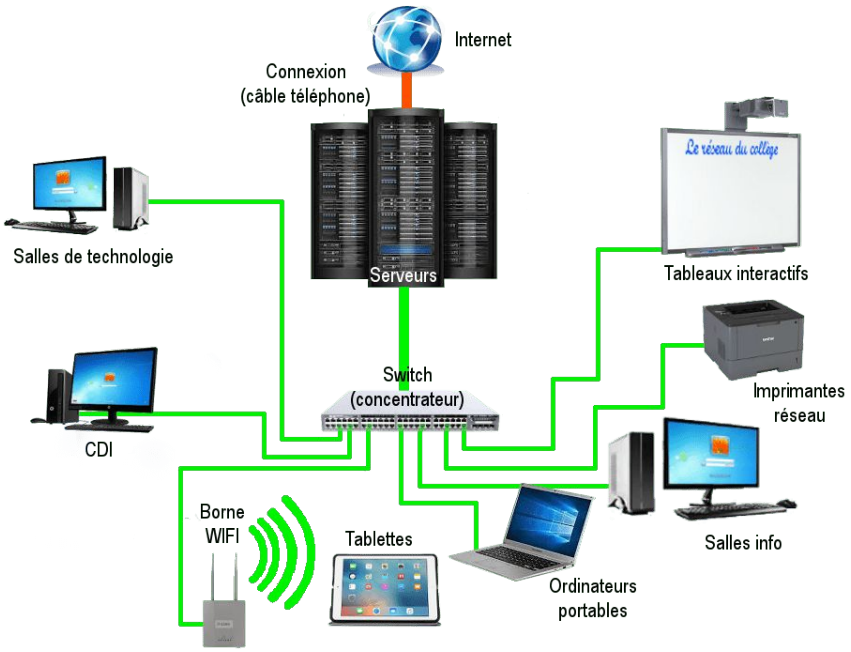
Introduction aux Réseaux Informatiques

bstorm TRAINING

Qu’est-ce qu’un réseau ?



Un réseau est un ensemble de machines connectées entre elles.

Il permet d’échanger des informations (fichiers, messages…).

Les réseaux peuvent être petits ou très grands (ex: Internet).

Pourquoi les réseaux ?

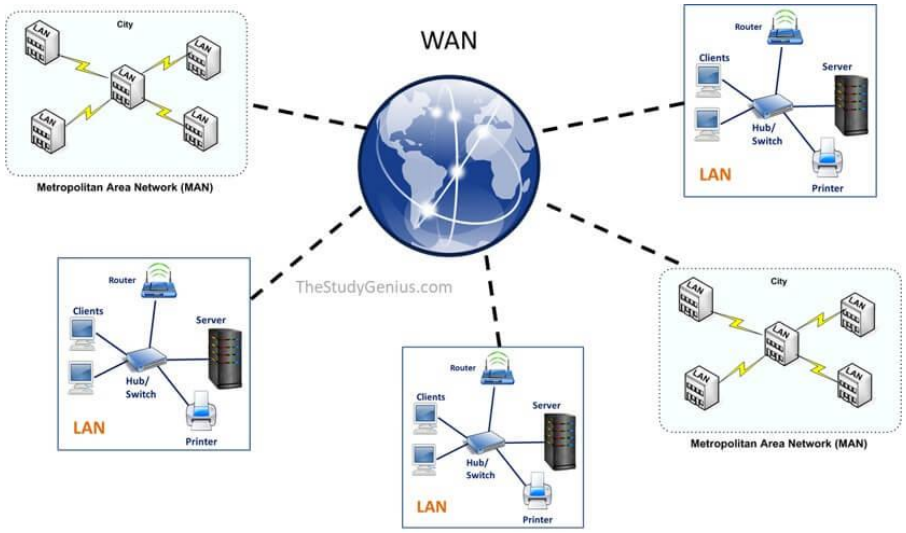
- Partager des ressources (imprimantes, fichiers…).
- Communiquer rapidement (emails, visio…).
- Accéder à Internet et aux services en ligne.

Types de réseaux

PAN – Personal Area Network - Il s'agit d'un réseau personnel à très courte portée, utilisé pour connecter des appareils autour d'une personne (ex: Bluetooth).

LAN – Local Area Network- Réseau à portée limitée (ex: réseau domestique, réseau d'un campus universitaire).

Types de réseaux



WAN – Wide Area Network - Il s'agit d'un réseau étendu couvrant une large zone géographique, souvent à l'échelle nationale ou mondiale (ex: Internet).

Les WAN permettent d'interconnecter plusieurs LAN ou autres réseaux via des technologies longues distance (Fibre, Satellite, Réseau Mobile, Réseaux radios etc)

Réseaux sans fil

WLAN – Réseau local sans fil (Wi-Fi).

Réseaux Cellulaires: 2/3/4/5G

VPN – Virtual Private Network, pour créer un tunnel sécurisé sur Internet.

Éléments physiques

Un réseau se compose de différents éléments physiques permettant sa mise en place.

⇒ La carte réseau.

Elle est le composant matériel qui permet à un appareil de se connecter à un réseau. Elle se charge de fournir une adresse physique à l'appareil auquel elle est associée. Il s'agit de l'adresse MAC, fournie par le fabricant de la carte réseau.

⇒ Les câble et autre supports de transmission

Ils permettent de transporter les données entre les appareils

Éléments physiques

=> Les commutateurs, aussi appelés switch

Composé de plusieurs port Ethernet, ils vont permettre de connecter plusieurs appareils sur un réseau local et gérer les flux de données.

Ils assurent entre autre la transmission de données vers les appareils concernés tout en jouant un rôle de multiprise intelligente pour le trafic réseau.

Éléments physiques

⇒ Le routeur

Le routeur est un équipement essentiel qui assure la liaison entre plusieurs réseaux, notamment entre LAN et WAN

C'est lui qui fourni le NAT (Network Address Translation) qui réalise la traduction des adresses IP de votre réseau local en adresse IP publique attribuée par le FAI (fournisseur d'accès à Internet)

Le routeur fournit souvent un service **DHCP**, qui attribue automatiquement une **adresse IP**, un **masque de sous-réseau**, une **passerelle**, et des **DNS** à chaque appareil connecté au réseau local.

Éléments physiques

⇒ Le modem

Le modem est l'élément qui permet de se connecter à internet via un FAI.

Son rôle sera de convertir les signaux numériques du réseau local en signaux exploitables sur les lignes téléphoniques, fibre optique, câble ou 4G/5G et inversement.

Le mot MODEM vient de MODulateur / DÉModulateur

Note: De nos jours, les FAI fournissent une "box internet" appelés "modem-routeur". Elles cumulent au minimum les deux rôles.

Connexion logique

Une connexion logique représente la manière dont deux appareils communiquent au niveau **logiciel.**

- Les éléments physique permettent d'établir une connexion
- La connexion logique permet de traiter l'information envoyée/reçue

Connexion logique

La connexion logique va établir un lien entre deux machines.

Elle va vérifier:

- L’adresse de l'émetteur
- L’adresse du destinataire
- La séquence d’envoi
- La vérification de l’intégrité des données (checksum)

Fonctionnement d’un réseau

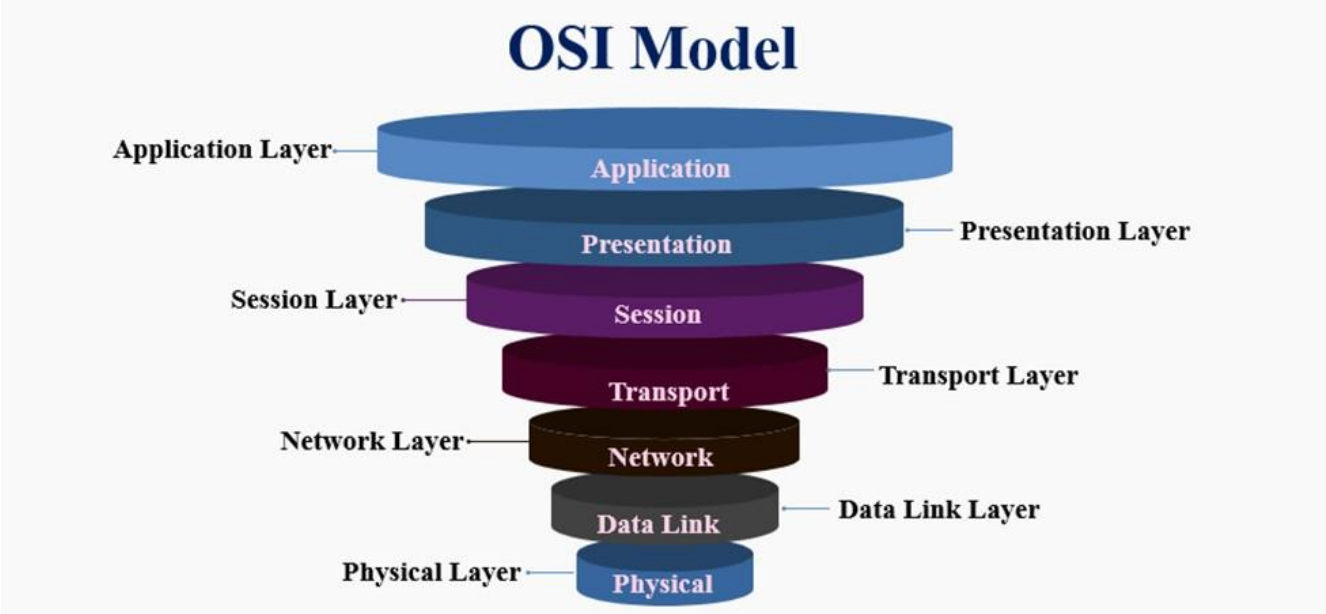
Le fonctionnement général d’un réseau repose sur l’interaction entre les éléments physiques, qui assurent la transmission des données, et les connexions logiques, qui organisent ces échanges selon des règles bien définies. Ensemble, ils permettent aux réseaux de transmettre efficacement des informations.

Fonctionnement d'un réseau

Pour qu'un transfert d'information de bout en bout soit réussi, il est nécessaire de suivre un ensemble de règles normalisées appelées protocoles de communication. Ces protocoles définissent les étapes, le format et les conditions de l'échange de données entre les équipements d'un réseau.

Afin d'assurer une compatibilité universelle et une bonne organisation, ces protocoles sont regroupés au sein de modèles standardisés, comme le modèle OSI ou le modèle TCP/IP, qui structurent les fonctions du réseau en couches hiérarchisées.

Modèle OSI - Vue d'ensemble



Standard en 7 couches pour organiser les réseaux.

Chaque couche a un rôle précis.

Les données passent de couche en couche jusqu'au destinataire.

Modèle OSI - Couche 1 : Physique

Transmet des bits via câbles, fibres ou ondes.

Spécifie les caractéristiques électriques, mécaniques et de signal.

Exemples : Ethernet (câble), Wi-Fi, fibre optique

=> tout ce qui transmet un signal brut (bits).

Modèle OSI - Couche 2 : Liaison de données

Assure une liaison fiable entre machines connectées.

Assure le transport des trames + adressage MAC

Exemples : Ethernet, Wi-Fi, Switch, VLAN,...

Modèle OSI - Couche 3 : Réseau

Gère l'adressage IP et le routage des paquets.

Permet la communication entre réseaux.

Exemples : IP, ICMP, routeur, IPV4/V6.

Internet Control Message Protocol = protocol permettant l'envoi de diagnostics et d'erreurs au sein du réseau, couplé à l'IP, Utilisé par PING, traceroute/tracert

Modèle OSI - Couche 4 : Transport

Transmission de données de bout en bout.

Garantit fiabilité (TCP) ou rapidité (UDP).

Découpe/réassemble les segments de données.

TCP: envoi propre, garanti, ordonné. C'est un recommandé avec accusé de réception et repassage du facteur en cas d'absence => Je veux être sûr que tu reçoives tout, dans le bon ordre..

UDP: tu cours dans une foule 100 personnes en criant des informations, tu ne t'arrêtes pas, entendront et comprendront ceux qui veulent => J'envoie, si t'attrapes tant mieux. :-)

Modèle OSI - Couche 5 : Session

Gère les connexions entre applications.

Synchronisation, reprise après interruption,...

=> ouvre, maintien et ferme les sessions

Exemples : Sessions SSL/TLS, RPC.

Modèle OSI - Couche 6 : Présentation

Formate, compresse, chiffre les données.

Assure la compatibilité entre systèmes différents.

Exemples : Chiffrement SSL/TLS, ASCII, JPEG, JSON, XML.

Modèle OSI - Couche 7 : Application

Fournit les services réseau aux utilisateurs finaux.

Elle ne représente pas l'application entière mais les protocoles et interfaces que l'application utilise pour communiquer sur le réseau

Exemples : HTTP (web) , FTP (transfert), SMTP (mail)

Modèle OSI - Résumé

Couche	Rôle
7 - Application	Interface Réseau coté Utilisateur (ex: navigateur, messagerie)
6 - Présentation	Formatage des données (cryptage, compression)
5 - Session	Gestion de la session de communication
4 - Transport	Fiabilité, contrôle des erreurs
3 - Réseau	Adressage et routage (IP)
2 - Liaison de données	Transmission locale, commutation
1 - Physique	Transmission brute (câbles, signaux, ondes)

Moyens mnémotechniques OSI (1→7)

- **P**etit **L**apin **R**ose **T**rouvé À la **S.P.A**.
- **P**our **L**e **R**éseau **T**out **S**e **P**asse **A**utomatiquement.

Les mots correspondent aux initiales des couches OSI.

Moyens mnémotechniques OSI (7→1)

- **A**près **P**lusieurs **S**emaines, **T**out **R**espire **L**a **P**aix.

À utiliser selon le sens de la communication, de la couche 7 -> 1

Modèle TCP/IP

Aussi appelé **modèle Internet,** Il est un simplification du modèle OSI, constitué de seulement 4 couches.

Il constitue le fondement d'internet, en permettant une communication universelle entre systèmes informatiques.

Ce modèle repose sur des protocoles ouverts et standardisés garantissant l'interopérabilité entre les équipements quels que soient leur constructeur ou leur système d'exploitation.

Sa simplification par rapport au modèle OSI réside dans le regroupement logique de certaines couches, ce qui le rend plus pratique et plus facile à implémenter.

Modèle TCP/IP - Couche 1 : Accès réseau

La couche 1 du modèle TCP/IP gère l'intégralité de la transmission des données sur le support physique c'est à dire l'équivalent des couches 1 et 2 du modèle OSI.

Elle reposera sur les protocoles Ethernet, Wi-fi, PPP, ARP...

Modèle TCP/IP - Couche 2 : Internet

La couche 2 du modèle TCP/IP est Internet. Elle permet l'adressage, le routage et l'acheminement des paquets entre le réseau source et le réseau de destination.

Elle correspond à la couche 3 du modèle OSI.

Elle reposera principalement les protocoles IPv4, IPv6, ICMP

Modèle TCP/IP - Couche 3 : Transport

La couche 3 du modèle TCP/IP se charge de gérer la fiabilité de la transmission, le contrôle des erreurs, le découpage et la reconstitution des données.

Elle est la seule couche du modèle TCP/IP qui correspond à une seule couche du modèle OSI: la couche 4 - Transport

Elle reposera sur les protocoles TCP et UDP

Modèle TCP/IP - Couche 4 : Application

La couche 4 du modèle TCP/IP se charge de fournir les services réseau aux applications utilisées par les utilisateurs finaux (navigateur web, client mail, etc).

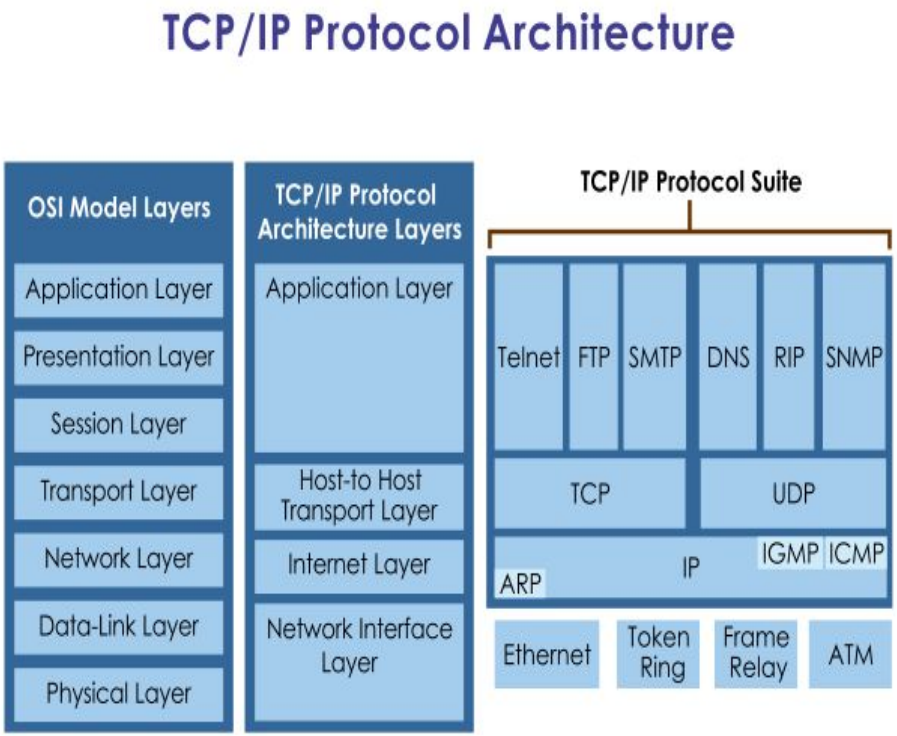
Elle regroupe les fonctions des couche 5, 6 et 7 du modèle OSI

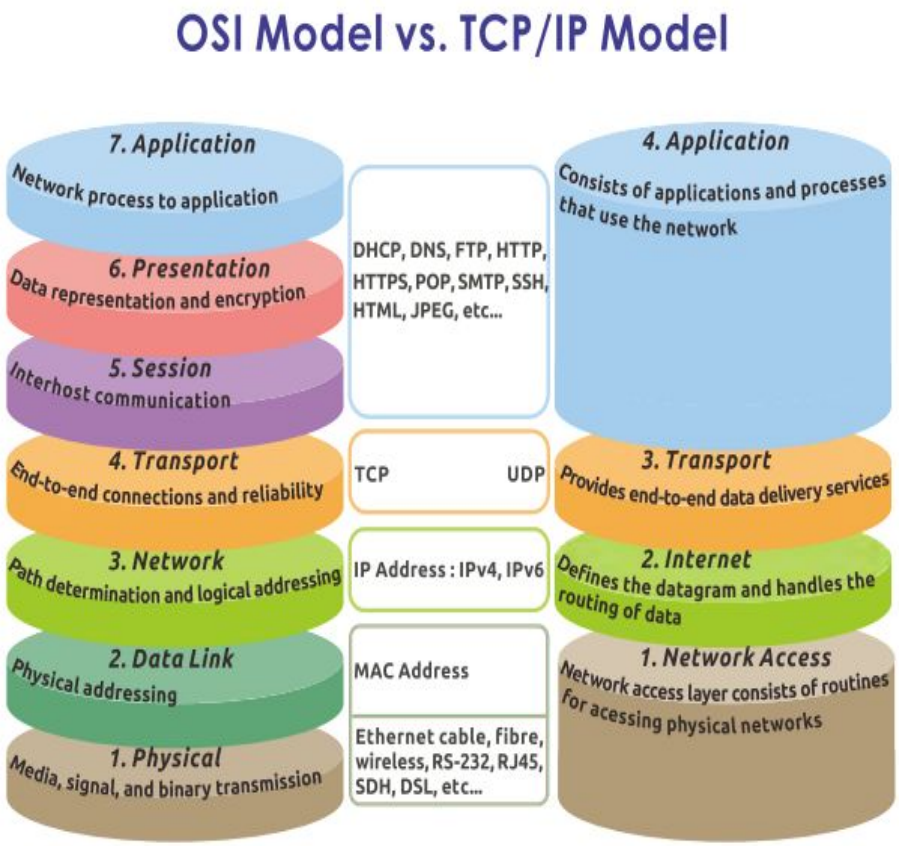
Elle reposera sur les protocoles HTTP(S), (S)FTP, SMTP, DNS, POP/IMAP,...

Différences OSI vs TCP/IP

Critère	Modèle OSI	Modèle TCP/IP
Nombre de couches	7 couches	4 couches
Niveau de détails	Très détaillé, séparation claire des fonctions	Simplifié, certaines couches sont fusionnées
But Initial	Modèle Théorique à des fin de standardisation	Modèle pratique, conçu pour Internet
Utilisation Réelle	Utilisé à des fin pédagogiques ou de référence	Modèle utilisé en pratique sur internet
Normalisation	Proposé par l'ISO	Proposé par le département de défense des états unis
Standard dominant	Moins utilisé seul	Standard de fait
Relation avec les protocoles	Les protocoles ne sont pas intégrés au modèle	Chaque couche a ses protocoles bien définis

Différences OSI vs TCP/IP





bstorm

Les protocoles de base

- HTTP/HTTPS : navigation Web.
- FTP/SFTP : transfert de fichiers.
- SMTP/POP/IMAP : email.
- DNS : résolution des noms de domaine.
- DHCP : attribution d’adresses IP.

Le protocole IP

Il est le protocole fondamental du modèle TCP/IP. Il permet d'acheminer les paquets de données d'un appareil à un autre à travers un ou plusieurs réseau.

Deux versions principales : IPv4 (courant, sur 32 bits), IPv6 (plus récent, 128 bits).

Permet un nombre quasi illimité d'adresses à savoir 2^{32} et 2^{128} adresses.

Le protocole IP

Seul, ce protocole n'est pas fiable de nature.

Il n'assure ni la livraison, ni l'ordre, ni la vérification des paquets.

Ces fonctions sont assurées par le protocole TCP si besoin.

Le protocole IP est utilisé avec d'autres protocoles tels que:

- ICMP pour le diagnostic réseau et les messages d'erreurs
- ARP pour la résolution des adresses MAC
- TCP ou UDP pour l'ordre/la rapidité de distribution

Les adresses IP

Une adresse IP est un identifiant unique attribué à chaque machine sur un réseau.

Elle permet aux appareils de s'identifier et de communiquer entre eux.

- Composées de 4 octets séparés par des points
- Chaque octet peut varier de 0 à 255
- Utilisent des masques pour définir les sous-réseaux.

Exemple: 192.168.1.1

Adresses IP publiques VS privées

IP publique : visible sur Internet, attribuée par votre fournisseur d'accès.

IP privée : utilisée dans les réseaux locaux, non routable sur Internet.

Plages privées :

- 10.0.0.0 à 10.255.255.255
- 172.16.0.0 à 172.31.255.255
- 192.168.0.0 à 192.168.255.255

Les routeurs font le lien entre IP privée et IP publique (via NAT).

Les masques de sous-réseau

Ils servent à déterminer la partie réseau et la partie hôte d'une adresse IP.

Notation sur 4 octets séparés par un point ou en notation CIDR (/XX) associée à l'adresse IP.

Attention: plus le masque est grand, moins il y a d'adresses disponibles.

CIDR: Classless Inter-Domain Routing => méthode d'écriture ignorant les anciennes classe A/B/C

Les masques de sous-réseau

Exemple:

	Notation standard	Notation CIDR
IP	192.168.1.1	192.168.1.1/24
Masque de sous-réseau	255.255.255.0	
Nombre d'adresses exploitables	254	254
Partie réseau	192.168.1	192.168.1
Partie hôte	.1	.1
Adresse réseau	192.168.1.0	192.168.1.0
Adresse broadcast	192.168.1.255	192.168.1.255

Les masques de sous-réseau

Considérant le fait qu'un masque de sous réseau est constitué de 4 octets et qu'il ne peut être composé que d'un nombre de bit successif à gauche:

- Masque minimale théorique => 128.0.0.0 ou /1, qui représente un 2.147.483.646 hôtes utilisables.

  Ce qui donne en binaire: 10000000.00000000.00000000.00000000

- Masque maximal théorique => 255.255.255.255 ou /32 qui représente 0 hôtes utilisables.

  Ce qui donne en binaire: 11111111.11111111.11111111.11111111

Nombre de machines selon le masque

- /30 → 2 machines utilisables (255.255.255.252)
- /29 → 6 machines utilisables (255.255.255.248)
- /28 → 14 machines utilisables (255.255.255.240)
- /24 → 254 machines utilisables (255.255.255.0)

Formule : 2^(32 - masque CIDR) - 2 (1 pour réseau, 1 pour broadcast)

Choisir le bon masque de sous-réseau

Étape 1 : estimer le nombre de machines nécessaires.

Étape 2 : choisir un masque qui offre au moins ce nombre.

Ex : besoin de 10 postes → /28 (14 addresses utilisables).

Utiliser des sous-réseaux permet de mieux gérer le réseau et limiter le trafic inutile.

A vous de jouer…!

- J’ai 32 machines et périphériques à mettre en réseau dans mon entreprise. Quel masque devrai-je utiliser pour être le plus proche possible de ce nombre?

- Mon réseau a évolué. j’ai désormais 139 machines et périphériques à connecter, comment dois-je adapter mon masque?

Diagnostic réseau

Il est important de pouvoir vérifier l'état de son réseau lorsqu'un problème se présente.

Les étapes de diagnostic peuvent varier selon le contexte mais il reste important de commencer par effectuer une vérification physique de son installation:

- Est ce que mon cable est branché? Correctement? Des 2 cotés?
- Est ce que j'ai bien mes voyants allumés sur ma box, sur mon switch, ma carte réseau?
- Est ce que mon cable est intègre (pas abimé, pas plié)?
- En cas de connexion wi-fi: est ce que je cherche à me connecter sur le bon réseau? Est ce que je suis sur le bon réseau?

Diagnostic réseau

Etape suivante s'assurer d'avoir une adresse IP correcte:

Sous windows nous pouvons utiliser la commande **ipconfig** dans le CLI ou un PS pour vérifier que nous disposons d'une adresse IP correcte.

De manière classique, les adresses IP locales sont généralement de type 10.X.X.X ou 192.X.X.X

Voir une adresse IP de type 169.X.X.X est souvent un indicateur d'une erreur DHCP

Sous Linux, nous pouvons utiliser la commande correspondante **ifconfig ou ip a**

Diagnostic réseau

La commande **ipconfig** possède pas mal d'options:

- ipconfig: affiche les informations de base (IPv4, masque de sous réseau, passerelle par defaut)
- ipconfig /all : afficher les informations de base + addresses MAC, serveurs DNS/DHCP, bail DHCP, nom du serveur DNS,...

Diagnostic réseau

La commande **ipconfig** nous permet également d'agir activement sur notre configuration réseau:

- ipconfig /release : permet de révoquer le bail DHCP et de libérer l'adresse utilisée
- ipconfig /renew: permet demander l'attribution d'une nouvelle adresse IP au serveur DHCP

Diagnostic réseau

Une fois que notre carte réseau est correctement configurée, il est temps de s'intéresser à la mise en réseau. Sommes nous connecter?

Nous pouvons essayer de communiquer avec notre passerelle. Dans un réseau domestique, la passerelle est déterminée par le DHCP, il s'agit généralement du modem/routeur par lequel nous passons pour aller sur internet. Cette adresse est visible lors de l'exécution de l'**ipconfig**

Nous pouvons effectuer une commande **ping** qui va, au moyen de frames ICMP, tenter d'entrer en communication avec le destinataire.

Un ping peut se faire, soit par adresse IP, soit par nom de domaine:

Exemples:

- ping 192.168.128.1
- ping google.com

Diagnostic réseau

Effectuer un ping vers votre passerelle vous permettra de savoir si votre mise en réseau local est ou semble fonctionnelle.

Nous pouvons ensuite tenter de communiquer vers l'extérieur.

Des ping peuvent être fait vers les adresses suivantes afin de savoir si vous disposez d'une connexion internet:

- ping 8.8.8.8 ou ping 8.8.4.4 pour tenter de communiquer avec l'un des nombreux serveurs de google
- ping 1.1.1.1 permet de tenter une communication avec un serveur cloudflare, un fournisseur DNS

Ces ping répondent? Parfait! Vous semblez connecté à internet. Vérifions le bon fonctionnement de votre DNS

Diagnostic réseau

Pour vérifier le bon fonctionnement de votre service DNS, pingez une adresse connue sur internet, google par exemple:

- ping google.com

Si vous avez une réponse positive, votre DNS fonctionne à merveille, si non, alors qu'un ping par adresse IP fonctionnait, vous être peut être confronté à un problème de service DNS

Les modifications de nom de domaine peuvent parfois mettre du temps à se propager. Pire, votre ordinateur pourrait avoir en mémoire une entrée DNS qui n'existe déjà plus.

Diagnostic réseau

Pour vérifier votre DNS, en alternative au ping vous pourriez utiliser la commande nslookup:

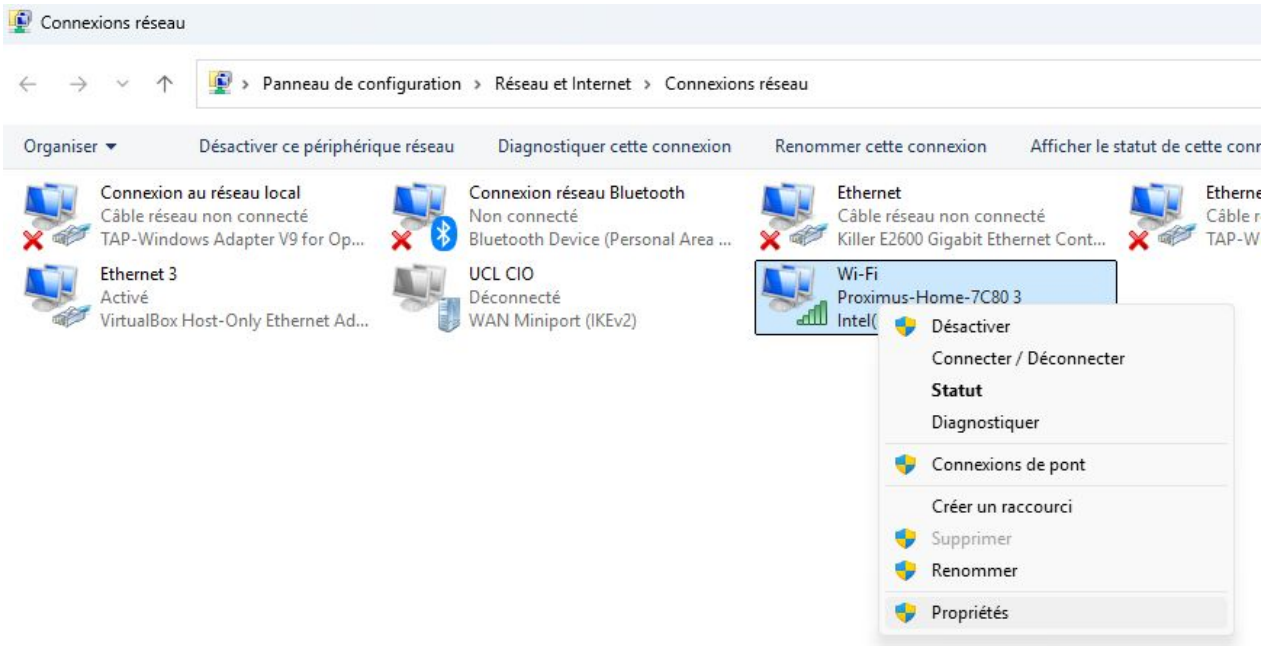
- nslookup google.com permettra de résoudre le nom de domaine de google et d'en obtenir l'ip associée
- nslookup 8.8.8.8 permettra de résoudre l'adresse ip 8.8.8.8 et de récupérer les informations DNS associées
- nslookup google.com 1.1.1.1 permet de résoudre le nom de domaine en utilisant un DNS personnalisé

Ces 3 commandes, si elles vous répondent par des erreurs sont des indicateurs d'un problème DNS

Diagnostic réseau

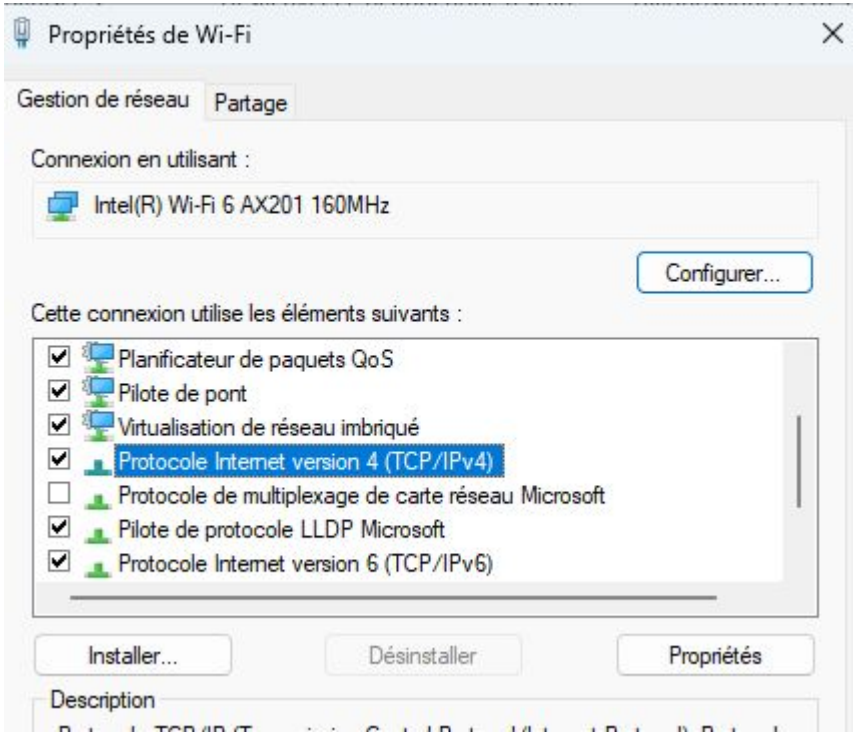
La commande **ipconfig /flushdns** vous permet de nettoyer vos informations DNS locales qui peuvent potentiellement être périmées.

Si votre résolution DNS ne fonctionne pas, essayez de définir vous même un DNS en allant dans les propriétés de votre carte réseau.



Diagnostic réseau

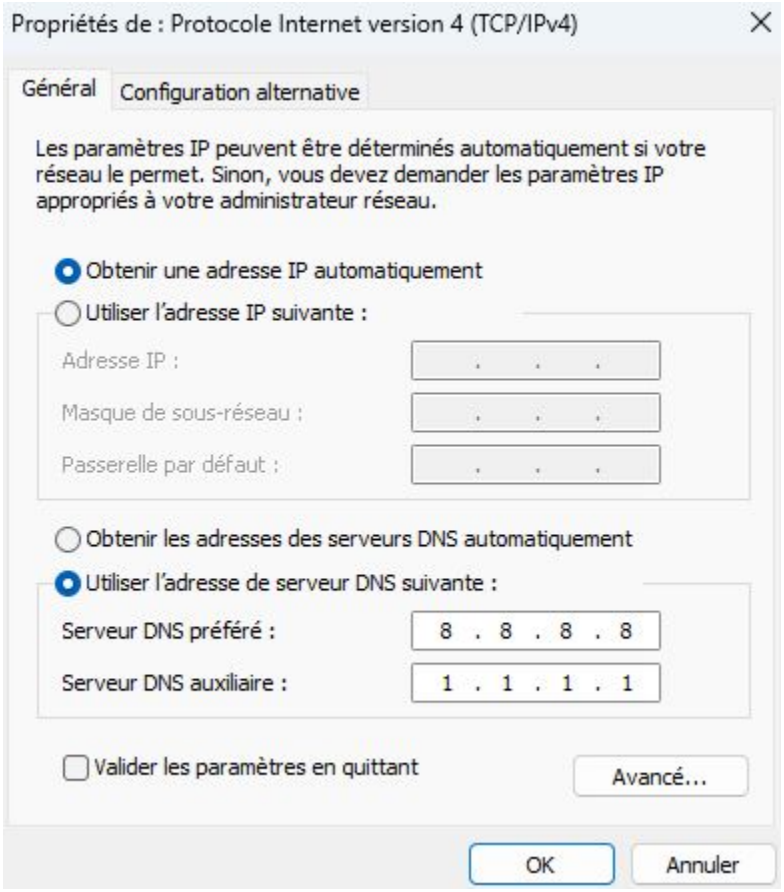
Editez les propriétés du service “Protocole Internet Version 4 (TCP/IPv4)”



bstorm

Diagnostic réseau

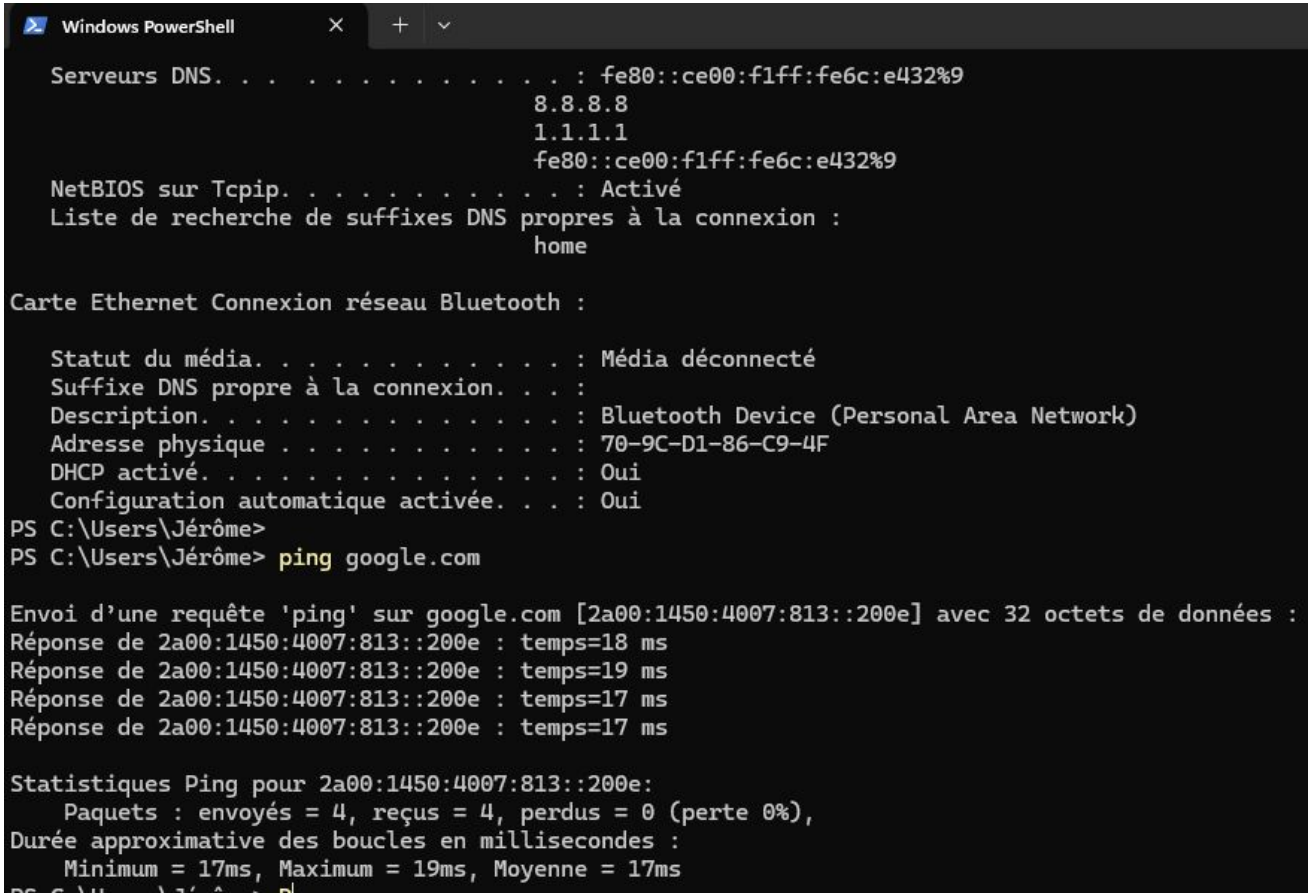
Définissez manuellement les serveurs DNS à utiliser



bstorm

Diagnostic réseau

Pinguez votre site préféré. Tout fonctionne? Félicitation, votre DNS est opérationnel!



Diagnostic Réseau: Correspondances Linux

WINDOWS	LINUX	Description
ipconfig	ip a ip address	Afficher IP, interface, masque, etc
ipconfig /all	ip -c a ip addr show	Version détaillée et plus lisible
ipconfig	ip r ip route	Afficher la route par défaut
ping ping x.x.x.x ping google.com	ping ping x.x.x.x ping google.com	Tester la connectivité réseau
nslookup …	nslookup … dig … host …	Vérifier la résolution DNS
ipconfig /flushdns	UBUNTU 20+ : sudo systemd-resolve –flush-caches	Vider le cache DNS local

Diagnostic Réseau: Correspondances Linux

WINDOWS	LINUX	Description
ipconfig /release	sudo dhclient -r	Libérer l'adresse IP
ipconfig /renew	sudo dhclient	Demander une nouvelle adresse IP

Testez-vous !

- Citez 3 types de réseaux.
- A quelle couche du modèle OSI correspond l'adressage IP ?
- Que fait un service DHCP ?
- Quelle différence entre TCP et UDP ?
- Donnez un exemple de protocole de couche application.
- Faites un diagnostic de votre réseau
  - Vérifiez vos paramètres
  - Vérifiez votre DNS
  - Passez manuellement sur le DNS de google 8.8.8.8
  - Vérifiez à nouveau vos paramètres pour valider vos modifications