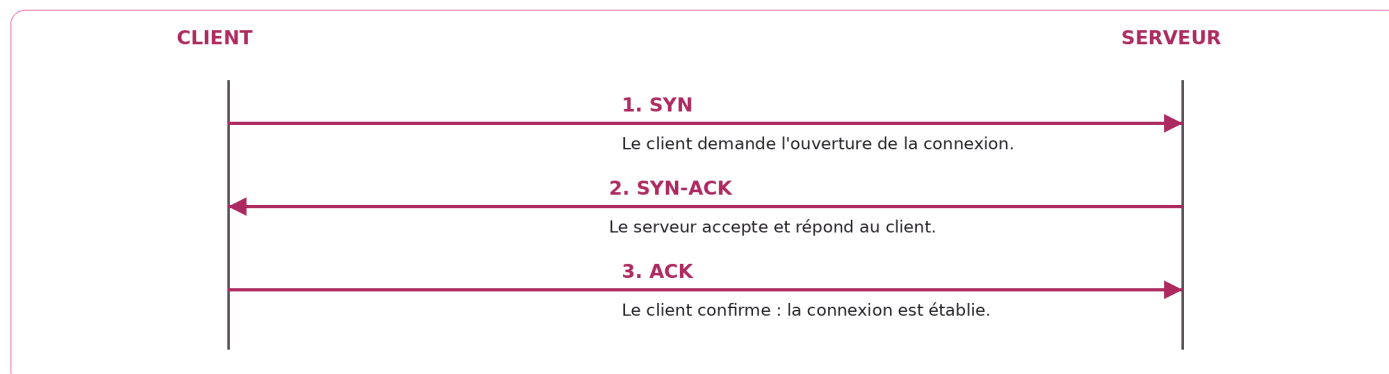
♥ **Formulation à garder : la couche 4 transporte les données entre extrémités et identifie les services avec les ports.**

18 TCP, UDP, ports et socket

TCP	protocole fiable, orienté connexion, avec accusés de réception.
UDP	protocole simple, sans connexion, sans garantie de livraison.
Port source	port souvent temporaire utilisé par la machine qui initie l'échange.
Port destination	port du service que l'on cherche à joindre.
Socket	adresse IP + port + protocole.
Flux réseau	protocole + IP source + port source + IP destination + port destination.

Mémo : Couche 4 = transport entre extrémités + identification des services avec les ports.

19 Schéma du 3-way handshake



20 Détail des étapes

1. SYN : le client demande l'ouverture d'une connexion TCP au serveur.
2. SYN-ACK : le serveur accepte la demande, répond au client et synchronise aussi sa propre connexion.
3. ACK : le client confirme la réponse du serveur.

♥ Après SYN -> SYN-ACK -> ACK, la connexion TCP est établie et les données peuvent être échangées.



21 TCP / UDP

TCP est un protocole de transport fiable et orienté connexion. Il établit une connexion avant l'échange de données, vérifie que les données arrivent correctement et peut redemander ce qui a été perdu.

UDP est un protocole plus simple, plus léger et sans connexion. Il ne garantit ni la livraison, ni l'ordre, ni la retransmission.

♥ **TCP = fiable, avec connexion. UDP = rapide, sans connexion, sans garantie de livraison.**

22 Drapeaux TCP principaux

SYN	demande d'ouverture de connexion.
ACK	accusé de réception.
FIN	fermeture normale d'une connexion.
RST	réinitialisation ou coupure brutale.
PSH	demande de transmission rapide à l'application.
URG	données urgentes, rarement utilisé aujourd'hui.

Mémo : TCP = fiable avec connexion ; UDP = simple, rapide, sans connexion.



23 NAT - Network Address Translation

NAT traduit une adresse IP en une autre adresse IP.

Il est souvent utilisé pour permettre à des machines en adresse privée d'accéder à Internet avec une adresse publique.

Exemple : plusieurs postes en 192.168.x.x peuvent sortir vers Internet via l'adresse IP publique de la box ou du routeur.

♥ NAT ne remplace pas un pare-feu : traduire une adresse et filtrer le trafic sont deux fonctions différentes.

24 PAT, NAPT et redirection

PAT (Port Address Translation) différencie plusieurs connexions grâce aux ports. Il permet à plusieurs machines privées de partager une même adresse IP publique.

NAPT traduit simultanément les adresses IP et les ports.

NAT	traduction d'adresse IP.
PAT	distinction par ports.
NAPT	traduction IP + ports.
Port forwarding	redirection d'un port public vers un service interne.



25 Firewall L3 / L4 / L7

Un pare-feu contrôle le trafic réseau selon des règles. Il peut autoriser, bloquer ou journaliser des flux.

Firewall L3	filtre selon IP source, IP destination et protocole IP.
Firewall L4	filtre selon TCP, UDP et les ports source ou destination.
Firewall L3/L4	règle du type : telle IP vers telle IP sur tel port.
Stateful	suit l'état des connexions.
Stateless	applique les règles paquet par paquet.
Firewall L7	analyse des informations applicatives.

26 Proxy, reverse proxy et WAF

Un proxy est un serveur intermédiaire entre un client et une ressource réseau. Il relaie les requêtes et peut filtrer, journaliser ou contrôler l'accès.

Un reverse proxy est placé côté serveur. Il reçoit les requêtes des clients et les transmet vers un ou plusieurs serveurs internes.

Un WAF (Web Application Firewall) est un pare-feu applicatif spécialisé dans la protection des applications web. Il analyse les requêtes HTTP/HTTPS pour bloquer certaines attaques applicatives.

♥ **Firewall L3/L4 = IP et ports. WAF = protection applicative web.**



27 Couche 5 - Session

La couche 5 gère la session de communication entre deux machines ou deux applications.

- ouverture de la session ;
- maintien du dialogue ;
- fermeture de la session ;
- organisation des échanges entre les deux côtés.

PDU Données.

Phrase simple Couche 5 = gérer la session / le dialogue.

♥ Dans la pratique TCP/IP, ces fonctions sont souvent gérées directement par les applications ou leurs protocoles.

28 Couche 6 - Présentation

La couche 6 s'occupe de la forme des données pour qu'elles soient compréhensibles par l'application qui les reçoit.

- encodage des caractères, par exemple ASCII ou UTF-8 ;
- formats de données, par exemple JPEG, PNG, JSON, PDF ;
- compression ;
- chiffrement et déchiffrement, selon la manière dont le cours présente TLS.

PDU Données.

Phrase simple Couche 6 = format, encodage, compression, chiffrement.

29 Couche 7 - Application

La couche 7 correspond aux services réseau utilisés par les applications.

Attention : la couche 7 n'est pas forcément le logiciel lui-même, comme Chrome ou Outlook. Elle correspond surtout aux protocoles et services utilisés par ces logiciels.

- HTTP / HTTPS = web ;
- DNS = résolution de noms ;
- SMTP / IMAP / POP3 = messagerie ;
- FTP / SFTP = transfert de fichiers ;
- SSH = accès distant sécurisé.

PDU Données.

Phrase simple Couche 7 = services et protocoles proches de l'utilisateur.

♥ DNS a un port en couche 4, mais le service DNS se comprend aussi en couche 7.

À retenir pour l'oral

Couche 5 gère la session et le dialogue.

Couche 6 gère le format des données.

Couche 7 gère les services applicatifs.

Mémo : Couches 5 à 7 = dialogue, format des données, services applicatifs.



30 Réponses propres à l'oral

À quoi sert le modèle OSI ?

Il découpe une communication réseau en couches. Il réduit la complexité, facilite l'interopérabilité, permet un développement modulaire et aide au diagnostic.

Rôle de la couche 1 ?

Elle transporte les bits sous forme de signaux sur un support physique.

Rôle de la couche 2 ?

Elle assure la communication locale avec des trames et des adresses MAC. Elle se divise en LLC et MAC.

Rôle de la couche 3 ?

Elle achemine des paquets IP entre une source et une destination au niveau réseau, à travers un ou plusieurs réseaux.

Rôle de la couche 4 ?

Elle assure le transport des données entre deux extrémités de communication et utilise TCP/UDP ainsi que les ports pour identifier les services.

31 Résumé final

Couche 1	bits, signaux et support physique.
Couche 2	trames, MAC, communication locale, VLAN, STP.
Couche 3	paquets IP, source/destination réseau, routage.
Couche 4	TCP/UDP, ports, transport et services.
Couches 5 à 7	session, format, services applicatifs.
NAT/PAT	traduction d'adresses et distinction par ports.
Firewall/WAF	filtrage réseau et protection applicative.