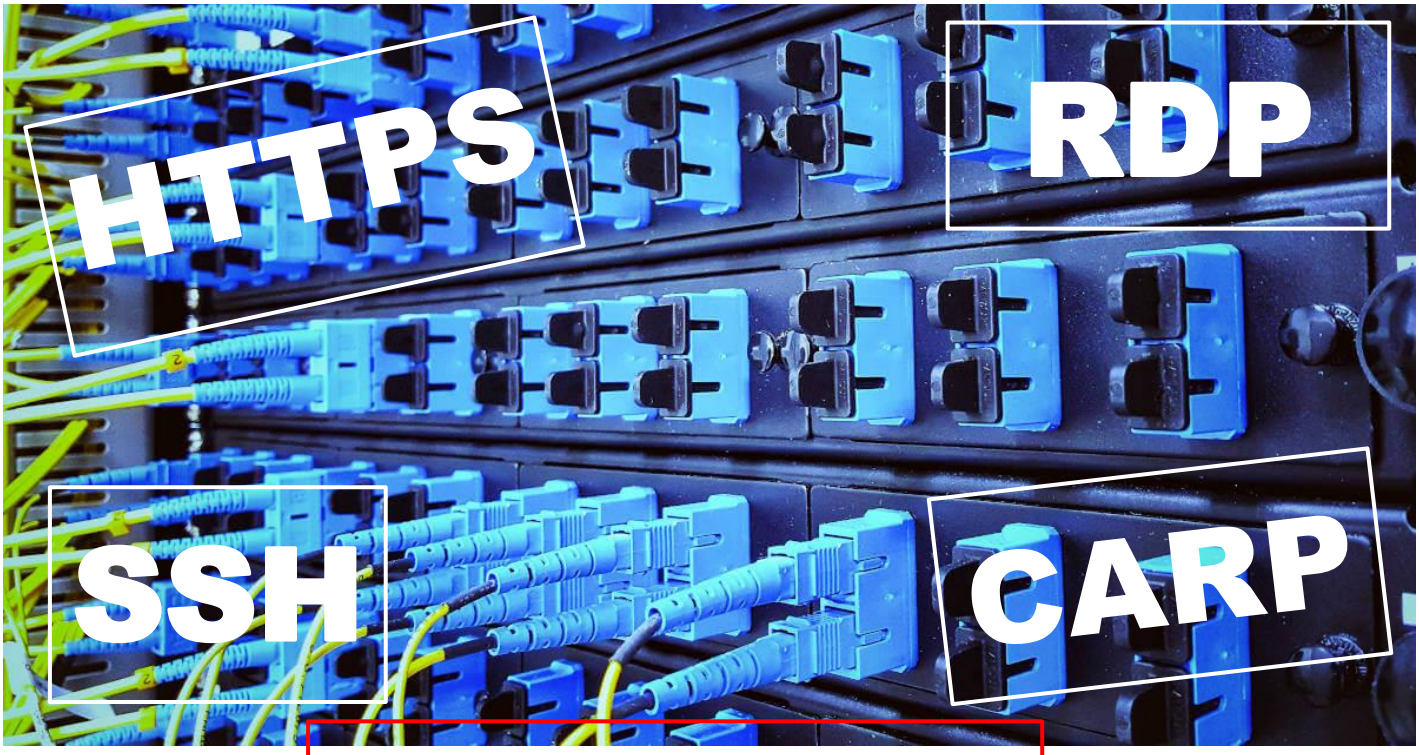
TUTOS-INFO
L'informatique par l'exemple

DOCUMENT

Comprendre les notions de PORTS PROTOCOLES



TCP/UDP

1 – QU'EST-CE QU'UN PORT ET QU'EST-CE QUE LE MODELE OSI ?

Un **port** est un **point virtuel où les connexions réseau commencent et se terminent**. Les ports sont **basés sur des logiciels et gérés par le système d'exploitation** d'un ordinateur. Chaque port est associé à un processus ou à un service spécifique.

Les ports **permettent** aux ordinateurs **de différencier facilement les différents types de trafic** : les courriers électroniques sont acheminés vers un port différent de celui des pages web même si les deux atteignent un ordinateur via la même connexion Internet.

Les ports sont normalisés sur tous les périphériques connectés au réseau, et **un numéro est attribué à chaque port**. La plupart des **ports sont réservés** à certains **PROTOCOLES**. Par exemple, tous les messages Hypertext Transfer Protocol (**HTTP**) vont au port **80**.

Alors que **les adresses IP permettent aux messages d'aller vers et depuis des périphériques spécifiques, les numéros de port permettent de cibler des services ou des applications spécifiques** au sein de ces périphériques.

On dénombre 65 535 ports normalisés (liste complète ici : liste complète

Le **modèle « OSI » est un modèle conceptuel du fonctionnement de l'Internet**.

Le **modèle OSI a été établi en 1984** afin de créer une **norme pour la conception des réseaux et la fabrication des équipements**.

Sans le modèle OSI, il n'y aurait pas de méthode standard pour concevoir l'infrastructure et les protocoles utilisés pour la communication : il serait donc plus difficile pour les administrateurs d'installer de nouveaux équipements et de les intégrer à des réseaux autres que le leur.

Grâce à ces normes, les administrateurs peuvent concevoir leur propre infrastructure, mais l'équipement peut toujours communiquer avec les autres de manière universelle.

Lorsque le modèle OSI a été établi, **7 couches ont été définies** pour établir des principes :

- Chaque couche possède un niveau d'abstraction distinct.
- Chaque couche remplit une fonction définie.
- Les couches sont définies pour créer des protocoles internationaux normalisés.
- Les couches facilitent la communication entre l'infrastructure et les applications.
- Chaque couche correspond à une fonction spécifique dans la communication réseau.

La normalisation de la communication à travers un réseau, y compris les réseaux externes (le cloud par exemple), facilite la communication indépendamment de l'endroit où les données sont envoyées ou d'où elles sont reçues.

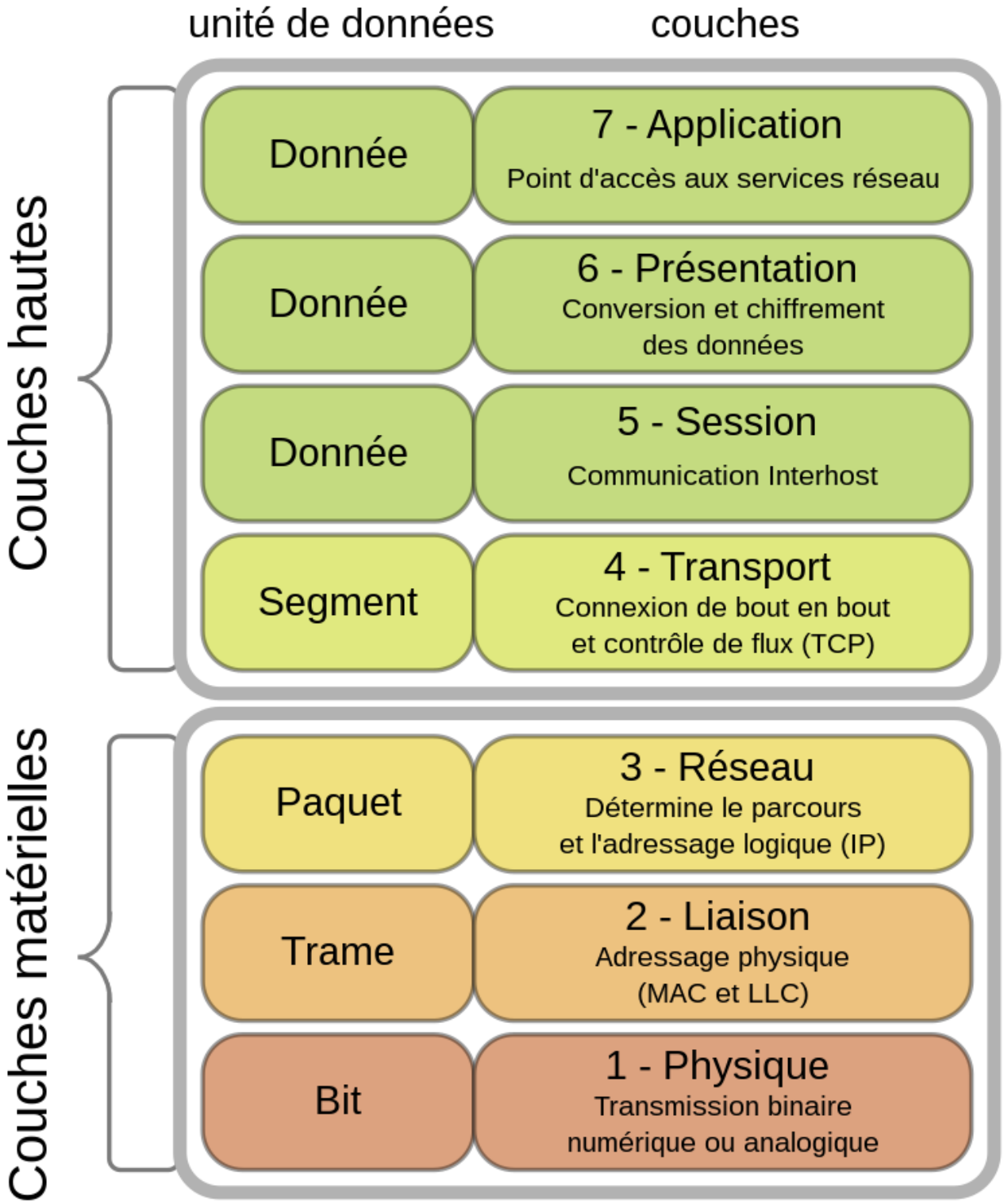
Le modèle OSI permet aux fabricants de créer leurs propres protocoles et normes d'équipement tout en permettant l'interconnexion avec d'autres fabricants.

Un autre avantage du modèle OSI qu'il est facile à dépanner. Lorsqu'un composant du réseau tombe en panne ou qu'une application ne communique pas avec le réseau, le modèle OSI aide les administrateurs à déterminer la couche et le composant défaillants.

La normalisation de la technologie moderne facilite la construction, la fabrication, le dépannage et la conception de nouvelles technologies à l'avenir.

PRESENTATION DU MODELE OSI

Les 7 couches du modèle OSI sont présentées ci-dessous et sont expliquées page suivante.



2 – LES 7 COUCHES DU MODELE OSI

Chaque couche a une fonction spécifique et communique et travaille avec les couches inférieure et supérieure.

Le modèle OSI est conceptuel, mais sa conception permet une communication à la fois physique et virtuelle sur un réseau. Nous allons commencer par la couche 7, qui est la couche la plus élevée de la pile.

Couche 7 – La couche d'application

La couche 7 est connue de la plupart des gens car **elle communique directement avec l'utilisateur**. Une application qui s'exécute sur un appareil peut communiquer avec d'autres couches OSI, mais l'interface fonctionne sur la couche 7. Par exemple, un client de messagerie qui transfère des messages entre le client et le serveur fonctionne sur la couche 7. Lorsqu'un message est reçu sur le logiciel client, c'est la couche application qui le présente à l'utilisateur.

Les protocoles d'application comprennent le SMTP (Simple Mail Transfer Protocol) et le HTTP, qui est le protocole de communication entre les navigateurs et les serveurs Web.

Couche 6 – La couche de présentation

Nous avons mentionné que la couche application affiche les informations aux utilisateurs, mais la couche présentation du modèle OSI est celle qui **prépare les données pour qu'elles puissent être affichées à l'utilisateur**. Il est courant que deux applications différentes utilisent l'encodage. Par exemple, la communication avec un serveur Web via HTTPS utilise des informations chiffrées. La couche de présentation est responsable de l'encodage et du décodage des informations afin qu'elles puissent être affichées en clair.

La couche de présentation est également responsable de la compression et de la décompression des données lorsqu'elles passent d'un appareil à un autre.

Couche 5 – La couche session

Pour communiquer entre deux appareils, **une application doit d'abord créer une session**, qui est unique à l'utilisateur et l'identifie sur le serveur distant. La session doit être ouverte suffisamment longtemps pour que les données soient transférées, mais elle doit être fermée une fois le transfert terminé. Lorsque de gros volumes de données sont transférés, la session est chargée de s'assurer que le fichier est transféré dans son intégralité et que la retransmission est établie si les données sont incomplètes.

Par exemple, si 10 Mo de données sont transférés et que seuls 5 Mo sont complets, la couche session s'assure que seuls 5 Mo sont retransmis. Ce transfert rend la communication sur un réseau plus efficace au lieu de gaspiller des ressources et de retransférer l'intégralité du fichier.

Couche 4 – La couche de transport

La couche transport est chargée de prendre les données et de les décomposer en petits morceaux. Lorsque des données sont transférées sur un réseau, elles ne sont pas transférées en un seul paquet.

Pour rendre les transferts plus efficaces et plus rapides, **la couche transport divise les données en segments** plus petits. **Ces petits segments contiennent des informations d'en-tête qui peuvent être réassemblées sur le périphérique cible**.

Les données segmentées sont également dotées d'un **contrôle d'erreur** qui indique à la couche session de rétablir une connexion si les paquets ne sont pas entièrement transférés au destinataire cible.

Couche 3 – La couche réseau

La couche réseau est **chargée de décomposer les données sur l'appareil de l'expéditeur et de les réassembler sur l'appareil du destinataire lorsque la transmission s'effectue sur deux réseaux différents**.

Lorsque l'on communique au sein d'un même réseau, la couche réseau est inutile, mais la plupart des utilisateurs se connectent à d'autres réseaux, tels que les réseaux dans le cloud.

Lorsque les données traversent différents réseaux, la couche réseau est chargée de créer de petits paquets de données acheminés vers leur destination, puis reconstruits sur l'appareil du destinataire.

Couche 2 – La couche de liaison de données

La couche réseau facilite la communication entre différents réseaux, mais **la couche liaison de données est responsable du transfert des informations sur le même réseau**.

La couche liaison de données **transforme les paquets reçus de la couche réseau en trames**. Tout comme la couche réseau, la couche liaison de données est **responsable du contrôle des erreurs** et du flux pour garantir la réussite de la transmission.

Couche 1 – La couche physique

Comme son nom l'indique, la couche physique est **responsable de l'équipement qui facilite le transfert des données**, comme les **câbles** et les **routeurs** installés sur le réseau. Cette couche est l'un des aspects de la transmission réseau où **les normes sont essentielles**. Sans normes, la transmission entre les appareils de différents fabricants est impossible.

3 – LES PRINCIPAUX PORTS ET PROTOCOLES ASSOCIES A CONNAITRE

Des types de données très différents circulent vers et depuis un ordinateur sur la même connexion réseau. **L'utilisation de ports aide les ordinateurs à comprendre ce qu'ils doivent faire avec les données qu'ils reçoivent**.

Supposons que Bob transfère un enregistrement audio MP3 à Alice en utilisant le protocole de transfert de fichiers (FTP). Si l'ordinateur d'Alice transmettait les données du fichier MP3 à l'application de messagerie d'Alice, cette dernière ne saurait pas comment les interpréter. Mais comme le transfert de fichiers de Bob utilise le port désigné pour le FTP (port 21), l'ordinateur d'Alice est en mesure de recevoir et de stocker le fichier.

Pendant ce temps, l'ordinateur d'Alice peut charger simultanément des pages web HTTP en utilisant le port 80, même si les fichiers de la page web et le fichier audio MP3 arrivent sur l'ordinateur d'Alice par la même connexion WiFi.

Les ports sont un concept de la couche transport (couche 4). **Seul un protocole de transport** tel que le protocole **TCP** (Protocole de Contrôle de Transmission) ou le **UDP** (Protocole de Datagramme Utilisateur) **peut indiquer à quel port un paquet doit être envoyé**. La notion de protocole TCP/UDP est expliquée dans les pages suivantes (voir point 4).

Il existe 65 535 numéros de port possibles, mais tous ne sont pas utilisés couramment.

Voici quelques-uns des ports les plus couramment utilisés, ainsi que le protocole réseau et le service qui leur est associé :

PORT	PROTOCOLE	SERVICE ASSOCIE
20/21	tcp	Le protocole **FTP** permet de **transférer des fichiers** entre un client et un serveur. Le port 21 correspond au flux de contrôle pour le transfert.
22	tcp	Utilisé par **SSH** qui est l'un des nombreux **protocoles de tunneling qui créent des connexions réseau sécurisées**.
25	tcp	Historiquement, **SMTP** est **utilisé pour le courrier électronique.**
53	udp	Utilisé par le **DNS** qui est un processus essentiel pour l'Internet moderne ; il **fait correspondre les noms de domaines lisibles par l'homme aux adresses IP lisibles par la machine**, ce qui permet aux utilisateurs de charger des sites Web et des applications sans avoir à mémoriser une longue liste d'adresses IP.
67/68	udp	Attribuent et suivent les adresses IP dynamiques et d'autres paramètres de configuration réseau (**DHCP**).
80	tcp	Protocole de transfert hypertexte, le **HTTP** est le **protocole qui rend le World Wide Web possible**.
110	tcp	**POP3** : reçoit et conserve les courriels à télécharger depuis le serveur Internet.
123	udp	Utilisé par le **NTP** qui **permet aux horloges des ordinateurs de se synchroniser entre elles, un processus essentiel pour le chiffrement**.
389	tcp	Utilisé par **LDAP** pour **accéder à des attributs et des objets** d'utilisateur au sein **d'un service Active Directory**.
443	tcp	**HTTPS** est la **version sécurisée et cryptée de HTTP**.
3306	tcp	Utilisé par **MYSQL**
3389	tcp	Lle protocole **RDP** permet aux utilisateurs de **se connecter à distance à leur ordinateur de bureau** depuis un autre périphérique.
8006	tcp	Utilisé par **l'interface web de Proxmox**.

L'Internet Assigned Numbers Authority (**IANA**) tient à jour la liste complète des numéros de port et des protocoles qui leur sont attribués.

4 – C'EST QUOI TCP/UDP ?

TCP ET UDP

Qu'est-ce que TCP (protocole de contrôle de transmissions) ?

Le protocole de contrôle de transmissions "**TCP**" (Transmission Control Protocol) est l'un des principaux moyens de transmission des données entre les réseaux sur Internet.

Il s'agit d'un **protocole de communication orienté connexion** qui permet aux appareils et applications informatiques **d'envoyer des données et d'en vérifier la livraison**.

Qu'est-ce qu'UDP (protocole de datagramme utilisateur) ?

"**UDP**" (protocole de datagramme utilisateur) est l'un des protocoles qui **permet le transfert de données entre les réseaux sur Internet**.

Il s'agit d'un **protocole de communication orienté message** qui permet aux appareils et applications informatiques **d'envoyer des données, sans en vérifier la livraison**. UDP est le mieux adapté à la communication en temps réel et aux systèmes de diffusion.

Quelles sont les trois différences entre TCP et UDP ?

1. **TCP exige une connexion fiable** entre le serveur et le destinataire, **ce qui peut ralentir le transfert de données**. **UDP est un protocole sans connexion, donc beaucoup plus rapide**.

2. **TCP garantit une transmission sans faille** des données, même si les paquets perdus ou endommagés sont retransmis. **UDP est un protocole « tire et oublie » qui ne vérifie pas les erreurs et ne renvoie pas les paquets de données perdus**.

3. **UDP est plus adapté à la diffusion et au streaming en direct**. **TCP est préférable pour les communications directes (mails, navigation Web ou transfert de fichiers).**

À quoi servent les protocoles TCP et UDP ?

TCP est de préférence **utilisé** pour les communications directes nécessitant une connexion fiable (**navigation Web, e-mails, SMS et transfert de fichiers**).

UDP sert de préférence pour la **transmission de données en direct et en temps réel**, lorsque la **vitesse est plus importante que la fiabilité**. UDP est normalement utilisé pour les **jeux en ligne**, le **streaming** en direct et les protocoles DNS.

Les ports TCP sont-ils différents des ports UDP ?

Oui, **les ports TCP et UDP sont différents, mais ils utilisent parfois le même numéro de port**. Par exemple, UDP/53 et TCP/53 sont tous deux utilisés pour le DNS, mais il s'agit de types de connexion différents. Les ports TCP sont conformes aux protocoles de contrôle de transmissions, tandis que les ports UDP sont conformes aux protocoles de datagramme utilisateur.

5 – POURQUOI FAUT-IL BLOQUER DES PORTS DANS UN PARE-FEU ?

Un pare-feu est un système de sécurité qui surveille et contrôle le trafic réseau en fonction d'un ensemble de règles de sécurité. Le pare-feu se dresse généralement entre un réseau de confiance et un réseau sans relation de confiance. **Le réseau non fiable est souvent Internet**. Par exemple, les réseaux de bureaux utilisent souvent un pare-feu pour protéger leur réseau des menaces en ligne.

Certains attaquants essaient d'envoyer du trafic malveillant à des ports aléatoires en espérant que ces ports ont été laissés « ouverts », signifiant qu'ils sont capables de recevoir du trafic. Cette action ressemble un peu à celle d'un voleur de voitures qui se promène dans la rue et essaie les portes des véhicules garés, en espérant que l'une d'entre elles soit déverrouillée.

C'est pourquoi le pare-feu doit être configuré pour bloquer le trafic réseau dirigé vers la plupart des ports disponibles. Il n'y a aucune raison légitime pour que la grande majorité des ports disponibles reçoivent du trafic.

Le pare-feu correctement configuré bloque par défaut le trafic vers tous les ports, à l'exception de quelques ports prédéterminés connus pour être d'usage courant. Par exemple, un pare-feu d'entreprise pourrait ne laisser ouverts que les ports 25 (courrier électronique), 80 (trafic web), 443 (trafic web) et quelques autres, permettant ainsi aux employés internes d'utiliser ces services essentiels, puis **bloquer le reste des plus de 65 000 ports**.