

Réseaux locaux et équipements actifs

NIKIEMA Ousmane
Ousmane.nikiema@outlook.com

Avril 2020

Table des matières

Première partie.....	3
I.1. Construire un réseau : le matériel	4
I.1.1. Les moyens utilisés (médias d'accès)	4
I.1.1.1. Les câbles	4
I.1.1.2. Le monde du sans-fil	5
I.1.2 Le plus important de tous : la carte réseau	8
I.1.3 Concentrateur (hub)	9
I.1.4 Commutateur (switch) et routeur : si peu ressemblants et si similaires	10
I.1.4.1. Le commutateur : juste une histoire d'échange de données.....	10
I.1.4.2. Le routeur, un véritable ordinateur	10
I.1.5 Répéteur.....	11
I.1.6 Bilan des matériels.....	11
 Deuxième partie	 13
II.1. L'adressage CIDR	14
II.1.1 Les masques à longueurs variables (VLSM)	14
II.1.1.1. Son utilité?	14
II.1.1.2. TD : implémentation des masques à longueurs variables	16
II.1.1.3. Conclusion et exercices.....	22
II.1.1.4. Ci-dessous les images d'illustration	23
 Troisième Partie	 26
I. Comment accéder au centre réseau et partage ?.....	27
1 ^{ère} méthode : (valable pour Windows 10)	27
3 ^{ème} méthode : (valable pour Windows 10).....	29
Quel Type De Réseau Local Choisir Et Pourquoi ?.....	30
○ Si vous êtes connecté en Wifi:.....	31
○ Si vous êtes connecté avec un câble réseau :.....	32
Partager vos données rapidement grâce au Groupe Résidentiel	34
Comment créer votre groupe résidentiel	35
Les paramètres requis	35
La création	36
○ Modifiez ce que vous partagez avec le groupe résidentiel.....	39
○ Autoriser tous les périphériques sur ce réseau :	40
○ Modifier le nom de votre bibliothèque multimédia.....	41
○ Autoriser les périphériques multimédia à se connecter à votre groupe	41

○ Les options relatives au mot de passe de votre groupe résidentiel	42
Se connecter à un groupe résidentiel.....	43
4. Partager des dossiers spécifiques avec le groupe résidentiel :	43
Dépanner, réparer et créer un réseau local facilement	44
Comprendre les bases de votre réseau local pour le dépanner et le configurer.....	44
L'adresse physique:	46
L'adresse IP	47
Comment créer un réseau local facilement et pas à pas	51
Configuration et création rapide de votre réseau local.....	52
Définir le nom de groupe de votre réseau	52
Et les autres paramètres , à quoi ça sert ?	56
Conclusion	59

Première partie

Les équipements réseaux

I.1. Construire un réseau : le matériel

Il faut savoir que pour construire un réseau, il faut du matériel. Tout comme il faut un moteur, des roues et autres pour construire une voiture. Nous verrons donc quels sont les appareils et comment ils sont reliés entre eux : câbles, transmission sans fil, etc.

I.1.1. Les moyens utilisés (médias d'accès)

En informatique, les médias d'accès sont les moyens utilisés pour rendre possible la communication (l'échange des informations) entre les ordinateurs. Voyons divers moyens de connecter des ordinateurs entre eux.

I.1.1.1. Les câbles

Un des médias d'accès les plus utilisés est le câble. Les câbles sont des liaisons physiques entre ordinateurs. Mais il en existe différentes sortes, nous allons en voir 2 principales.

I.1.1.1.1. Câble Ethernet

Le câble Ethernet est sûrement le type de câble le plus utilisé pour connecter des ordinateurs entre eux dans un réseau local. À moins que votre réseau soit entièrement sans-fil, vous en avez sûrement chez vous. Il relie généralement un ordinateur personnel à un routeur (ce que l'on appelle parfois une «box»). Le nom formel de ces câbles est **paire torsadée**, en anglais *twisted pair*. À l'intérieur se trouvent en réalité 4 paires de fils de cuivre qui servent notamment aux transmissions électroniques. Il en existe plusieurs catégories, les plus courantes sont la 5, la 5E et la 6. Elles possèdent des caractéristiques physiques différentes qui font varier leur longueur et leur débit. Ainsi, un câble de catégorie 5 (**CAT5**) ne peut ni mesurer plus de 100 mètres, ni dépasser les 100 Mb/s. Un câble **CAT5E** peut, pour la même longueur, supporter un débit de 1 Gb/s.

i

Les paires peuvent être protégées contre les interférences extérieures par une feuille d'aluminium. On parle de **blindage**, en anglais *shield*. On retrouve ce terme dans des acronymes comme UTP-**CAT5** (Unshielded Twisted Pair Category 5).

Il existe deux types de câble Ethernet : les câbles Ethernet droits et les câbles Ethernet croisés. Ces derniers permettent de relier directement entre eux deux ordinateurs alors que les câbles droits servent à relier un ordinateur à un autre appareil comme un *hub* ou un *switch* que nous allons vous présenter dans ce chapitre.



Comment faire pour reconnaître un câble droit d'un câble croisé?

Généralement, c'est marqué sur l'emballage. 🍊

Si vous n'avez plus l'emballage, il suffit de regarder les embouts des câbles :



FIGURE I.2.1. – Embouts de câble Ethernet

Sur cette photo, on voit que les couleurs des fils à l'intérieur des embouts sont dans le même ordre sur les deux *connecteurs* : c'est donc un câble **droit**. Si le premier fil en partant de la gauche est inversé avec le 3ème et que le 2ème est inversé avec le 6ème, c'est un câble **croisé**. Sinon, c'est un câble dit «bâtard», mais c'est rare.

Ce type de câble est parfois appelé «câble **RJ45**» : c'est un abus de langage, **RJ45** est le nom de l'*interface* du câble (en gros, son embout).

I.1.1.1.2. Câble téléphonique

Le câble téléphonique est communément appelé **RJ11**. Ici aussi c'est un abus de langage, **RJ11** n'est pas le câble, mais bien l'interface. C'est ce que l'on peut utiliser pour le téléphone et le modem. En France, ce type de câble est peu utilisé : les prises en T sont très courantes pour les lignes DSL, qui fonctionnent sur des fils de cuivre. Ce type de liaison tend à disparaître au profit de la fibre optique.

Ce tutoriel n'ayant pas pour objectif d'aller dans les détails techniques électroniques qui constituent ces câbles et leurs spécificités, ces notions seront suffisantes pour le moment. Si vous voulez approfondir vos notions sur les câblages, nous vous conseillons Google et Wikipédia. 🍊

I.1.1.2. Le monde du sans-fil

L'air est aussi un média d'accès en réseau informatique. C'est un espace global qui englobe d'autres médias d'accès, dont nous allons parler. On peut diffuser des ondes électromagnétiques dans l'air et dans l'espace : ce sont ces ondes qui permettent de transporter des informations.

I.1.1.2.1. Le Bluetooth

Le Bluetooth, qui signifie littéralement dent bleue (:D) est une technologie développée par plusieurs entreprises (Agere, IBM, Intel, Microsoft, Motorola, Nokia et Toshiba) permettant la communication en utilisant l'espace hertzien (qui permet la diffusion d'ondes radio) entre les équipements électroniques, afin de minimiser l'utilisation des câbles entre les imprimantes, ordinateurs, scanners, PDA, téléphones, etc. Ce système exploite donc les ondes radio. D'ailleurs, vous allez apprendre du vocabulaire aujourd'hui : quand plusieurs entités sont en communication par le biais du Bluetooth, ce réseau formé est qualifié de **piconet** ;) . Piconet vient de pico- network, en français on peut traduire ça par picoréseau. Dans un picoréseau, les appareils utilisent la relation **maître-esclave** : le maître donne des ordres, l'esclave obéit. Quand plusieurs picoréseaux sont reliés, les esclaves peuvent avoir plusieurs maîtres, on parle alors de scatternet ou inter-réseau. Le mot «scatternet» signifie littéralement «réseau dispersé».



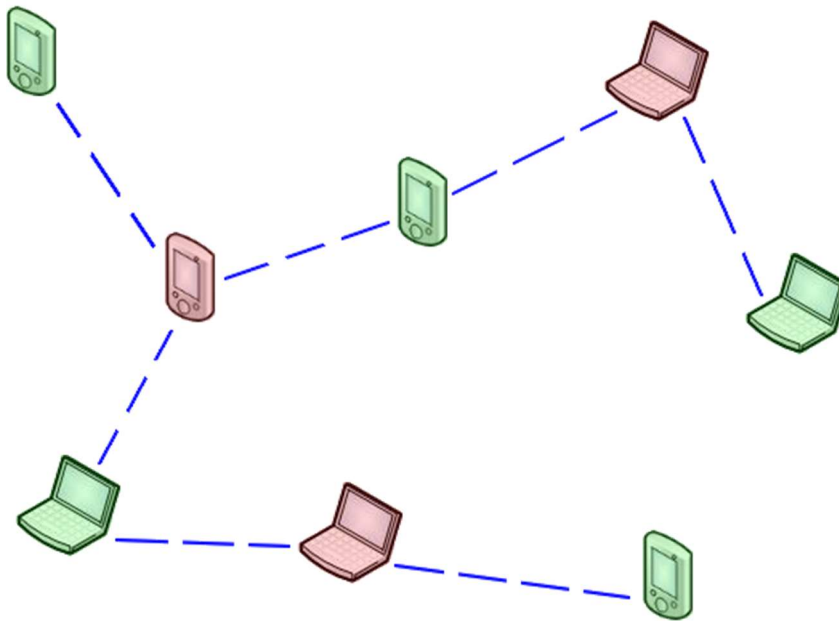
En Bluetooth, un esclave ne peut communiquer qu'avec son ou ses maîtres. Il ne peut pas communiquer avec d'autres esclaves ou maîtres. Inversement, un maître ne peut communiquer qu'avec son ou ses esclaves (bien qu'un maître puisse être lui-même esclave d'un autre). D'ailleurs, un maître ne peut pas avoir plus de 7 esclaves.

Voici des schémas expliquant ces 2 types de réseaux (piconet et scatternet):



Les réseaux de zéro - zestedesavoir.com

FIGURE I.2.2. – Un piconet, ou picoréseau



Les réseaux de zéro - zestedesavoir.com

FIGURE I.2.3. – Un scatternet

Pour la petite histoire, le nom Bluetooth vient d'un roi danois qui s'appelait Harald 1er, surnommé Harald Blåtand, ce qui signifie «l'homme à la dentbleue». 🍊

Il existe 3 classes en Bluetooth : la classe 1, la 2 et la 3. Ce qui les différencie est juste la portée. Dans la classe 1, la portée peut aller jusqu'à 100 mètres, dans la catégorie 2, elle est d'une dizaine de mètres, et dans la classe 3, elle est de quelques mètres seulement (moins de 10). C'est cette 3ème classe qui est utilisée dans les téléphones portables.

I.1.1.2.2. L'infrarouge

L'infrarouge est un autre moyen de transmission des données sans fil, qui exploite la lumière. Il est moins pratique que le Bluetooth car il faut que les périphériques qui communiquent entre eux soient à moins de 1,50m de distance. Ils doivent aussi être alignés : la lumière ne se propage pas dans les environs comme les ondes radio. Autrefois, beaucoup de téléphones utilisaient l'infrarouge, mais il s'est rapidement fait remplacer par le Bluetooth, bien que certains appareils utilisent les deux. Il existe toujours actuellement des imprimantes, souris, claviers sans fil utilisant l'infrarouge.

I.1.1.2.3. Le Wi-Fi

Le Wi-Fi est certainement le moyen de transmission de données sans fil le plus utilisé. Sa portée pouvant excéder les 200 mètres en espace ouvert et sa vitesse de débit théorique de l'ordre du gigabit par seconde (Gb/s) font que cette technologie est aujourd'hui très utilisée dans les réseaux locaux pour accéder à Internet. Il est impressionnant de constater le nombre de points

d'accès Wi-Fi sécurisés ou non que l'on peut capter un peu partout. «Wi-Fi» peut être considéré comme le nom commercial de la norme IEEE 802.11, norme qui régit cette technologie.

Ces méthodes de transmission d'information ne serviraient à rien si l'on n'avait pas de matériel pour les exploiter... Heureusement, il y en a, et pas qu'un peu! 🍏

I.1.2 Le plus important de tous : la carte réseau

La carte réseau est le composant le plus important, elle est indispensable. C'est par elle que transitent toutes les données à envoyer et à recevoir du réseau par un ordinateur. Il n'y a pas grand-chose à dire sur cet appareil. La seule chose que vous devez connaître, c'est la notion d'**adresse MAC** : c'est l'adresse physique de la carte. Elle permet d'identifier la machine dans un réseau, un peu comme l'**adresse IP**. Nous ne devrions pas encore en parler, mais il serait bien difficile de comprendre le fonctionnement de certains matériels... Pour faire court et ne pas vous embrouiller si tôt, l'adresse physique est relative à la carte réseau. Elle lui est attribuée à sa fabrication et ne peut pas changer (ce n'est pas tout à fait vrai, mais l'idée est là). L'adresse **IP** est relative au réseau : elle change tout bonnement suivant le réseau. Vous comprendrez mieux ce que sont ces adresses dans la sous-partie sur le commutateur (*switch*). La carte réseau est aussi appelée NIC en anglais, pour *Network Interface Card*. Voici à quoi peut ressembler une carte réseau :



FIGURE I.2.4. — Image originale par Barcex sous licence CC BY SA 3.0 [Lien vers](#)

[l'image d'origine](#)



La carte réseau de la photo comporte un port femelle Ethernet : ce port peut accueillir un câble Ethernet mâle (connecteur **RJ45**). Les cartes réseau internes sont souvent des cartes PCI, c'est-à-dire qu'elles s'enfoncent dans un port PCI.

i

Une clé Wi-Fi est aussi une carte réseau à elle toute seule, sauf que contrairement à une carte comme celle ci-dessus, elle se présente sous forme d'une clé USB et se branche sur un port USB.

I.1.3 Concentrateur (hub)

Un *hub* est un dispositif en réseau qui permet de mettre plusieurs ordinateurs en contact. Définition pas très précise, puisque tout dispositif en réseau (ou presque) a le même but. 🍊 Bref, ce qu'il faut retenir est qu'un *hub* est très bête, enfin, moins intelligent que les autres. Ce qu'il fait est tout simple : il reçoit des données par un port, et envoie ce qu'il reçoit aux autres. Il a une interface de réception (un port) et une interface de diffusion (plusieurs autres ports par où les autres ordinateurs sont connectés).

Attention, une interface permet la réception ET la diffusion. Comme vous pouvez le voir sur la photo ci-dessous, le *hub* n'a pas juste deux interfaces physiques, où on entre par la gauche et on ressort à droite, non ! L'interface de réception est logique.

Exemple : j'ai un *hub* à 4 ports, avec 4 ordinateurs connectés. J'ai le port 1, 2, 3, 4 (ici, interface = port). Si l'ordinateur 4 (au port 4) veut communiquer avec les autres, moi le *hub*, je reçois les données au port 4 (c'est mon port de réception) et je renvoie les données aux ports 1, 2, et 3 : ce sont les ports de diffusion.

!

Je ne renvoie plus les données au port 4, car c'est mon port de réception. 🍊



FIGURE I.2.5. – Un hub (image domaine public)

Ce qu'on lui reproche est le manque de confidentialité. Eh oui, le *hub* ne garde pas de secret : tout ce qu'un ordinateur lui dit, il l'envoie aux autres. Heureusement, les autres vérifient bien si ça leur est destiné, et si ça ne l'est pas, ils laissent tomber les données et ne les lisent pas.

?

C'est toujours sécurisant, non?

Non, pas du tout, à partir du moment où les données arrivent jusqu'à la carte réseau, elles peuvent toujours être lues (mais on n'est pas là pour un cours de sécurité informatique).

I.1.4 Commutateur (switch) et routeur : si peu ressemblants et si similaires

Le commutateur (ou *switch*) et le routeur sont 2 appareils fondamentalement différents, et pourtant, leurs rôles se ressemblent tellement ! Au-delà de leur architecture, il faut comprendre leur différence au niveau d'un réseau.

I.1.4.1. Le commutateur : juste une histoire d'échange de données

Un commutateur fonctionne à peu près comme un *hub*, sauf qu'il est plus discret et intelligent. Il n'envoie pas tout ce qu'il reçoit à tout le monde, mais il l'envoie uniquement au destinataire. Si l'ordinateur 1 envoie des données à l'ordinateur 2, seul ce dernier les recevra et pas les autres connectés. Afin de déterminer l'ordinateur à qui il faut renvoyer les données, le *switch* se base sur les adresses physiques (adresses **MAC**) des cartes réseau. Pour faire une analogie avec la vie réelle, une adresse **MAC** est un peu comme une adresse postale. C'est une suite de 6 nombres hexadécimaux, par exemple 00-16-D4-C7-6E-D3. Si vous ne savez pas ce qu'est l'**hexadécimal**, ce n'est pas bien grave pour le moment, mais pensez à consulter [notre annexe sur le sujet](#) à l'occasion. On en a souvent besoin en informatique (et pas qu'en réseau). Nous n'étudierons pas les adresses **MAC** dans ce chapitre, elles seront étudiées à partir de la partie 3, lorsque nous aborderons réellement la communication dans un réseau.

Un commutateur transmet donc des données aux autres ordinateurs en se basant sur leurs adresses **MAC**. Les transmissions sont plus confidentielles, les autres ne savent rien des données ne leur étant pas destinées. Son utilisation reste limitée aux réseaux locaux.



FIGURE I.2.6. – Des switchs - Image par Jellyfishz sous licence CC BY SA 4.0

[Lien vers l'image d'origine](#)

I.1.4.2. Le routeur, un véritable ordinateur

Un routeur ressemble à un *switch* sur le plan de l'utilisation : en effet, il permet de mettre plusieurs ordinateurs en réseau. Mais cela va plus loin : il permet de mettre en contact 2 réseaux

fondamentalement différents. Dans une petite installation, avec un ou plusieurs ordinateurs connectés à une « box » (qui est en fait un routeur), il est la frontière entre le réseau local et Internet.

Un routeur a plusieurs interfaces. Pour continuer dans notre exemple de frontière avec Internet, il possède une interface connectée à Internet (généralement, cela se traduit par un câble branché sur la prise téléphonique ou sur un boîtier fibre optique) et plusieurs autres interfaces sur lesquels se connectent des ordinateurs voulant accéder à Internet (ce qui se traduit généralement par des câbles Ethernet ou des connexions Wi-Fi).

i

Notez aussi que le routeur n'est pas uniquement utilisé pour aller sur Internet, on l'utilise aussi dans un réseau strictement local.

I.1.5 Répéteur

Un répéteur (*repeater* en anglais) agit un peu comme un *hub*, mais ce dernier n'a que 2 interfaces. Son intérêt est de renvoyer ce qu'il reçoit par l'interface de réception sur l'interface d'émission, mais plus fort. On dit qu'il régénère et réémet le signal. En transmission sans fil (radio, téléphone) on parle aussi de relais. Un répéteur permet de couvrir des distances plus grandes que les distances maximales fixées par le matériel que l'on utilise : par exemple, dans un réseau sans fil (Wi-Fi), la portée maximale entre 2 appareils est d'environ 50 mètres en intérieur. En plaçant un répéteur peu avant ces 50 mètres, vous pouvez connecter 2 appareils à 100 mètres de distance. Toutefois, le fait que les informations soient renvoyées « plus fort » peut dégrader la qualité du signal dans les réseaux sans fil. Pour prendre un exemple parlant, en radiophonie, si l'on se trouve trop loin d'un relais, la qualité du son que l'on entend est dégradée.

I.1.6 Bilan des matériels

Afin de conclure ce chapitre, nous allons récapituler le matériel vu et son utilité. Un tableau récapitulatif vaut mieux qu'un long discours :

Matériel	Utilité
Carte réseau	La carte réseau est le matériel de base indispensable, qui traite tout au sujet de la communication dans le monde du réseau.
Concentrateur (<i>hub</i>)	Le concentrateur permet de relier plusieurs ordinateurs entre eux, mais on lui reproche le manque de confidentialité.
Commutateur (<i>switch</i>)	Le commutateur fonctionne comme le concentrateur, sauf qu'il transmet des données aux destinataires en se basant sur leurs adresses MAC (adresses physiques). Chaque machine reçoit seulement ce qui lui est adressé.
Routeur	Le routeur permet d'assurer la communication entre différents réseaux pouvant être fondamentalement différents (réseau local et Internet).

Répéteur	Le répéteur reçoit des données par une interface de réception et les renvoie <i>plus fort</i> par l'interface d'émission. On parle aussi de <i>relais</i> en téléphonie et radiophonie.
----------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Dans ce chapitre de culture informatique, nous avons examiné différents composants que l'on peut utiliser en réseau. Il est vraiment important de comprendre leur fonctionnement pour pouvoir choisir ce qui sera utilisé dans différents cas.

Mais on en fait quoi de tout ce matériel ? Les câbles, on les branche où ? Quelles machines doivent être reliées entre elles ?

Rendez-vous au prochain chapitre pour répondre à ces questions!

Deuxième partie

L'adressage CIDR (VLSM)

II.1. L'adressage CIDR

Nous vous avons dit en parlant des classes que ces dernières avaient presque entièrement disparu parce qu'elles étaient devenues obsolètes. Elles ont été remplacées par un système d'adressage plus fiable et plus performant, à savoir l'adressage CIDR, qui est l'objet de ce chapitre. Étant donné qu'il s'agit du système d'adressage utilisé actuellement, vous feriez mieux d'être plus concentrés que lorsque nous avons traité des classes. 🍊 C'est parti !

II.1.1 Les masques à longueurs variables (VLSM)



Comme précédemment, la compréhension de cette section demande beaucoup de concentration. Papier et crayon vous seront utiles pour faire des calculs et prendre des notes. Si vous vous contentez de lire, vous risquez de ne pas retenir grand-chose !

VLSM, pour *Variable Length Subnet Mask* (soit **masque de sous-réseaux à longueur variable**) est une technique utilisée dans le but de mieux gérer les adresses IP, tout comme le CIDR. En fait, VLSM est une extension de CIDR. La différence est que le CIDR est plus utilisé au niveau internet et le VLSM est plus utilisé dans un réseau local, mais les deux permettent de minimiser la perte d'adresses. 🍊



Pour mettre en place un réseau aux masques à longueurs variables, il faut être sûr que les routeurs supportent les protocoles compatibles au VLSM. Quelques-uns de ces protocoles sont **OSPF, EIGRP, RIPv2, IS-IS**. Vous n'avez pas besoin de connaître ce qu'ils sont et ce qu'ils font, nous étudierons quelques-uns d'entre eux en temps voulu. 🍊

II.1.1.1. Son utilité?

Pour comprendre à quoi sert l'implémentation des masques de sous-réseaux variables, nous allons considérer un scénario.

Vous avez un réseau de 250 hôtes. Vous voulez réduire la congestion de ce dernier et décidez de le subnetter en plusieurs sous-réseaux. Grâce aux techniques du subnetting et aux règles que vous avez apprises, vous décidez de le subnetter en cinq réseaux de 50 hôtes chacun.



Il est impossible d'obtenir cinq réseaux de 50 hôtes pile chacun (d'ailleurs, c'est une mauvaise pratique de choisir un masque qui nous donne exactement le nombre d'hôtes dont nous avons besoin). À la rigueur, nous pourrions obtenir cinq réseaux pouvant contenir au moins 50 hôtes. Dans ce cas, le réseau pourrait contenir un maximum de 62 hôtes si on masque 2 bits.



Vous obtenez alors vos cinq sous-réseaux et vous êtes contents : le but est atteint. 🍊

Maintenant, imaginez que vous êtes un administrateur réseau employé dans une entreprise. Vous avez un sous-réseau **192.168.100.0/24**. Votre patron vous dit qu'il souhaite une segmentation par fonctions, comme nous l'avons étudié dans l'analyse des contraintes et plan d'adressage. Il vous

donne les spécifications suivantes :

- Un sous-réseau de 50 hôtes, uniquement pour les secrétaires de l'entreprise.
- Deux sous-réseaux de 12 hôtes chacun, pour les techniciens et les comptables.
- Un sous-réseau de 27 hôtes pour les développeurs d'applications.

Pour une meilleure compréhension de ce qui nous est demandé, considérons le schéma ci-dessous auquel vous devez vous référer.

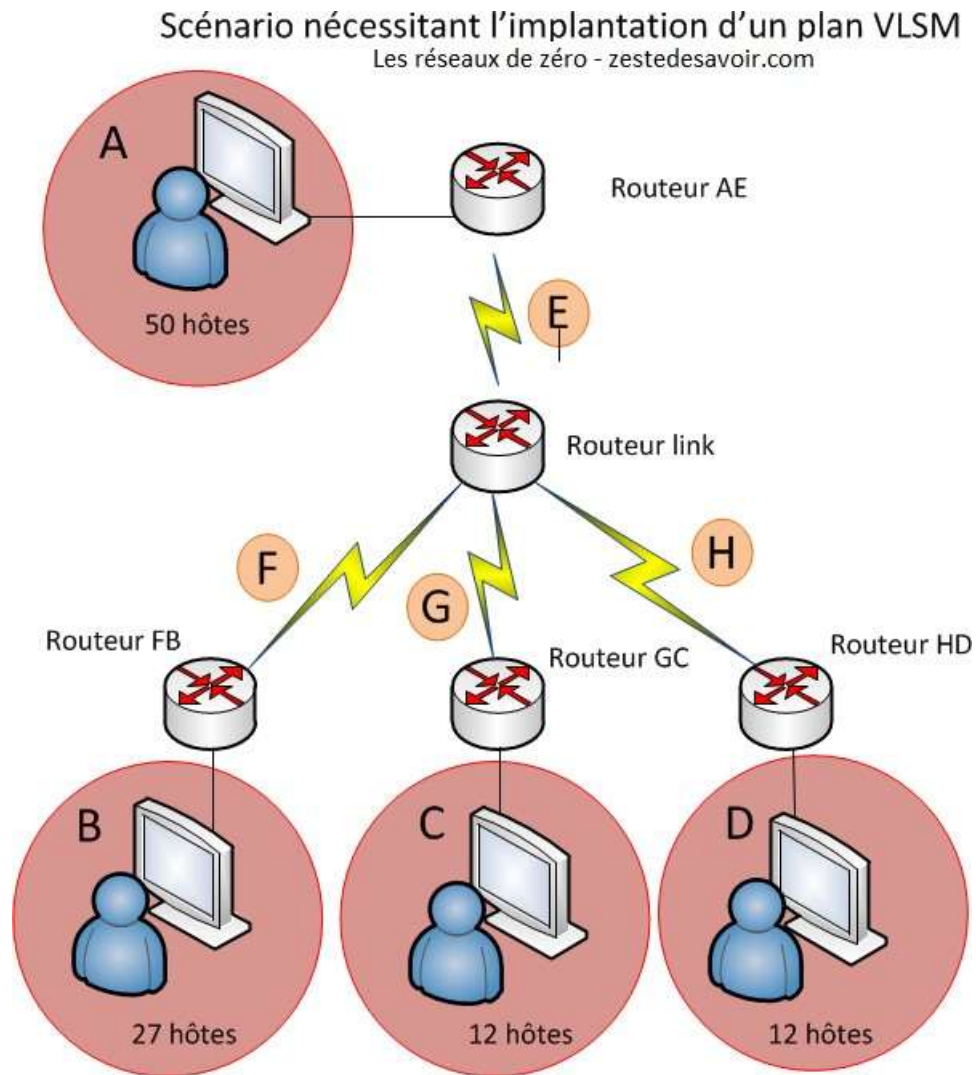


FIGURE III.6.1. – Scénario nécessitant l'implantation d'un plan VLSM

Les cercles rouges représentent les sous-réseaux que nous voulons obtenir. Nous avons au total cinq routeurs :

- *routeur_AE*, qui relie le réseau A et E;
- *routeur_link*, qui relie les réseaux F, G et H au réseau E;
- etc.



N.B. : les réseaux E, F, G et H sont en orange pour une raison précise. Il s'agit en fait des interfaces de liaison.

Comment allez-vous mettre cela en place en subnettant ? Ce n'est pas possible, car le subnetting nous permet d'avoir plusieurs sous-réseaux ayant un même nombre d'hôtes et un même masque, mais ayant des portées d'adresses différentes pour marquer la fin et le début d'un sous-réseau. Or dans notre

étude de cas, le patron (le boss, quoi :soleil :) nous demande de créer des sous-réseaux aux masques à longueurs variables. En fait, si on analyse bien la situation, il nous faut créer des sous-réseaux différents dans des sous-réseaux, c'est ce qu'on appelle **subnetter un subnet** (sous-réseauter un sous-réseau :-°). Il faudra donc, à partir d'un network ID, obtenir un masque différent pour chaque sous-réseau. 🍌 Si nous en étions encore à l'adressage par classes, cela serait impossible car il faut un même masque pour chaque sous-réseau. Ainsi, un réseau tel que 192.168.187.0 n'aurait qu'un seul masque, soit 255.255.255.0.

II.1.1.2. TD : implémentation des masques à longueurs variables

Pour comprendre le calcul des masques variables, nous allons implémenter cela dans un réseau local. La solution au scénario ci-dessus se fera comme dans un TD. Les prérequis pour pouvoir suivre et comprendre ce TD sont :

- Maîtrise de la notion de masque de sous-réseau et son utilité.
- Maîtrise des 8 premières puissances de 2.
- Maîtrise de la conversion du binaire au décimal et l'inverse.
- Maîtrise de la notion du subnetting et sa procédure.
- Maîtrise de la notion de passerelle et son rôle.
- Maîtrise de l'adressage CIDR et sa notation.

Pour réussir ce challenge posé par votre patron, il vous faudra suivre des étapes de planification d'adresses. C'est parti! 🍌

— Étape 1 : se focaliser sur le sous-réseau qui a le plus grand nombre d'hôtes

Nous allons commencer par localiser le sous-réseau qui a le plus grand nombre d'hôtes, le sous-réseau A en l'occurrence (50 hôtes).

?

Combien de bits devons-nous utiliser pour avoir au moins 50 hôtes?

On y va avec les puissances de deux et notre formule $2^n - 2$.

- $2^{1-2} = 0$;
- $2^{2-2} = 2$;
-
- $2^{6-2} = 62$. Stop! Nous allons donc devoir garder 6 bits de la partie « host » de notre masque.

En binaire, nous obtenons donc : 11000000 . 10101000 . 01100100. nnnhhhhh avec n les bits disponibles pour le réseau, et h les bits **qu'on ne doit pas masquer** pour obtenir au moins 50 hôtes.

— Étape 2 : choisir un network ID pour l'étape 1

Une fois que nous avons résolu le plus grand sous-réseau, il nous faut choisir quel subnet ID donner à ce sous-réseau. Nous avons retenu, dans l'étape 1, que nous n'avions que 2 bits pour le sous-réseau, ce qui donne (en se focalisant sur le 4e octet) les combinaisons suivantes que vous êtes censé trouver ~~les doigts dans le nez~~ :

- 00hhhhhh;
- 01hhhhhh;
- 10hhhhhh;
- 11hhhhhh.

En remplaçant le h (pour hôte) par 0 (puisque nous ne les masquons pas), on obtient le network ID pour chaque sous-réseau, soit les suivants :

- 00000000 = .0
- 01000000 = .64
- 10000000 = .128
- 11000000 = .192

N'ayant que 2 bits masqués pour le sous-réseau, on peut donc utiliser un masque de /26 ou 255.255.255.192 pour chacun de ses sous-réseaux obtenus, juste comme on ferait dans un réseau utilisant l'adressage par classe. 🍊

Voilà. Nous avons 4 network ID, vous pouvez choisir **n'importe lequel** pour le sous-réseau A. Dans ce TD, nous choisissons au hasard .64, soit la notation **192.168.100.64/26 (network ID/masque)**. Les autres sous-réseaux devront se contenter des trois sous-réseaux restants.



?

D'où vient le /26?

C'est une blague? 🍊 Vous êtes censés savoir comment on a obtenu le /26. Nous avons gardé 6 bits pour les hôtes, or une adresse IP est constituée de 32 bits, donc $32-6 = 26$ bits.

— Étape 3 : se focaliser sur le second plus grand sous-réseau

Le second plus grand sous-réseau contient dans notre exemple 27 hôtes pour les développeurs d'applications. Il s'agit du sous-réseau B. Nous allons refaire les calculs de l'étape 1. Nous n'allons donc pas détailler cela. Nous aurons besoin d'au moins 5 bits pour les hôtes ($2^5-2 = 30$, $30 > 27$, donc O.K.). En binaire, nous avons :

11000000 . 10101000 . 11001000 . nnnhhhhh

N'est-ce pas? Alors, nous pouvons faire toutes les combinaisons possibles avec les trois bits pour n, n'est-ce pas? **Faux!**



Faux? 🍊 Nous n'avons besoin que de 5 bits. C'est logique puisque nous en avons trois consacrés au sous-réseau, non?

Oui, mais non! :D Si vous le faites ainsi, vous êtes en train de subnetter le network ID original soit le 192.168.100.0, alors que c'est ce que nous avons déjà fait dans l'étape 1, en masquant 2 bits pour le réseau. Mais ici, nous voulons **subnetter un subnet**. C'est totalement différent, nous allons donc prendre un sous-réseau déjà obtenu dans l'étape 1 et le re-subnetter à nouveau.:-° Avouez que cela devient complexe. 🍊

Dans l'étape 1, nous avons obtenu 4 combinaisons, soit 4 network ID. Nous avons sélectionné le 255.255.255.192 soit le /26 pour le sous-réseau A. Il nous reste donc trois network ID disponibles, soit :

- 00000000 = .0/26
- 01000000 = .64/26 // sous-réseau A
- 10000000 = .128/26
- 11000000 = .192/26

Choisissons le .128 dont le network ID sera **192.168.100.128/26**, ce qui donne en binaire (focus sur le 4e octet) : 10000000. Or nous n'avons besoin que de 5 bits disponibles pour les hôtes, alors qu'ici nous en avons 6. Nous allons donc supprimer un bit pour les hôtes et l'allouer au sous-réseau. 🍊

10n00000.

Voilà! Nous avons donc 3 bits pour le sous-réseau et 5 pour les hôtes. Maintenant, nous pouvons donc créer deux sous-réseaux à partir du sous-réseau original. ;) C'est cela l'intérêt du VLSM, on subdivise encore un sous-réseau. Nous avons donc :

- 10000000 = .128
- 10100000 = .160

Bravo, vous venez de subnetter un subnet comme un pro, vous devez en être fier. 🍊 En résumé, voici ce que nous avons fait :

1. Nous disposons à l'origine d'un network ID de 192.168.100.0/24.
2. Nous l'avons subdivisé pour obtenir un sous-réseau ayant un masque de 192.168.100.64/26 et pouvant contenir au moins 50 hôtes.
3. Nous avons pris le sous-réseau obtenu dans l'étape 2 et l'avons *re-subnetté* en deux sous-réseaux (.128 et .160) qui auront un masque de.../27. 🍊



Comment avez-vous obtenu le /27?

Encore la même question? :D Dans les deux sous-réseaux que nous avons obtenus, nous avons 3 bits pour les sous-réseaux et 5 pour les hôtes. Nous avons donc laissé 5 bits non masqués pour obtenir au moins 27 hôtes ($2^5 - 2 = 30$). Une adresse IP valant 32 bits, $32 - 5 = 27$.;) D'où les réseaux .128 et .160 qui ont tous deux un même préfixe :/27. 🍊

Ici également, nous pouvons choisir n'importe quel network ID : choisissons le premier, soit .128/27. Le sous-réseau restant (.160/27) pourrait être utilisé dans le futur, s'il y a un agrandissement du sous-réseau.

Voici la liste des network ID que nous avons obtenus depuis l'étape 1:

- 00000000 = .0/26 | libre pour être re-subnetté
- 01000000 = .64/26 | sous-réseau A
- 10000000 = .128/26 | Nous ne pouvons plus l'utiliser, il a été re-subnetté
- **10000000** = .128/27 | Nous prenons celui-ci pour le sous-réseau B
- **10100000** = .160/27 | nous gardons celui-ci pour le futur

?

Mais... mais... comment obtient-on 128/26 ET 128/27?

C'est faire preuve de concentration que de poser cette question ! La réponse est simple : nous avons 128/26 au départ, mais comme nous l'avons re-subnetté, nous avons changé de masque, en gardant le network ID originel : nous avons donc le 2e 128, mais avec un masque de /27.



Étape 4 : se focaliser sur le troisième plus vaste sous-réseau

Le troisième plus vaste sous-réseau est le réseau C et D de 12 hôtes chacun. Cette étape est exactement la répétition des étapes 1 et 3, avec les mêmes calculs. Nous avons besoin d'au moins 12 hôtes. $2^4 - 2 = 14$, ce qui nous suffit. Nous allons donc garder 4 bits pour les hôtes et disposerons donc de 4 bits pour la partie réseau du masque. Au lieu de reprendre le network ID de base et masquer 4 bits comme nous l'aurions fait dans un cas de subnetting classique, nous allons devoir re-subnetter un subnet déjà subnetté comme nous l'avons fait dans l'étape 3. Vous avez le choix : vous pouvez décider de re-subnetter le **192.168.100.0/26**, **192.168.100.128/27** ou **192.168.100.160/27**. Pour ce TD, choisissez **192.168.100.160/27**. Nous avons donc ceci en binaire :

10100000

Nous avons 5 bits libres pour les hôtes, ce qui était suffisant pour le réseau B qui nécessitait 27 hôtes. Mais pour le réseau C ou D, nous aurons une perte de $27 - 12 = 15$ hôtes, et c'est ce que nous voulons éviter. Nous allons donc retirer un bit de la partie hôte et l'allouer à la partie réseau de notre masque de manière à avoir 4 bits pour les hôtes et 4 pour la partie réseau car $2^4 - 2 = 14$, ce qui nous convient. ;) Nous avons donc:

101**n**0000

- **10** représente ici les deux bits consacrés au réseau au départ dans l'étape 1. C'est notre motif de base : nous ne devons pas le changer, le reste de nos subnets en binaire **doit commencer par 00**.
- **1** représente le bit sur lequel nous nous sommes concentrés dans l'étape 3.
- **n** est le bit supplémentaire que nous allons ajouter à la partie réseau du masque de manière à ne rester qu'avec 4 bits pour les hôtes. 🍊

Grace à ce bit de plus que nous avons, nous pouvons donc avoir deux combinaisons (soit le laisser à 0 ou le masquer à 1), ce qui nous donne la possibilité d'obtenir deux autres sous-réseaux à partir du sous-réseau de base, ce qui nous donne (avec le focus sur le 4e octet toujours) :

- 10100000 = .160
- 10110000 = .176

Il ne nous reste plus qu'à trouver le nouveau masque pour ces deux nouveaux sous-réseaux, ce qui est simple puisque nous n'avons qu'à compter le nombre de bits masqués. Soit **11111111.11111111.11111111** puisque nous n'avons que 4 bits pour les hôtes, le reste des bits est donc masqué pour la partie réseau. 🍏 Nous aurons donc un masque de **255.255.255.240** ou **/28** pour la notation CIDR.

Résumons donc tous les subnets obtenus depuis l'étape 1 afin de choisir un network ID pour les réseaux C et D.

- 00000000 = .0/26 | subnet libre pour être re-subnetté
- 01000000 = .64/26 | déjà utilisé par le sous-réseau A
- 10000000 = .128/26 | Nous ne pouvons plus utiliser celui-ci, car nous l'avons re-subnetté
- 11000000 = .192/26 | subnet pour un futur agrandissement
- 10000000 = .128/27 | déjà utilisé pour le sous-réseau B
- 10100000 = .160/27 | nous ne pouvons plus l'utiliser, car nous l'avons re-subnetté
- 10100000 = .160/28 | Prenons celui-ci pour le sous-réseau C
- 10110000 = .176/28 | Prenons celui-ci pour le sous-réseau D
- Remarque 1 : nous nous retrouvons avec deux **160** : un avec **/27** et l'autre avec **/28**, pour les mêmes raisons que nous avons deux **128**. Nous vous avons expliqué cela. 🍏
- Remarque 2 : nous ne pouvons plus utiliser un sous-réseau déjà subnetté.

— Cinquième et dernière étape : déterminer les network ID pour les interfaces de liaison

Regardez sur votre schéma. Comment allons-nous nouer ces sous-réseaux entre eux ? Par un routeur bien entendu, et c'est exactement ce que fait le routeur **routeur_link** dans le schéma. Mais comme chaque routeur, il possède deux interfaces de liaison. Il faut donc deux adresses IP pour relier F et E, deux pour relier G et E, et deux pour relier H et E. ;) Nous pouvons le faire les yeux fermés en binaire, nous n'avons besoin de 2 bits car $2^2 - 2 = 2$. Ça tombe pile-poil. ;) Nous devons donc choisir un sous-réseau libre pour être re-subnetté. Vous pouvez choisir celui que vous voulez parmi les sous-réseaux libres que nous avons obtenu jusqu'ici. Pour suivre ce TD, choisissez le sous-réseau **00000000/26**. Ici également, nous nous rendons compte que ce sous-réseau a été subnetté de manière à obtenir au moins 50 hôtes (sous-réseau A), voilà pourquoi 6 bits sont disponibles pour les hôtes. Or nous n'avons besoin que de deux bits. Qu'allons-nous faire ? Exactement ce que nous avons fait dans les étapes précédentes, nous allons allouer 4 bits de plus à la partie réseau du masque pour ne rester qu'avec deux bits pour les hôtes. ;) Nous obtenons donc ceci :

```
00**nnnn**hh
```

Maintenant nous avons 4 bits alloués au réseau, ce qui donne la possibilité d'obtenir 16 sous-réseaux (2^4) à partir de ce sous-réseau. Vous devez être capable de déterminer chacun de ces

16 sous-réseaux, mais comme nous sommes gentils aujourd'hui, nous vous écrivons **les huit premiers, l'avant-dernier et le dernier.** ;) Nous avons donc :

- 00000000 = .0/30
- 00000100 = .4/30
- 00001000 = .8/30
- 00001100 = .12/30
- 00010000 = .16/30
- 00010100 = .20/30
- 00011000 = .24/30
- 00011100 = .28/30
- 00100000 = .32/30
-
-
- 00111000 = .56/30
- 00111100 = .60/30

! N.B. : chacun de ces sous-réseaux nous donnera deux hôtes disponibles, vous pouvez donc choisir quatre sous-réseaux parmi les 16 pour les interfaces de liaison, c'est-à-dire pour les adresses **IP** de chaque interface du routeur. Nous allons choisir les quatre premiers, soit de .0/30 -.12/30.

Tenez, si on vous demandait d'agréger les 12 sous-réseaux restants (soit à partir de .16/30) en utilisant la technique du supernetting pour obtenir une seule route, laquelle obtiendrez-vous ?

Un indice ?

👁 Contenu masqué n°4

Ne regardez la réponse qu'après avoir vraiment essayé de trouver : cela ne vous aide pas si vous ne faites pas un effort de pratiquer. 🍎

👁 Contenu masqué n°5

Résumons chacun des sous-réseaux trouvés depuis l'étape 1 :

- 00000000 = .0/26 | nous ne pouvons plus utiliser celui-ci, nous l'avons re-subnetté
- 00000000 = .0/30 | utilisons celui-ci pour le sous-réseau E
- 00000100 = .4/30 | sous-réseau F
- 00001000 = .8/30 | sous-réseau G
- 00001100 = .12/30 | sous-réseau H
- 01000000 = .64/26 | sous-réseau A
- 10000000 = .128/26 | Nous ne pouvons plus utiliser celui-ci, car nous l'avons re-subnetté
- 11000000 = .192/26 | subnet pour un futur agrandissement

- 10000000 = .128/27 | sous-réseau B
- 10100000 = .160/27 | nous ne pouvons plus l'utiliser, car nous l'avons re-subnetté
- 10100000 = .160/28 | sous-réseau C
- 10110000 = .176/28 | sous-réseau D

II.1.1.3. Conclusion et exercices

Ce TD vous a certainement aidé à mieux assimiler le principe du VLSM et du Supernetting. Nous avons au passage revu un certain nombre de notions. En effet, nous avons pratiqué les calculs des puissances de 2, la conversion des masques du décimal au binaire et vice versa, le subnetting d'un réseau, l'interconnexion de deux sous-réseaux différents par le biais d'un routeur etc. Plusieurs autres cas de pratique viendront avec le temps pour vous faire pratiquer tout ce que nous avons appris depuis la première partie du cours : le design de l'infrastructure d'un réseau, l'analyse des contraintes et la mise en place de la meilleure infrastructure répondant au mieux aux besoins, la segmentation des réseaux selon des exigences, la planification d'un plan d'adressage, le diagnostic et bien d'autres joyeusetés qui vous donneront indubitablement un savoir-faire dans le domaine, savoir-faire assez solide pour être admis en stage d'entreprise dans le domaine du réseau. 🍏

Pour terminer, nous vous donnons quelques exercices, pas difficiles du tout.

Dans ce TD, nous n'avons fait que trouver les network ID de chaque subnet qui répondaient aux consignes de notre patron, ce qui, mine de rien, représente plus de 50 % du travail.) À présent, votre travail consistera à la détermination des plages d'adresses pour chaque sous-réseau. Voici, en résumé, ce que vous devez faire :

- Pour chaque sous-réseau (A, B, C, D, E, F et G), déterminez les plages d'adresses. Dans ces plages, déterminez celles que vous allez assigner aux hôtes. Par exemple pour le réseau C, nous aurons 14 adresses utilisables, mais seulement 12 assignables car notre réseau ne comprend que 12 hôtes; les deux autres seront une perte, certes, mais réduite au maximum.
- Choisissez la première adresse IP de chaque plage pour le routeur.
- Éditez le schéma que vous avez utilisé pour ce TD et inscrivez les adresses IP de chacune des interfaces de chaque routeur ainsi que leurs masques respectifs (notation avec un / exigée), pour obtenir quelque chose de similaire au schéma **Figure 1.0** (les adresses IP sont fictives et nous avons omis les masques). Si vous ne pouvez pas l'éditer, contentez-vous de résumer cela dans un tableau. 🍏
- Ajoutez trois hôtes dans les réseaux A, B, C et D et inscrivez, à côté de chacun d'eux, leurs adresses IP et masques respectifs. Votre schéma doit ressembler au schéma **Figure 1.1**. (Ici également, les adresses IP sont fictives et nous nous limitons à un hôte par réseau pour gagner le temps. 🍏)
- Finalement, faites communiquer les hôtes de chaque réseau entre eux. C'est-à-dire, un hôte A1 du réseau A doit communiquer avec un hôte du réseau B, un autre du réseau C et un autre du réseau D. Vous n'avez pas besoin d'un logiciel de simulation pour le faire. Mettez juste des flèches pour illustrer le cheminement du message envoyé, ensuite déterminez les routes (ou les adresses IP des interfaces) par lesquelles ce message passera pour arriver à son destinataire. Votre schéma doit ressembler au schéma **Figure 1.2** (ici également, les adresses sont fictives et nous n'avons pas mis les masques de chaque adresse). Vous pouvez, bien entendu, résumer cela dans un tableau à défaut du schéma.

II.1.1.4. Ci-dessous les images d'illustration

Figure 1.0 - Les réseaux de zéro - zestedesavoir.com

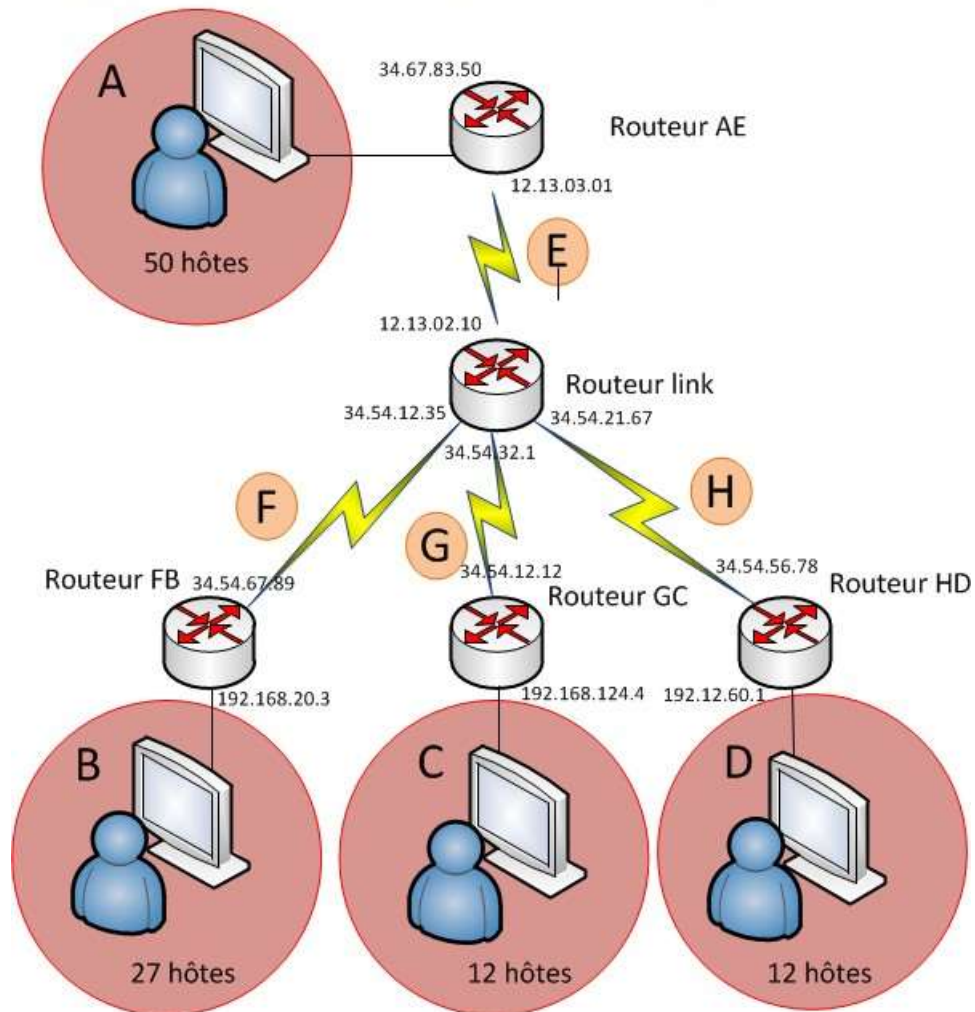


FIGURE III.6.2. – Figure 1.0

Figure 1.1 - Les réseaux de zéro - zestedesavoir.com

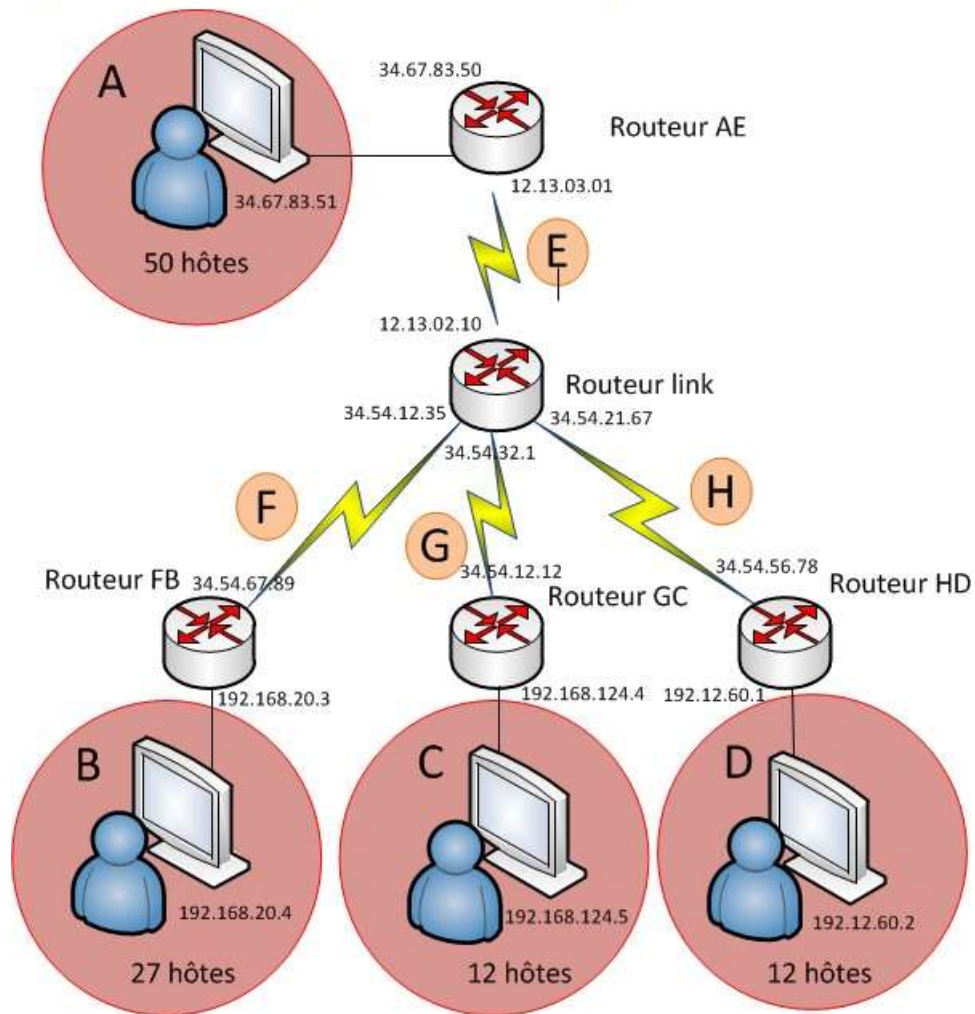


FIGURE III.6.3. – Figure 1.1

Figure 1.2 - Les réseaux de zéro - zestedesavoir.com

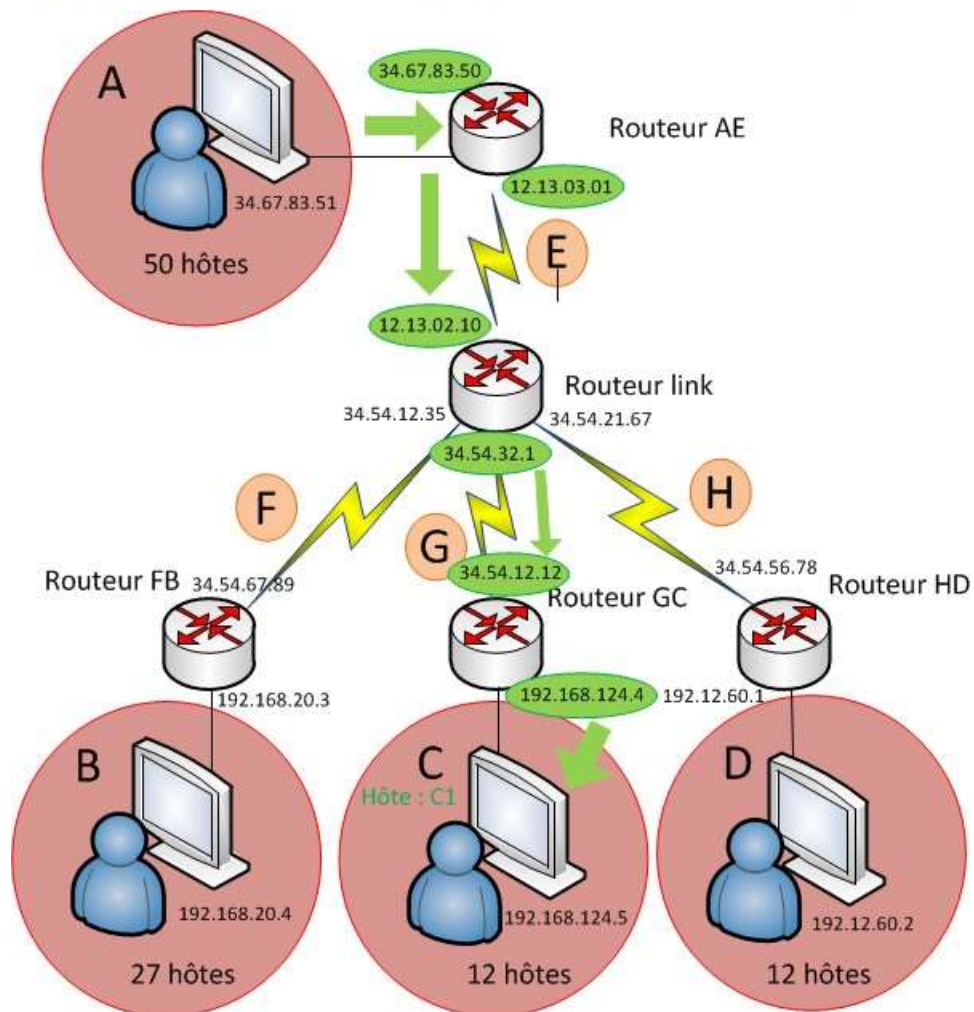


FIGURE III.6.4. – Figure 1.2

Voilà ! Lorsque vous aurez fini, vous pourrez poster vos solutions sur leforum.

i

Il est vraiment important de réussir ces exercices toutseul.

Troisième Partie

Comment créer un réseau local sous Windows

Créer un réseau local sous Windows est étroitement lié au centre réseau et partage du système qui est l'un des plus importants paramètres de votre environnement informatique.

Il vous permet de visualiser chaque réseau auquel vous vous connecter ainsi que les informations vous concernant et vous permettant d'y accéder comme votre adresse IP ou votre adresse MAC.

C'est aussi grâce au centre réseau et partage que vous pouvez définir les ressources communes à partager et configurer les différentes permissions à accorder.

Bref vous l'avez compris:

C'est le centre réseau et partage qui permet de configurer et de paramétrer entièrement la gestion de vos réseaux.

Vous le savez certainement:

La plupart des utilisateurs évitent d'y accéder de peur de changer ou supprimer un des paramètres sans pouvoir le réinitialiser.

Ou tout simplement parce qu'ils ne comprennent pas la majeure partie des options présentées dans l'interface.

Il faut être conscient que la compréhension des concepts de base du centre réseau et partage est la clé pour résoudre plusieurs problèmes liés au partage et transfert de fichiers.

Et la meilleure partie:

Ces problèmes sont très simple à diagnostiquer et à résoudre comme vous le verrez au fur et à mesure de cet article.

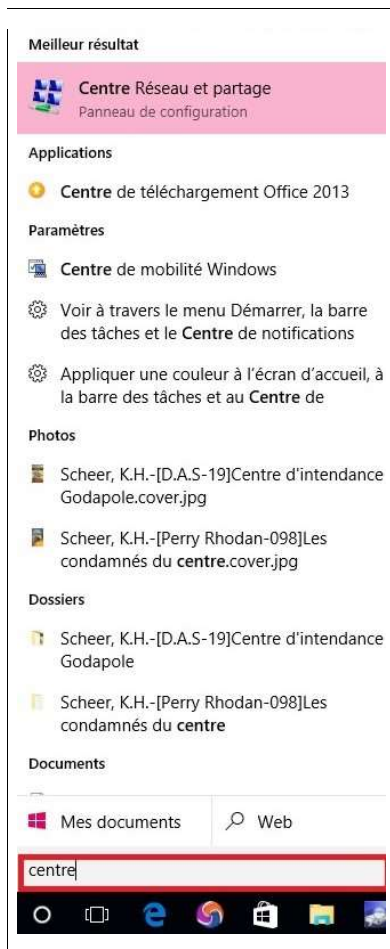
Avant de commencer, sachez que toutes les consignes présentées dans ce tutoriel sont applicables aussi bien sur [Windows 10](#) que sur Windows 8 et Windows 8.1. Elles sont aussi valables pour Windows 7 avec quelques infimes différences.

I. Comment accéder au centre réseau et partage ?

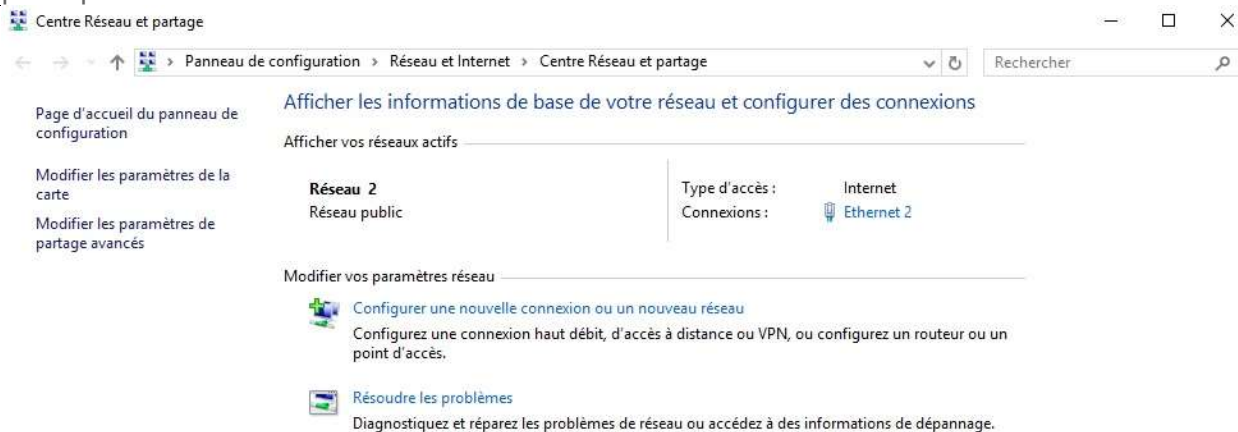
1^{ère} méthode : (valable pour Windows 10)

La méthode la plus rapide pour ouvrir le centre réseau et partage est d'écrire le mot "centre" dans la zone d'exécution comme il est montré dans l'image ci-dessous:

Centre réseau et partage Windows 10

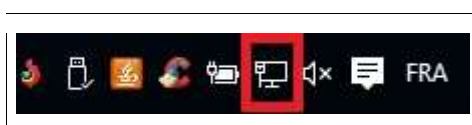


Cliquez ensuite sur l'option "**Centre Réseau et Partage**" et vous aurez accès à l'interface principale:



2^{ème} méthode : (Toutes Les versions de Windows)

Cette méthode consiste à cliquer sur l'icône réseau qui se trouve en bas et à votre droite dans la barre de notifications :



Dans le menu contextuel (celui du bouton droit) cliquez sur l'option "**Ouvrir le centre réseau et partage**" :

Résoudre les problèmes

Ouvrir le Centre Réseau et partage

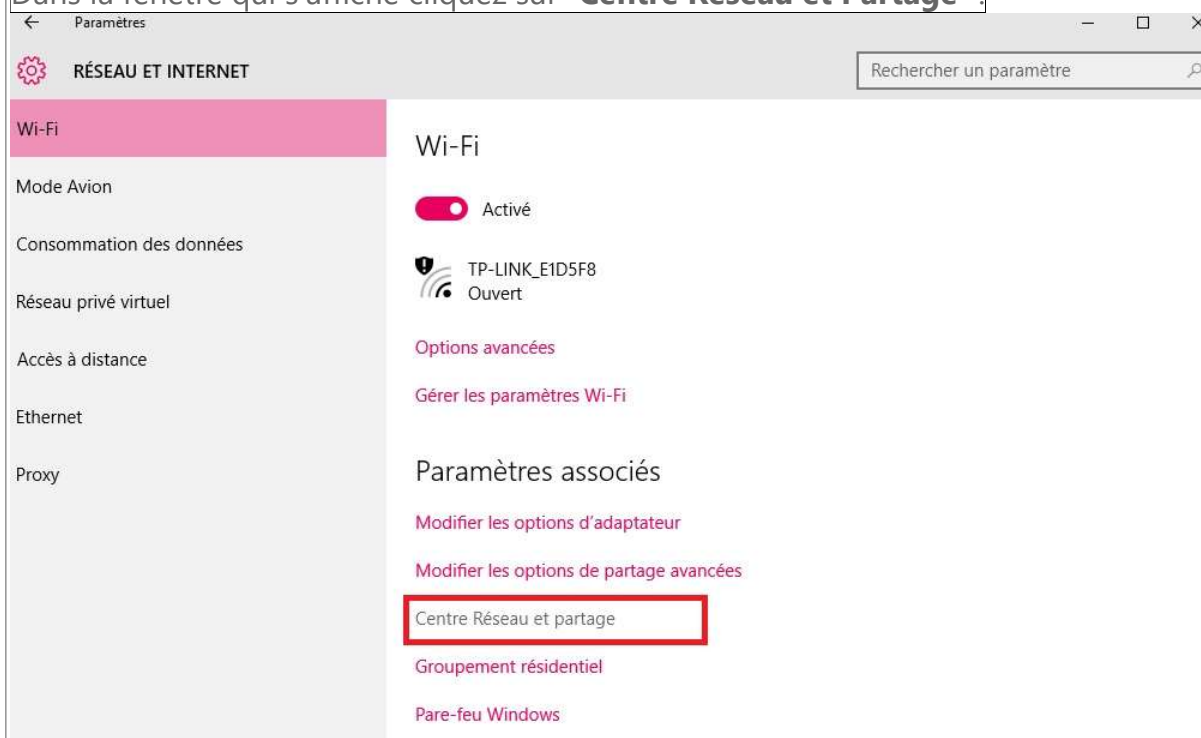
Vous aurez accès à l'interface principale.

3^{ème} méthode : (valable pour Windows 10)

Cliquez sur le menu démarrer pour activer la commande "**Paramètres**" puis cliquez sur l'option "**Réseau et Internet**" :



Dans la fenêtre qui s'affiche cliquez sur "**Centre Réseau et Partage**" :



Et voilà vous avez accès à l'interface principale .

A ce stade vous devriez avoir l'interface du Centre Réseau et Partage affichée devant vous. Ce qui est essentiel pour ce qui va suivre.

Quel Type De Réseau Local Choisir Et Pourquoi ?

Vous avez raison de vous en soucier:

La sécurité des données est cruciale.

En fait, il y a toujours une question qui se pose:

Est ce qu'on peut me voler mes données si je me connecte à un réseau ?

Et on se voit encore plus susceptible lorsqu'on se connecte dans des endroits publics.

Il faut se rendre à l'évidence:

Se faire "pirater" est possible

Mais la bonne nouvelle c'est qu'on peut se protéger grâce à une configuration optimale de votre système.

Vous pouvez suivre notre tutoriel "[Le Guide Ultime Pour Avoir Une Protection Pc Efficace](#)" pour y remédier.

Cependant, même en ayant une protection complète, le choix du type de votre réseau est primordial dans la mesure où le partage de données peut se faire même sans que vous ne le remarquiez.

Il faut savoir qu'il existe 2 types de réseaux :

les réseaux privés et les réseaux publics.

Un réseau public est un réseau auquel vous vous connectez occasionnellement comme dans une gare, un aéroport ou chez un ami.

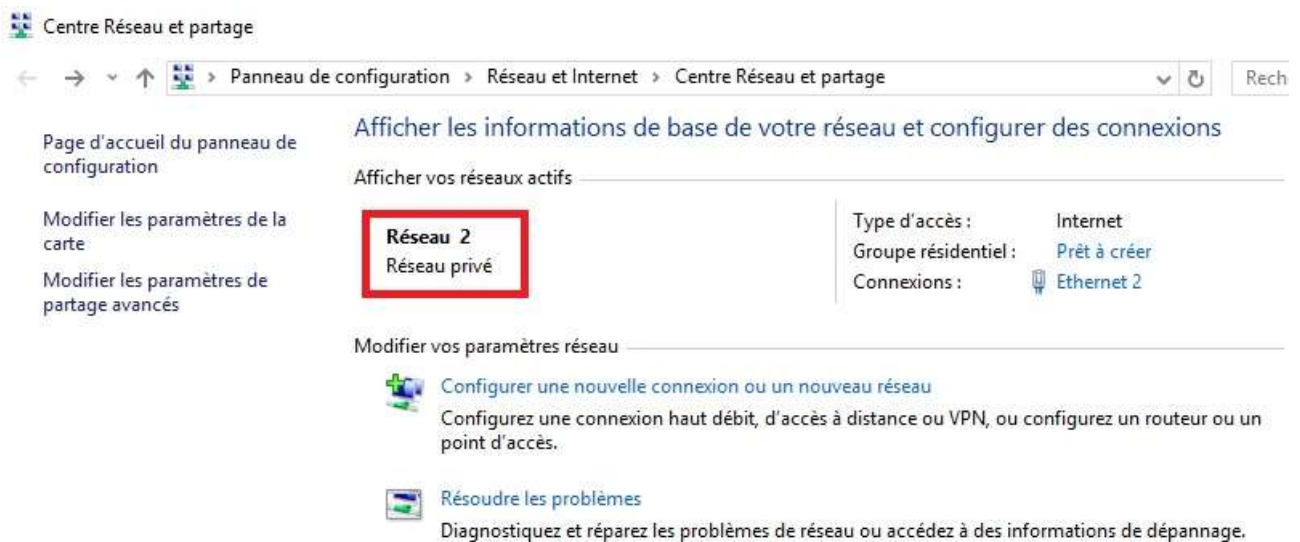
Un réseau privé est un réseau auquel vous êtes continuellement connecté et dans lequel les membres sont connus et ne présentent aucune menace.

Donc, comme vous l'avez compris, si vous êtes connecté à un réseau Wifi public il vaut mieux limiter les partages pour plus de sécurité!

Voici comment faire :

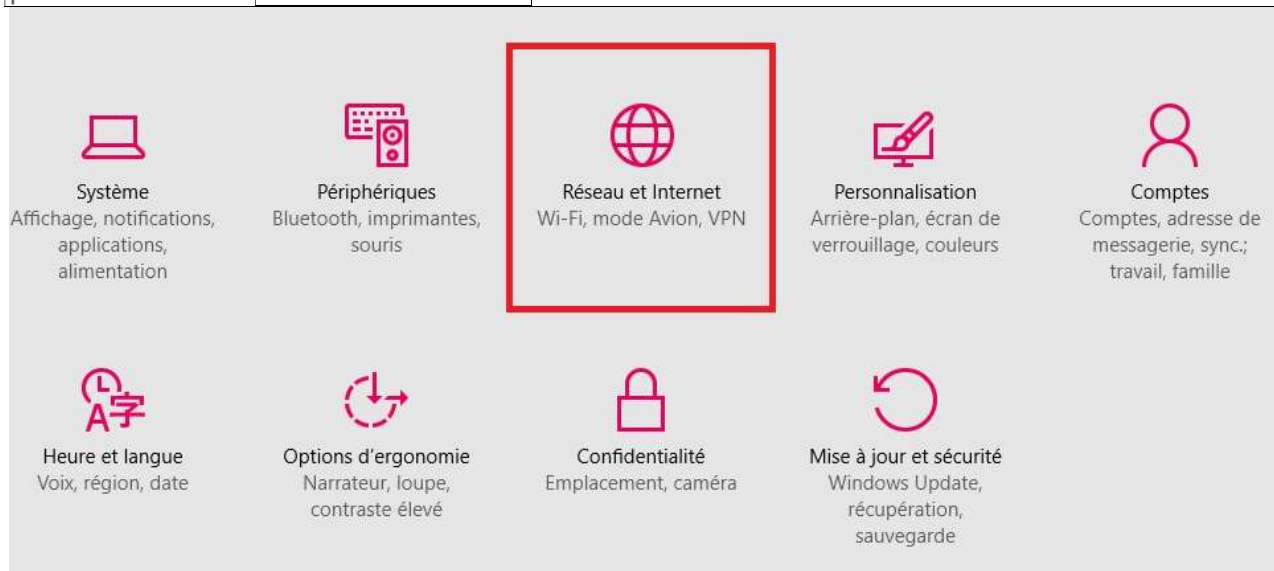
En premier lieu, il faut connaître dans quel type de réseau vous êtes.

Vous pouvez le découvrir grâce à l'interface du centre réseau et partage:



centre réseau et partage

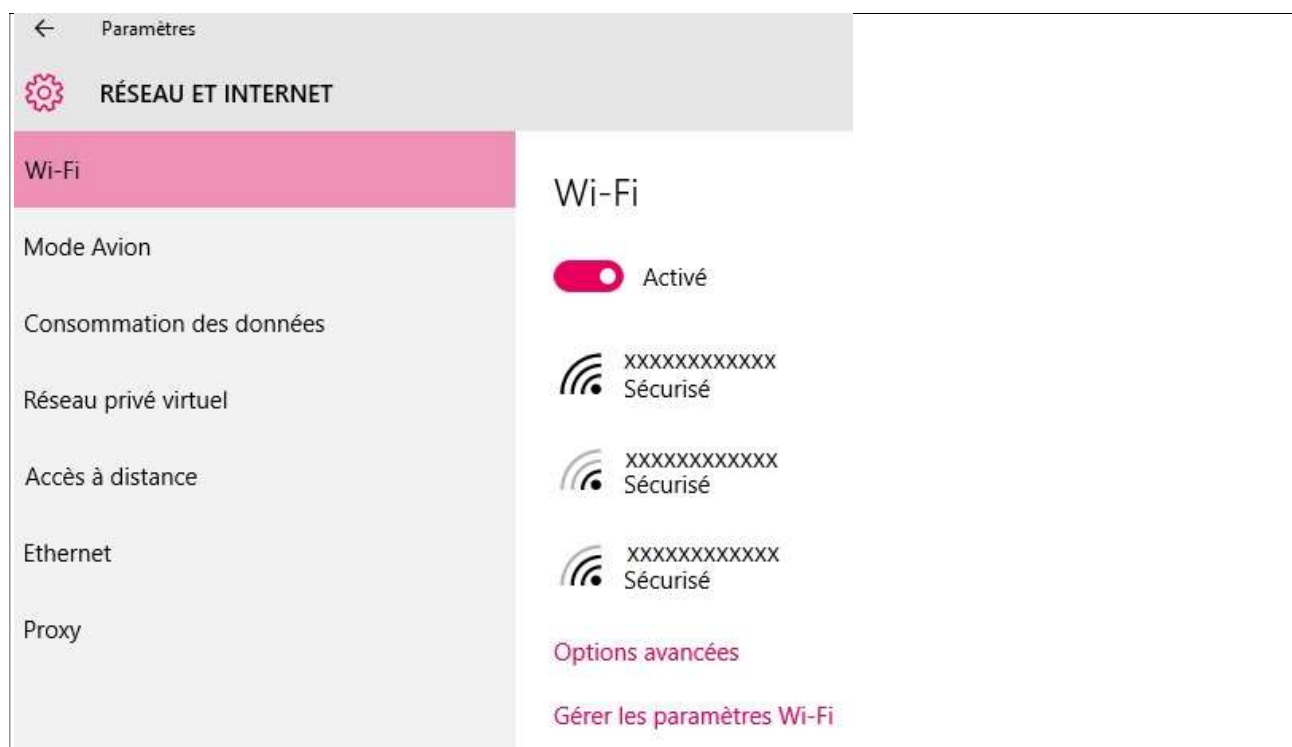
Pour changer le type du réseau, cliquez sur le menu "**Démarrer**" puis accédez aux paramètres puis à la section "**Réseau et Internet**" :



Dans l'interface qui apparaît, vous avez 2 choix possibles selon votre mode de connexion :

- **Si vous êtes connecté en Wifi:**

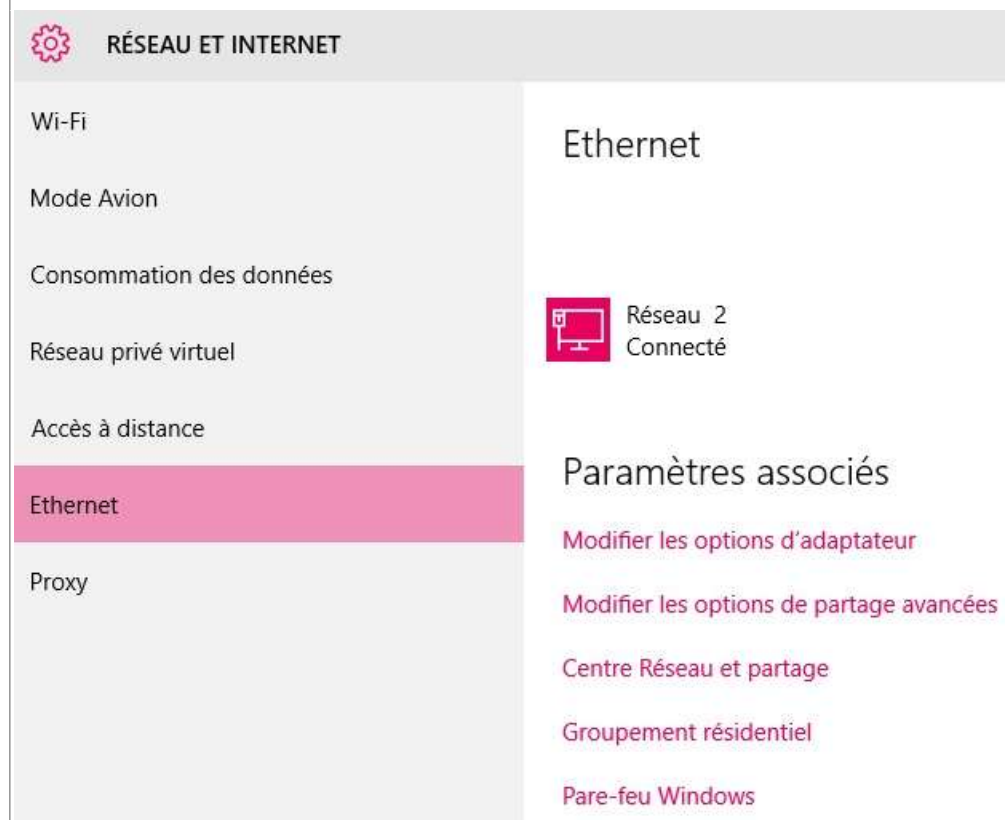
Cliquez sur l'option "**Wifi**" du menu à votre gauche:



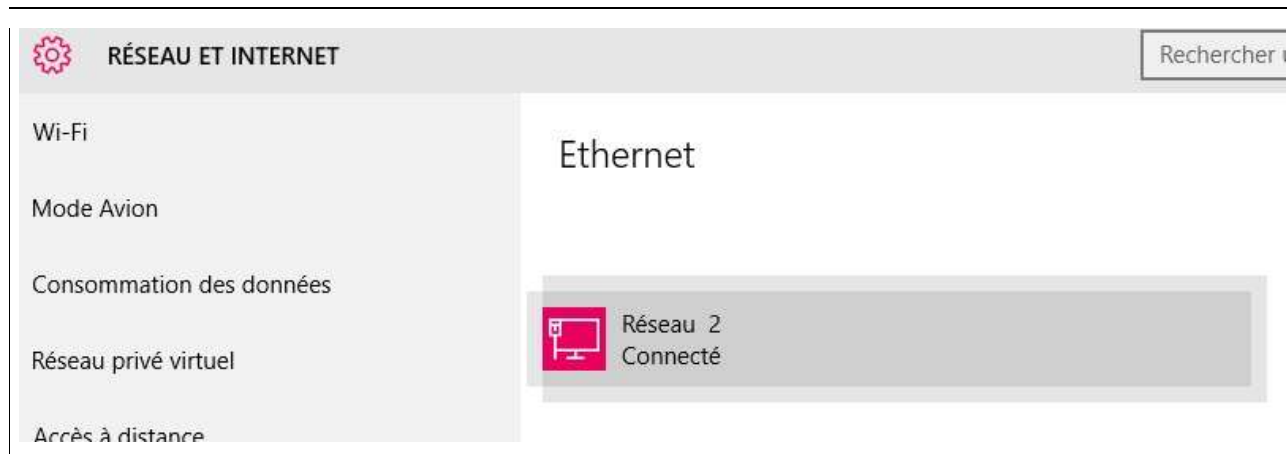
○ **Si vous êtes connecté avec un câble réseau :**

Il faut configurer la connexion Ethernet Windows.

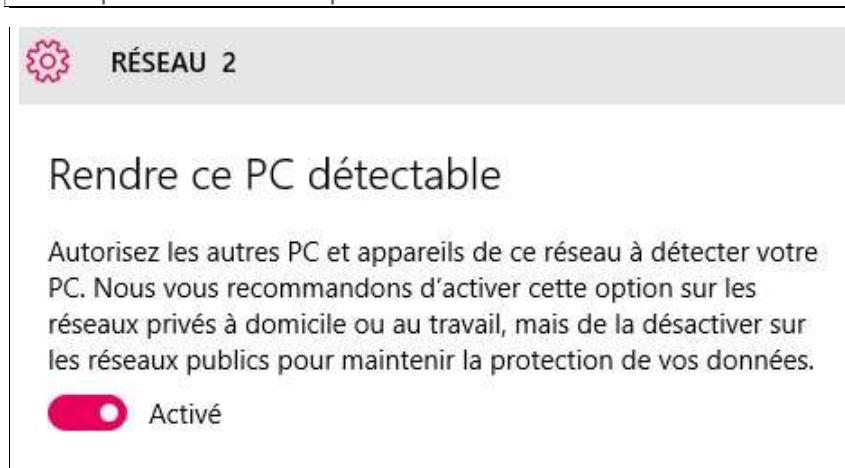
Dans l'interface qui apparaît cliquez sur l'option "Ethernet" du menu à votre gauche:



Puis cliquez sur le nom de votre connexion affiché à votre droite :



Dans le menu qui s'affiche désactiver l'option "**Rendre ce PC détectable**" pour passer du mode public en mode privé :



Si le concept des réseaux privés et publics est encore un flou.

J'explique avec un exemple:

Supposons que vous êtes connecté dans une gare, il vaut mieux rendre votre PC indétectable pour limiter les partages et ainsi garder toutes vos données pour vous même.

Par contre, si vous êtes chez un ami de confiance et que vous avez un dossier "Série" sur votre PC et que vous voulez lui donner l'accès à ce dossier par réseau (Procédure que nous verrons un peu plus loin dans ce guide) alors il vaudrait rendre votre PC détectable sur le réseau.

Vous remarquerez aussi qu'à chaque fois que vous vous connectez sur un réseau Windows vous demande de partager votre réseau avec vos contacts :

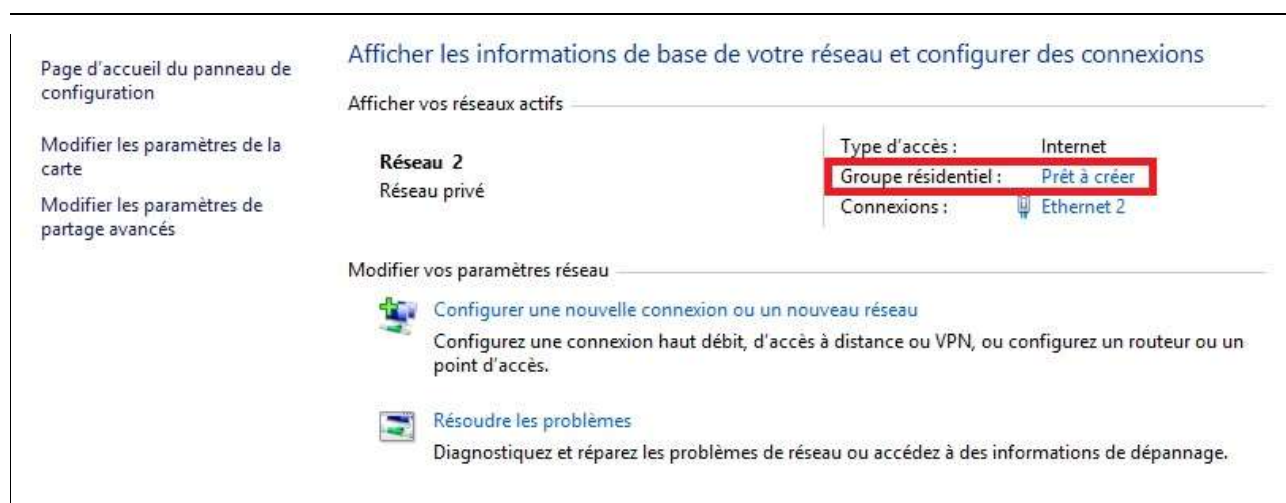


Il suffit de cocher ou de ne pas cocher l'option demander pour partager ou non vos données (Avez vous remarqué que la fenêtre est de couleur rose ? vous pouvez aussi personnaliser la couleur de vos fenêtres dans Windows 10 et personnaliser toute votre interface en suivant le tutoriel "[Personnaliser l'Interface De Windows 10 De 5 Façons Différentes](#)")

Mais bien que Windows 10 vous laisse le choix, il est toujours plus sûr de revérifier votre statut et de le changer manuellement.

Lorsque vous passer en mode Public, sachez que même si vous n'avez pas de dossiers partagés, Windows partage les dossiers publics à votre place. Donc si vous y stocker des fichiers ils seront accessibles aux autres membres du réseau. Les dossiers publics sont dans le dossier "Utilisateurs" de la racine C:

Revenons à l'interface de ce bon vieux centre réseau et partage qui donne toutes les informations utiles à propos du réseau sur lequel vous êtes connecté :



l'option qui nous intéresse à ce stade est le groupe résidentiel qui affiche le statut "**Prêt à créer**".

Mais avant de répondre à cet appel du système, il faut bien évidemment comprendre la notion de "**Groupe résidentiel**".

Partager vos données rapidement grâce au Groupe Résidentiel

Un groupe résidentiel est une méthode pour gérer un réseau privé (sur lequel le partage est activé) et qui permet de créer un groupe incluant des dossiers partagés accessible grâce à un code fixé au préalable.

L'avantage est que le partage est très pratique et devient simple et rapide pour chaque périphérique de votre groupe sans pour autant ayant des configurations à réaliser pour chaque connexion.

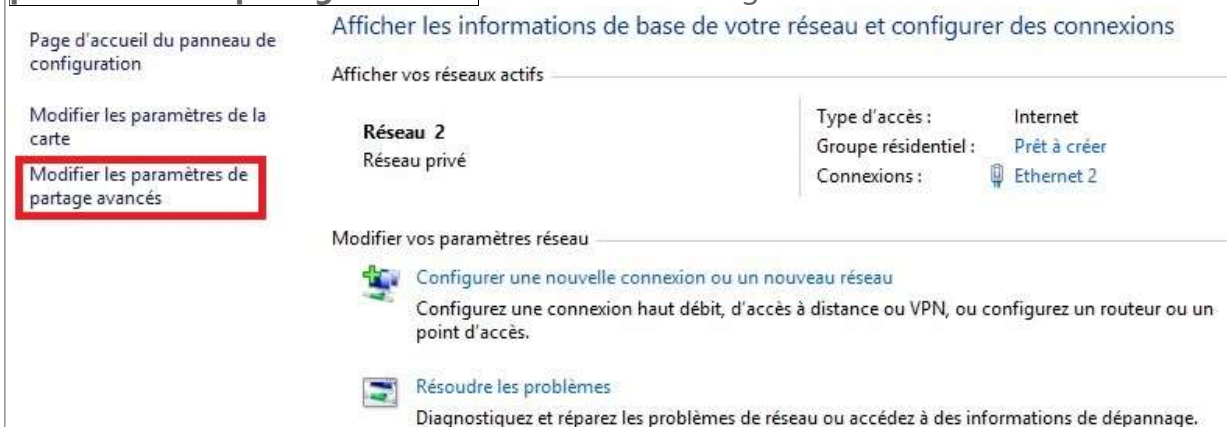
Ce qui fait que même en n'étant pas un expert en la matière vous serez capable de partager vos données avec toute votre famille et amis, ainsi que tous vos périphériques comme votre TV, tablette ou smartphone.

Comment créer votre groupe résidentiel

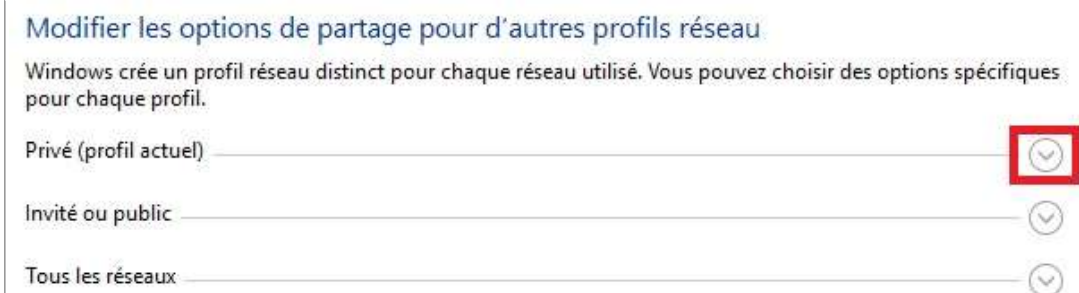
Les paramètres requis

Comme je l'ai déjà mentionné, pour utiliser un groupe résidentiel il faut d'abord activer le partage. Pour cela, nous allons procéder comme suit :

dans l'interface du centre réseau et partage cliquez sur l'option "**Modifier les paramètres de partage avancés**" du menu à votre gauche :



Dans l'interface qui s'affiche, développer l'onglet "**Privé**" en cliquant sur la petite flèche comme indiqué ci-dessous :



Dans les options, cochez:

- Activez la découverte de réseau
- Activez la configuration automatique des périphériques connectés au réseau
- Activer le partage de fichiers et d'imprimantes
- Autoriser Windows à gérer les connexions des groupes résidentiels (recommandé)

Vous devrez avoir les options suivantes cochées :

Privé (profil actuel) ⌵

Recherche du réseau

Quand la découverte du réseau est activée, cet ordinateur peut voir les autres ordinateurs et périphériques du réseau, et peut lui-même être vu par les autres ordinateurs du réseau.

☒ Activer la découverte de réseau

☒ Activez la configuration automatique des périphériques connectés au réseau.

☐ Désactiver la découverte de réseau

Partage de fichiers et d'imprimantes

Lorsque le partage de fichiers et d'imprimantes est activé, toute personne sur le réseau peut accéder aux fichiers et aux imprimantes que vous avez partagés à partir de cet ordinateur.

☒ Activer le partage de fichiers et d'imprimantes

☐ Désactiver le partage de fichiers et d'imprimantes

Connexions du Groupement résidentiel

En général, Windows gère les connexions aux autres ordinateurs du groupe résidentiel. Mais si vous avez le même compte d'utilisateur et le même mot de passe sur tous vos ordinateurs, vous pouvez configurer le Groupement résidentiel pour utiliser votre compte.

☒ Autoriser Windows à gérer les connexions des groupes résidentiels (recommandé)

☐ Utiliser les comptes d'utilisateurs et les mots de passe pour se connecter à d'autres ordinateurs

La création

Maintenant que les options requises sont activées, vous pouvez créer votre groupe résidentiel en allant à l'interface du centre réseau et partage puis en cliquant sur l'option **"Prêt à créer"** :

Page d'accueil du panneau de configuration

Modifier les paramètres de la carte

Modifier les paramètres de partage avancés

Afficher les informations de base de votre réseau et configurer des connexions

Afficher vos réseaux actifs


Réseau 2
Réseau privé


Type d'accès : Internet

Groupe résidentiel : Prêt à créer

Connexions : Ethernet 2

Modifier vos paramètres réseau

 Configurer une nouvelle connexion ou un nouveau réseau
Configurez une connexion haut débit, d'accès à distance ou VPN, ou configurez un routeur ou un point d'accès.

 Résoudre les problèmes
Diagnosticuez et réparez les problèmes de réseau ou accédez à des informations de dépannage.

Dans Windows 10, si cette option n'apparaît pas dans l'interface du centre réseau et partage, vous pouvez y accéder en cliquant sur le menu **"Démarrer"**

→ **"Paramètres"** → **"Wifi"** ou **"Ethernet"** → **"Groupement résidentiel"**

Dans la fenêtre qui s'affiche, cliquez sur le bouton **"Créer un groupe résidentiel"** :

Partager avec d'autres ordinateurs domestiques



Le réseau ne comporte actuellement aucun groupe résidentiel.

Un groupe résidentiel vous permet de partager des fichiers et des imprimantes avec d'autres ordinateurs sur votre réseau domestique. Vous pouvez également diffuser du contenu multimédia vers des périphériques.

Le groupe résidentiel est protégé par un mot de passe et vous aurez toujours la possibilité de choisir ce que vous partagez avec le groupe.

[Modifier les paramètres de partage avancés...](#)

[Démarrer l'utilitaire de résolution des problèmes liés au Groupement résidentiel](#)

Créer un groupe résidentiel

Fermer

Cliquez ensuite sur le bouton "Suivant" :



Créer un groupe résidentiel

Vous pouvez partager des fichiers et des imprimantes avec d'autres ordinateurs. Vous pouvez également diffuser du contenu multimédia vers des périphériques.

Le groupe résidentiel est protégé par un mot de passe et vous aurez toujours la possibilité de choisir ce que vous partagez.



Suivant






Annuler

Sélectionnez les dossiers que vous voulez partager sur votre groupe résidentiel puis cliquez sur le bouton "Suivant" :

← Créer un groupe résidentiel

Partager avec d'autres membres du groupe résidentiel

Sélectionnez les fichiers et périphériques que vous acceptez de partager et définissez les niveaux d'autorisation.

Bibliothèque ou dossier	Autorisations
 Images	Partagé ▼
 Vidéos	Partagé ▼
 Musique	Partagé ▼
 Documents	Non partagé ▼
 Imprimantes et périphériques	Partagé ▼ Partagé Non partagé

Suivant

Annuler

Le mot de passe requis pour les nouveaux périphériques de votre groupe résidentiel s'affiche :

← Créer un groupe résidentiel

Utilisez ce mot de passe pour ajouter des ordinateurs à votre groupe résidentiel

Pour accéder aux fichiers et imprimantes situés sur d'autres ordinateurs, ajoutez ces derniers à votre groupe résidentiel. Vous avez besoin du mot de passe suivant.

Notez ce mot de passe :

ew9aM2zb7p

[Imprimer le mot de passe et les instructions](#)

Si vous oubliez le mot de passe de votre groupe résidentiel, vous pouvez l'afficher ou le changer en ouvrant Groupement résidentiel dans le Panneau de configuration.

Terminer

Ce mot de passe est à saisir une seule fois lors de la première connexion.

Si l'opération s'est bien déroulée vous aurez le message "**Jonction effectuée**" au lieu de "**Prêt à la création**" :

Page d'accueil du panneau de configuration

Modifier les paramètres de la carte

Modifier les paramètres de partage avancés

Afficher les informations de base de votre réseau et configurer des connexions

Afficher vos réseaux actifs

Réseau2
Réseau privé

Type d'accès : Internet
Groupe résidentiel : **Jonction effectuée**
Connexions :  Wi-Fi

Modifier vos paramètres réseau



Configurer une nouvelle connexion ou un nouveau réseau

Configurez une connexion haut débit, d'accès à distance ou VPN, ou configurez un routeur ou un point d'accès.




Résoudre les problèmes

Diagnostiquez et réparez les problèmes de réseau ou accédez à des informations de dépannage.


Vous avez la possibilité de configurer totalement votre groupe résidentiel en cliquant sur la mention "**Jonction effectuée**" :


Modifier les paramètres du groupe résidentiel

Bibliothèques et périphériques que vous partagez à partir de cet ordinateur

 Images

 Vidéos

 Musique

 Imprimantes et périphériques

Modifier ce que vous partagez avec le groupe résidentiel

Autoriser tous les périphériques sur ce réseau, tels que les téléviseurs et les consoles de jeu, à lire mon contenu partagé

Autres actions liées aux groupes résidentiels

Afficher ou imprimer le mot de passe du groupe résidentiel



Modifier le mot de passe...

Quitter le groupe résidentiel...

Modifier les paramètres de partage avancés...

Démarrer l'utilitaire de résolution des problèmes liés au Groupement résidentiel

Comme vous pouvez le constater, les options, de par leurs libellés, sont faciles à gérer.

Commençons par l'option:

Modifiez ce que vous partagez avec le groupe résidentiel

Cette option permet de changer la liste des dossiers que vous partagez avec le groupe et cela en changeant le statut en "**Partagé**" ou en "**Non partagé**" :

Partager avec d'autres membres du groupe résidentiel

Sélectionnez les fichiers et périphériques que vous acceptez de partager et définissez les niveaux d'autorisation.

Bibliothèque ou dossier	Autorisations
Images	Partagé
Vidéos	Partagé
Musique	Partagé
Documents	Partagé Non partagé
Imprimantes et périphériques	Partagé

Suivant

Annuler

○ Autoriser tous les périphériques sur ce réseau :

Cette option vous permet de partager des données avec d'autres périphériques comme votre télévision. Ce qui est pratique si vous avez un dossier "**Films**" partagé de façon à regarder le contenu de ce dossier (des films) directement sur votre télévision. Pour cela cliquez sur l'option en question pour afficher la fenêtre suivante :

Sélectionner les options de diffusion multimédia en continu pour les ordinateurs et les périphériques

La diffusion multimédia en continu est désactivée.

La diffusion multimédia en continu vous permet d'envoyer votre musique, vos images et vos vidéos à d'autres ordinateurs et périphériques sur votre réseau. Elle vous permet également de recevoir des fichiers multimédias d'autres ordinateurs et périphériques.

Si vous activez la diffusion multimédia en continu, votre profil de réseau et vos paramètres de pare-feu actuels seront modifiés. Activez-la uniquement sur des réseaux de confiance, tels que des réseaux domestiques ou d'entreprise.

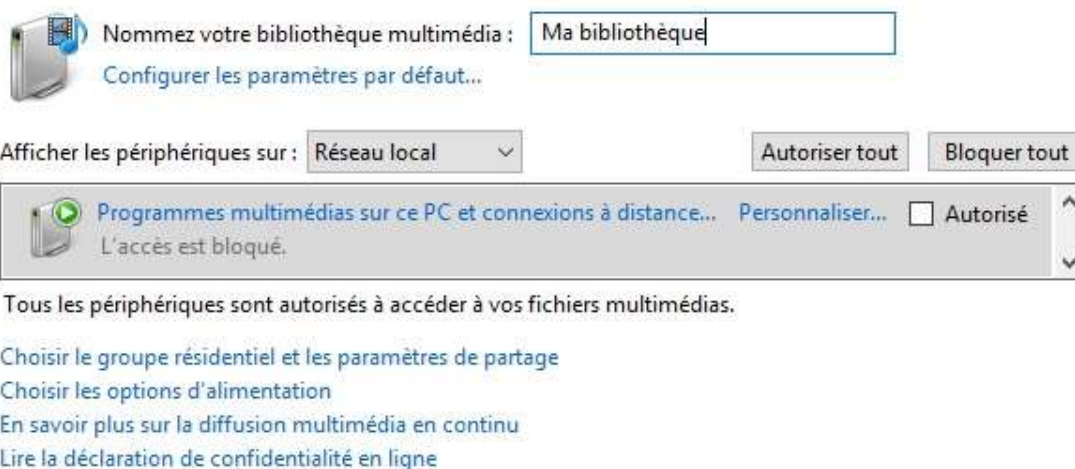
Activer la diffusion multimédia en continu

[En savoir plus sur la diffusion multimédia en continu](#)

[Lire la déclaration de confidentialité en ligne](#)

En cliquant sur le bouton "**Activer la diffusion multimédia en continu**" vous afficherez l'interface de configuration :

Sélectionner les options de diffusion multimédia en continu pour les ordinateurs et les périphériques



Cette fenêtre permet de configurer des périphériques annexes pour que les dossiers partagés dans votre groupe résidentiel leur soient accessibles.

Cette configuration consiste en les opérations suivantes:

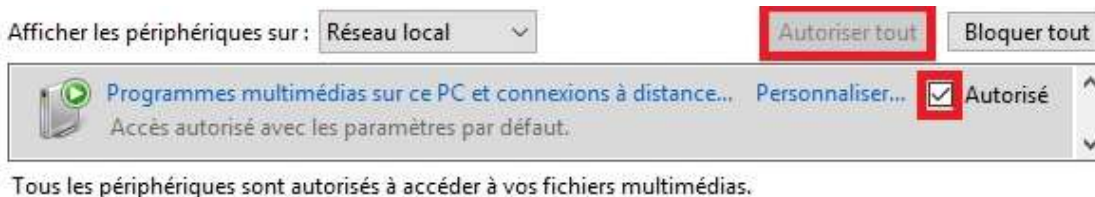
○ **Modifier le nom de votre bibliothèque multimédia**

Donner un nom à votre bibliothèque multimédia qui est l'ensemble des dossiers du groupe. Vous pouvez le voir dans l'image ci-dessous : le nom est "**Ma bibliothèque**".

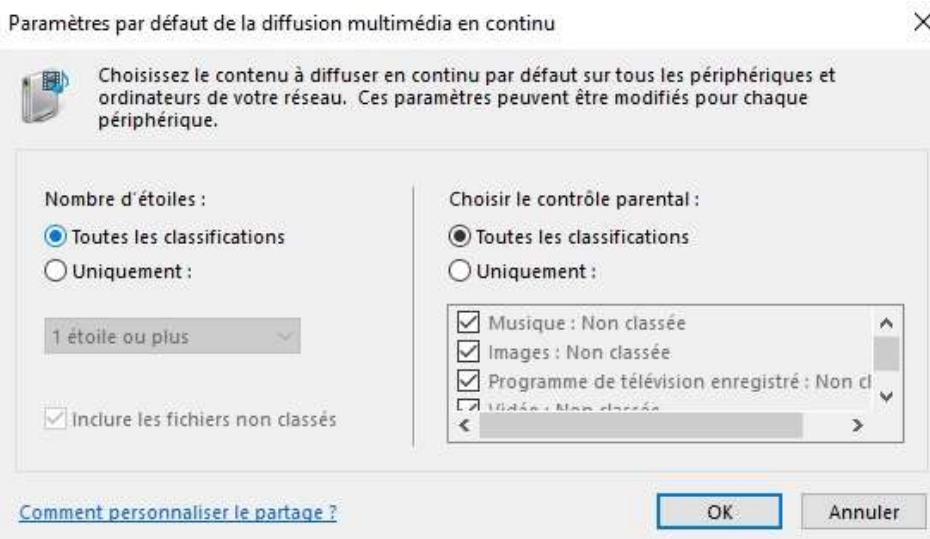


○ **Autoriser les périphériques multimédia à se connecter à votre groupe**

Il suffit de cliquer sur le bouton "**Autoriser tout**" pour rendre accessible votre groupe aux applications et aux périphériques multimédia. En plus la case "**Autoriser**" sera d'elle même cochée.



Il vaut mieux laisser toutes les autres options intactes sans aucun changement. Les options en question sont celles affichées en cliquant sur l'option "**Personnaliser**" :



Cependant, pour ceux qui veulent filtrer le contenu partagé, ils peuvent sélectionner par classe les catégories de fichiers à utiliser, surtout si c'est dans le cadre d'un **contrôle parental**.

o **Les options relatives au mot de passe de votre groupe résidentiel**

Dans cette rubrique vous afficher votre mot de passe ou l'imprimer.

Vous pouvez même le changer en un mot de passe plus simple à retenir, vu que les mots de passe sont générés aléatoirement par le système.

Les 2 options concernées sont

"Afficher ou imprimer le mot de passe du groupe résidentiel"

et **"Modifier le mot de passe"** :

[Modifier les paramètres du groupe résidentiel](#)

Bibliothèques et périphériques que vous partagez à partir de cet ordinateur

Images

Vidéos

Musique

Documents

Imprimantes et périphériques

[Modifier ce que vous partagez avec le groupe résidentiel](#)

[Autoriser tous les périphériques sur ce réseau, tels que les téléviseurs et les consoles de jeu, à lire mon contenu partagé](#)

Autres actions liées aux groupes résidentiels

[Afficher ou imprimer le mot de passe du groupe résidentiel](#)

[Modifier le mot de passe...](#)

[Quitter le groupe résidentiel...](#)

[Modifier les paramètres de partage avancés...](#)

[Démarrer l'utilitaire de résolution des problèmes liés au Groupement résidentiel](#)

Vous devez être conscient que seulement votre bibliothèque est partagée dans votre groupe résidentiel. Un autre utilisateur n'est pas obligé de partager ses dossiers que

s'il crée lui aussi son propre groupe résidentiel ou qu'il veuille partager ses propres

dossiers

Se connecter à un groupe résidentiel

Maintenant que votre groupe résidentiel est créé et proprement configuré, quelle serait son utilité si on ne s'y connecte pas ?

La procédure est trop simple, car il suffit juste de cliquer sur l'option "**Joindre**" qui apparaît sur l'interface du centre réseau et partage sur le PC qui vient de se connecter à votre réseau. Le système lui demande de saisir le mot de passe que vous aurez fourni (étant le créateur et par conséquent l'administrateur) et le tour est joué !

Si un problème persiste et qu'un nouvel utilisateur ne peut pas accéder à votre groupe résidentiel, essayez de vérifier les options de partage avancé expliqué au début de la partie consacrée aux groupes résidentiels de cet article.

4. Partager des dossiers spécifiques avec le groupe résidentiel :

L'avantage d'un groupe résidentiel réside surtout dans la grande facilité de partage de ressources.

Ces ressources étant essentiellement issues de votre bibliothèque multimédia.

Mais soyons honnêtes:

Qui a vraiment des dossiers tellement ordonnés pour qu'ils se trouvent tous dans le même emplacement?

Ou encore qui stockent tous ses dossiers sur un même et seul support?

Et encore, qui de nous n'a pas de dossier dans lequel il copie plein de trucs "à voir"?

Personnellement, j'ai 2 disques externes dans lesquels je sauvegarde mes MP3, mes séries, les films que je veux regarder et tous mes autres documents.

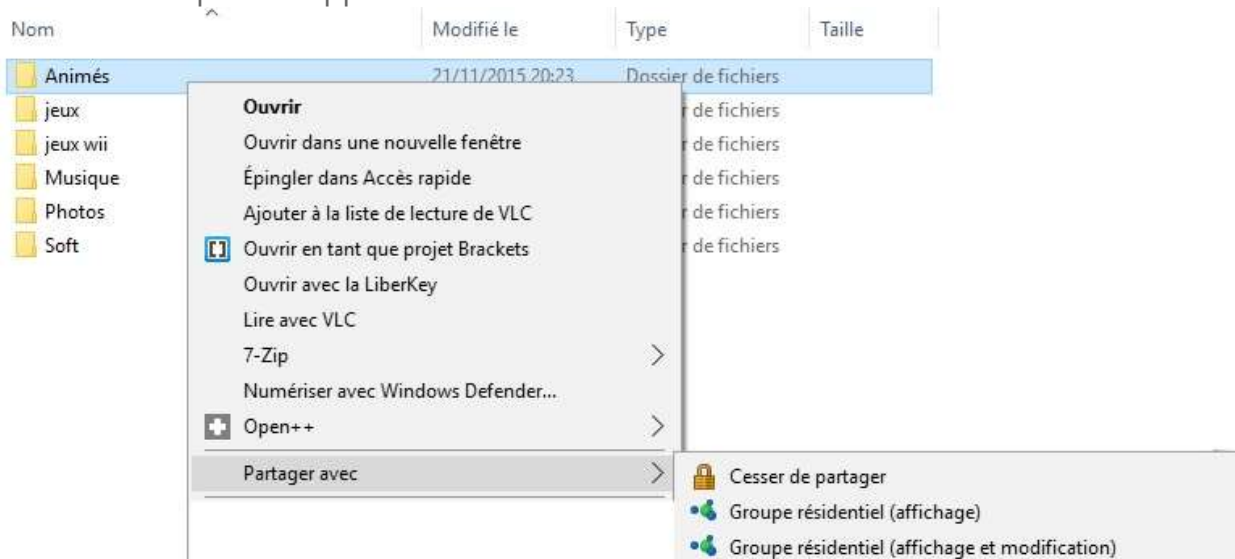
L'intérêt serait de pouvoir aussi les partager dans un groupe résidentiel pour pouvoir y accéder d'un autre emplacement mon réseau privé.

En fait c'est hyper facile à réaliser:

Il suffit juste de sélectionner le dossier à partager puis de cliquer avec le bouton droit et d'activer l'option "Partager avec" puis de choisir l'une des 2 options disponibles :

- **"Groupe résidentiel (Affichage)"** : ce qui donne seulement le droit de lecture sans pouvoir y modifier quelque chose.
- **"Groupe résidentiel (Affichage et modification)"** : ce qui donne aux utilisateurs du groupe le droit de lecture et d'écriture (ils peuvent aussi modifier le contenu du dossier partagé).

Si par exemple je veux partager le dossier "**Animés**" qui se trouve sur la partition D:\ de mon PC je devrais choisir "**Partager avec**" et sélectionner "**Groupe résidentiel (affichage)**" pour éviter tout risque de suppression accidentelle:



La commande "**Cesser de partager**" parle d'elle même : elle permet de ne plus partager un dossier.

Dépanner, réparer et créer un réseau local facilement

Est ce que c'est possible ?

Non, c'est trop difficile pour moi ? Je n'y connais rien!

Des questions de ce genre peuvent être légitimes dans un sens, mais elles viennent toutes du fait que les facettes techniques d'un réseau vous sont totalement inconnues.

Je vous garantis que si vous preniez la peine de comprendre juste un petit peu les notions nécessaires (qui sont vraiment simples), tout le charabia qu'on vous balance sera très clair.

Alors pour commencer, et pour nous faire une idée des notions nécessaires à connaître nous allons afficher les informations relatives à votre réseau.

Comprendre les bases de votre réseau local pour le dépanner et le configurer

Pour cela, dans le centre réseau et partage cliquez sur l'option "**Connexions**" :

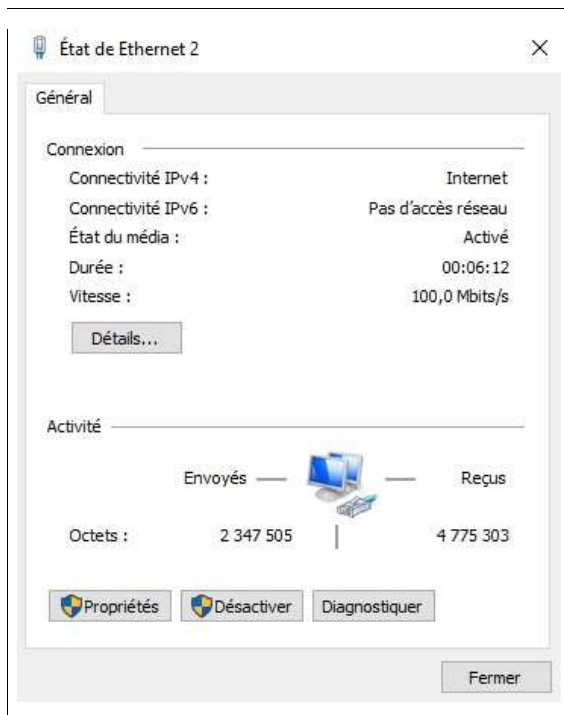
[Afficher les informations de base de votre réseau et configurer des connexions](#)

Afficher vos réseaux actifs

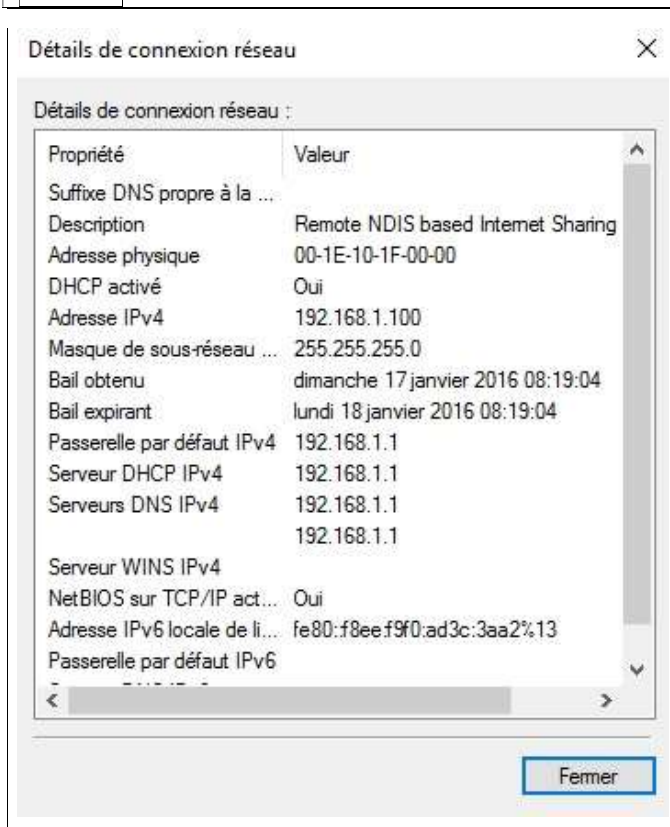
Réseau 2
Réseau privé

Type d'accès : Internet
Groupe résidentiel : Jonction effectuée
Connexions : Ethernet 2

Ce qui aura pour effet d'afficher la fenêtre suivante :



Les détails techniques concernant votre réseau sont en réalité affichés grâce au bouton **"Détails"** :

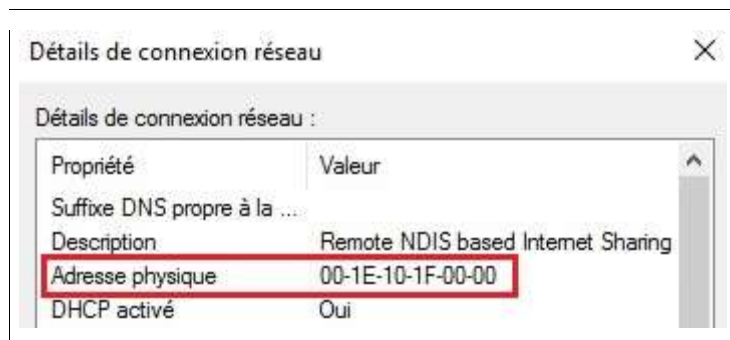


Nous n'allons pas déchiffrer toutes ces notions, mais plutôt essayer de comprendre les plus importantes :

- **L'adresse physique**
- **L'adresse IP**
- **Le DHCP**
- **Le masque sous réseau**

L'adresse physique:

Dans la fenêtre des détails, c'est la 3ème ligne :



Une adresse physique ou une adresse MAC (c'est le même terme) est l'adresse de votre carte réseau.

Elle est unique dans le monde.

En d'autres termes:

Chaque périphérique connecté à n'importe quel réseau possède une adresse physique.

Cela s'applique aux ordinateurs, aux tablettes, aux smartphones...etc.

Mais à quoi ça sert ?

Cette adresse est très pratique du fait qu'elle permet de différencier chaque périphérique à part et de manière unique.

Par exemple:

Si vous avez chez vous un ordinateur, 3 smartphones et une tablette qui sont connectés à Internet grâce à un seul et même routeur, un routeur étant l'appareil fourni par votre fournisseur d'accès lors d'un abonnement à n'importe quel forfait, l'ensemble que forme ces appareils sont un réseau local.

Quelqu'un qui voudrait envoyer des informations depuis Internet à l'un des appareils de votre réseau local, l'envoie en réalité à l'adresse du routeur qui lui différencie le destinataire grâce à son adresse physique.

Je connais mon adresse MAC, et après?

Si vous connaissez l'adresse MAC de chaque périphérique dont vous disposez, vous pouvez créer votre réseau en filtrant les appareils grâce à cette adresse.

Ce qui veut dire que vous pouvez donner l'accès à votre réseau seulement aux adresses physiques dont vous disposez.

Vous pouvez réaliser cette procédure en suivant notre tutoriel "[Autoriser ou empêcher des périphériques de se connecter à votre réseau wifi grâce à leurs adresses MAC](#)".

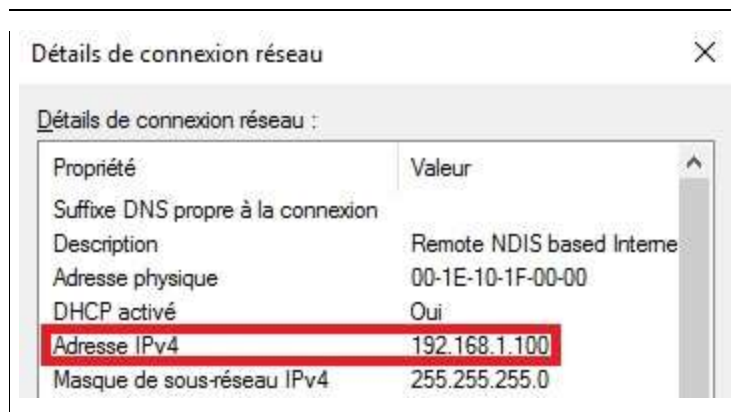
La plupart d'entre nous ignorent que le grand avantage de connaître son adresse MAC permet de retrouver votre PC ou votre smartphone ou votre tablette en cas de perte ou de vol.

C'est grâce à cette adresse que les services spécialisés peuvent retrouver votre appareil.

Il s'avère donc très utile de connaître son Adresse Physique.

L'adresse IP

Votre adresse IP est représentée dans la fenêtre des détails par la 5ème ligne :



Une adresse IP est un moyen d'identification numérique d'un appareil connecté à Internet.

Cette adresse est aussi unique mais elle n'est en aucun cas permanente comme une adresse physique.

Chaque périphérique connecté à internet possède une adresse IP.

Vous pouvez la reconnaître grâce à la forme composée de 4 chiffres séparés par des points : xxx.xxx.xxx.xxx

Le concept est très facile à comprendre grâce à cette astuce :

- Dans votre navigateur Internet, au lieu de saisir l'adresse www.wikipedia.org saisissez l'adresse IP : **91.198.174.192**

Vous aurez exactement le même résultat !

Ce qui montre que tout est connecté à Internet grâce à des adresses IP.

Oui vous l'avez compris et vous vous demandez certainement :

A quoi ça m'avance de connaître mon adresse IP ?

En fait, théoriquement ça ne vous avance en absolument rien du tout !

Ça existe, et c'est comme ça.

Pour communiquer et envoyer des données sur Internet, une adresse IP est essentielle.

D'un autre côté (le côté pratique), vous pouvez tirer un grand avantage du fait de connaître votre adresse IP et cela suivant votre activité :

Personnellement j'ai besoin de cette adresse pour me connecter à des serveurs privés de jeu en ligne.

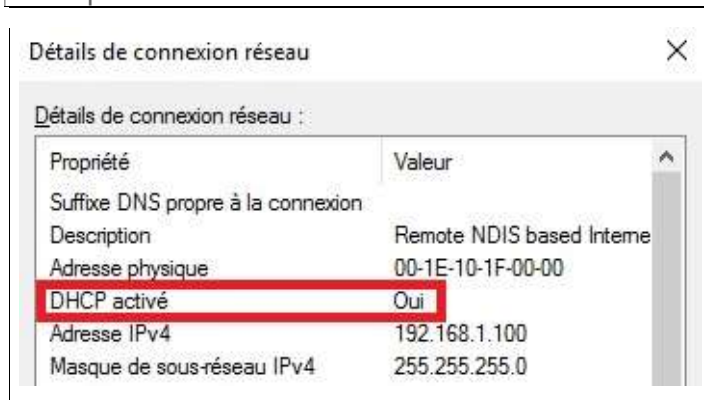
En plus, pour utiliser certains gestionnaires de téléchargement, on a souvent besoin de connaître son adresse IP pour l'utiliser dans les différentes configurations possibles du dit gestionnaire.

Elle est utile aussi dans plein de domaines, comme le domaine de la télésurveillance qui utilise des caméras IP (sans entrer dans les détails !)

Mais en général, c'est dans un souci de sécurité et d'une bonne gestion de son réseau qu'il est préférable de connaître son adresse IP. Pour cela, il est utile de savoir qu'il existe 2 types d'adresses IP :

○ **Les adresses IP dynamiques:**

Ces adresses sont générées automatiquement par le système grâce à la fonction **DHCP** qui est représentée dans la fenêtre des détails à la 4ème ligne.



Elles changent instantanément à chaque redémarrage ou réinitialisation.

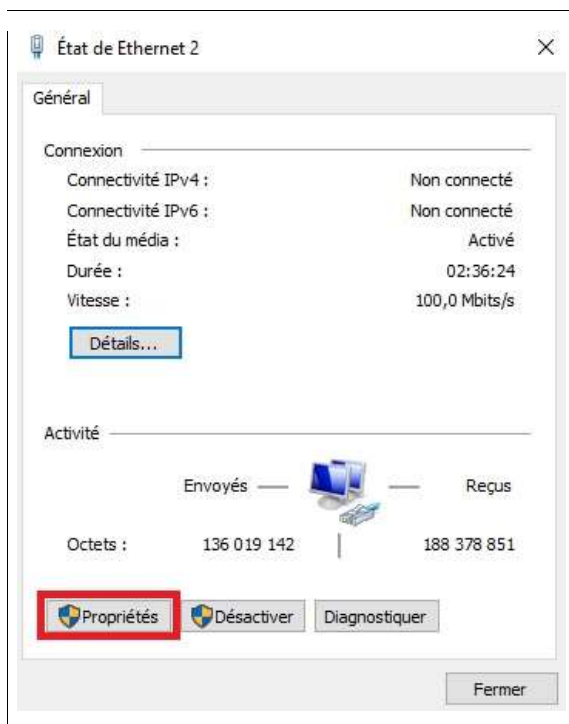
○ **Les adresse IP fixes**

Elles sont définies manuellement par l'utilisateur et permettent d'avoir une adresse IP fixe permanente.

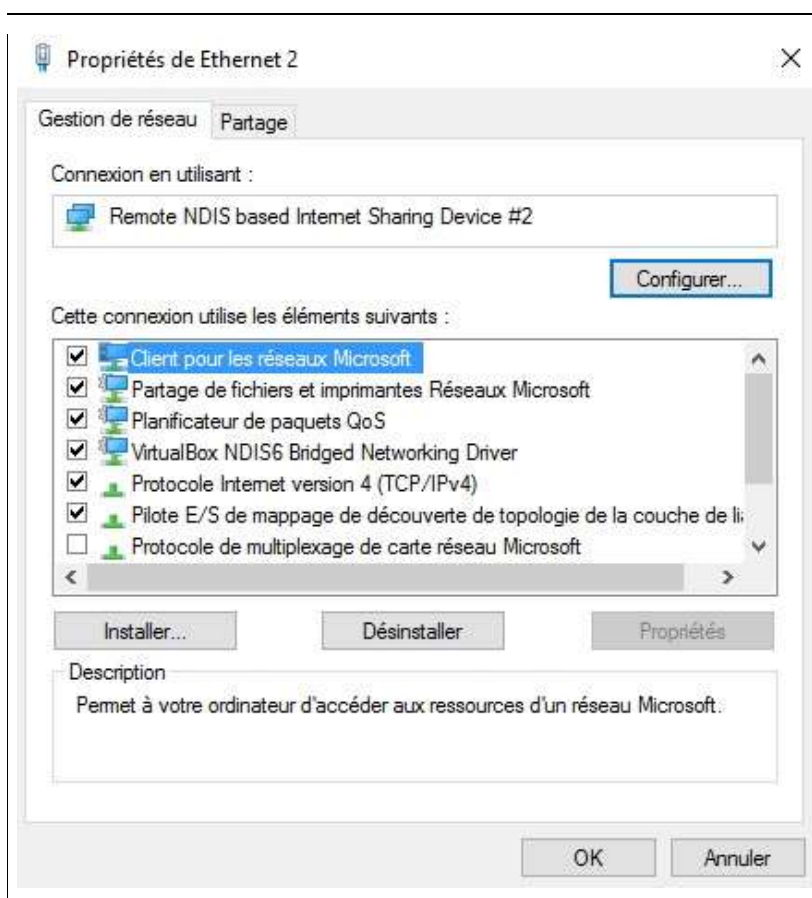
Cela peut être utile dans l'optique d'offrir un accès plus rapide à un serveur ou à un site.

On peut définir une adresse IP fixe en procédant comme suit :

1. Dans la fenêtre des détails de votre réseau, cliquez sur le bouton "**Propriétés**" :



2. Dans la fenêtre qui apparaît, vous avez la liste des éléments et des protocoles utilisés pour votre réseau :

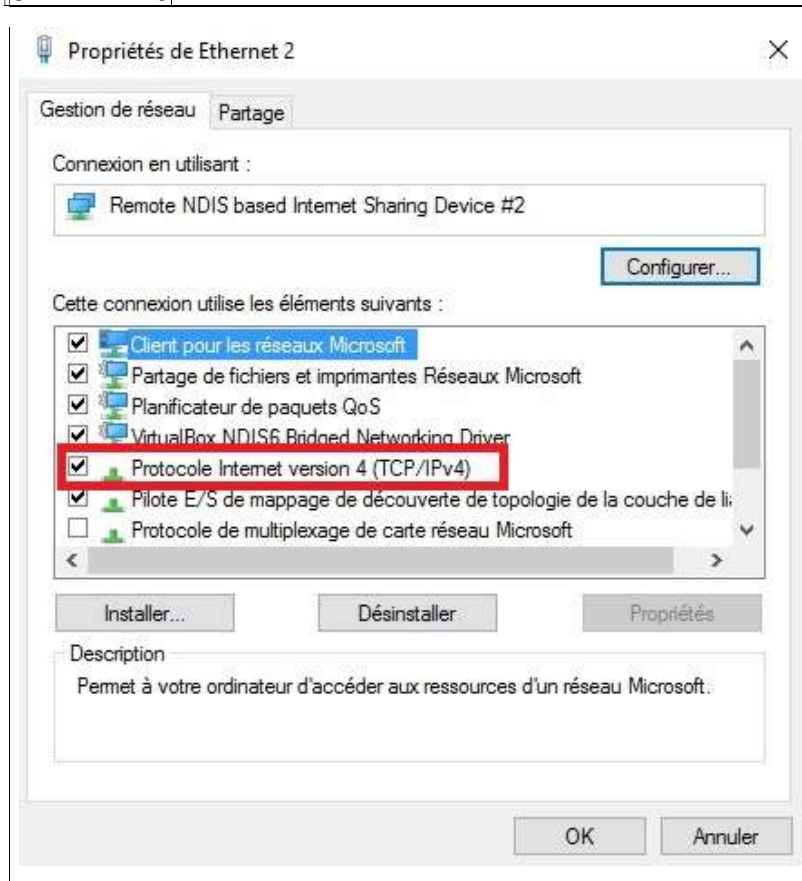


Nous n'allons pas lister tous ces éléments un par un, ce serait trop long et un peu compliqué à suivre. Par contre, la seule notion à laquelle on va s'attaquer est "**protocole**". En fait, un protocole est une série d'étapes à configurer pour créer un lien stable entre les différents éléments d'un réseau.

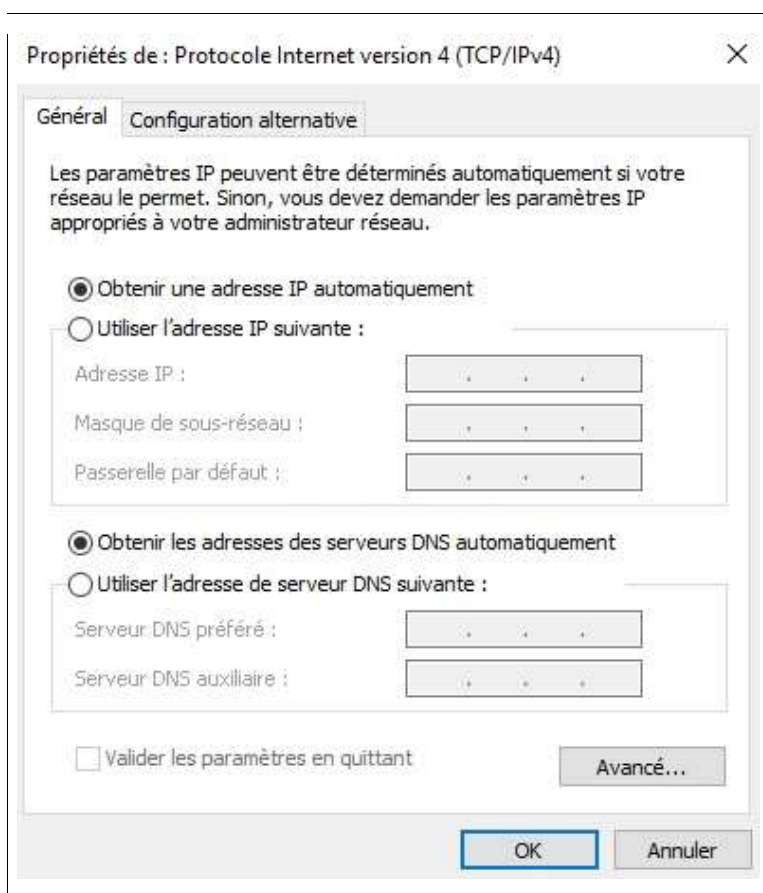
Pour faire simple, ce sont les règles à suivre pour avoir une harmonie parfaite entre les périphériques d'un même réseau.

Encore plus simple, c'est la configuration qu'on doit avoir pour que votre réseau soit fonctionnel (je peux plus simplifier !).

3.Donc, pour accéder à ce protocole et le configurer manuellement, nous allons sélectionner dans la fenêtre des éléments du réseau "**Protocole Internet version (TCP/IPv4)**" :



4. En cliquant sur le bouton "**Propriétés**", vous afficherez l'interface ci-dessous :



Comme vous pouvez le voir les deux options cochées par défaut sont:

“**Obtenir une adresse IP automatiquement**”

et “**Obtenir les adresses des serveurs DNS automatiquement**”.

Ces 2 options font que la fonction **DHCP** est activée (C’est celle qui génère les adresses IP automatiquement comme je l’ai déjà expliqué).

Pour attribuer une adresse IP fixe, il suffit de cocher “**Utiliser l’adresse IP suivante**” puis de saisir l’adresse IP que vous voulez. Nous allons voir ce type de configuration en détail plus loin dans ce cours.

A ce stade, vous devriez être capable de déterminer le type de votre réseau pour mieux configurer votre groupe résidentiel et vos partages. De plus, vous êtes certainement en mesure de connaître votre adresse MAC, votre adresse IP et de savoir si c’est une adresse IP dynamique ou fixe.

Dans ce qui va suivre nous allons suivre les étapes de la création d’un réseau personnel en listant les problèmes les plus fréquents ainsi que la ou les méthodes possibles pour les éviter et les réparer.

Comment créer un réseau local facilement et pas à pas

Il n’est pas du tout difficile de créer un réseau local pour pouvoir bénéficier de tous les avantages que cela apporte comme le partage de fichiers.

C’est plutôt une question d’organisation plus qu’un problème de configuration ou de notions techniques car il ne vous est demandé que de fournir le matériel adéquat qui consiste en :

- **Une carte réseau:**
Qui peut être de 2 types: **filaire** donc qui se connecte grâce à **un câble réseau** ou **sans fil** qui utilise le wifi.
- **Un hub ethernet:**
Cet appareil est essentiel pour mettre 2 ordinateurs en partage Windows.
Le mot "Ethernet" fait référence au réseau local, on peut aussi utiliser le mot "LAN"
Une fois que le matériel requis soit disponible, vient la configuration des paramètres systèmes.

Configuration et création rapide de votre réseau local

Pour commencer, veillez bien à ce que tout la connectique soit branchée. Ce qui consiste à brancher les câbles réseau ou à activer les connexions Wifi en saisissant un mot de passe éventuel.

Ceci étant réglé, voici les étapes à suivre :

Définir le nom de groupe de votre réseau

Le nom de groupe est tout simplement le nom qui va être affiché qui est par défaut **"Workgroup"**.

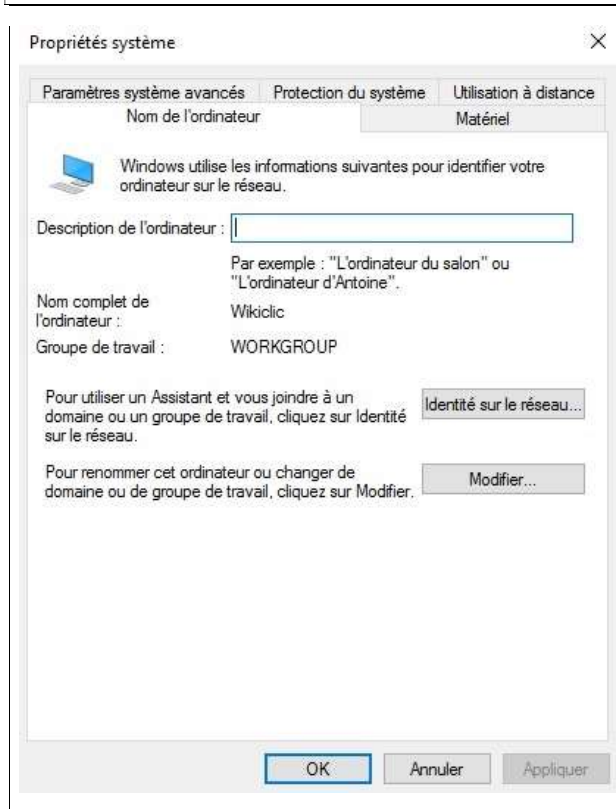
Pour cela, cliquez sur l'icône du poste de travail sur le bureau avec le bouton droit de la souris.

Puis cliquez sur la commande propriétés pour faire apparaître l'interface suivante :

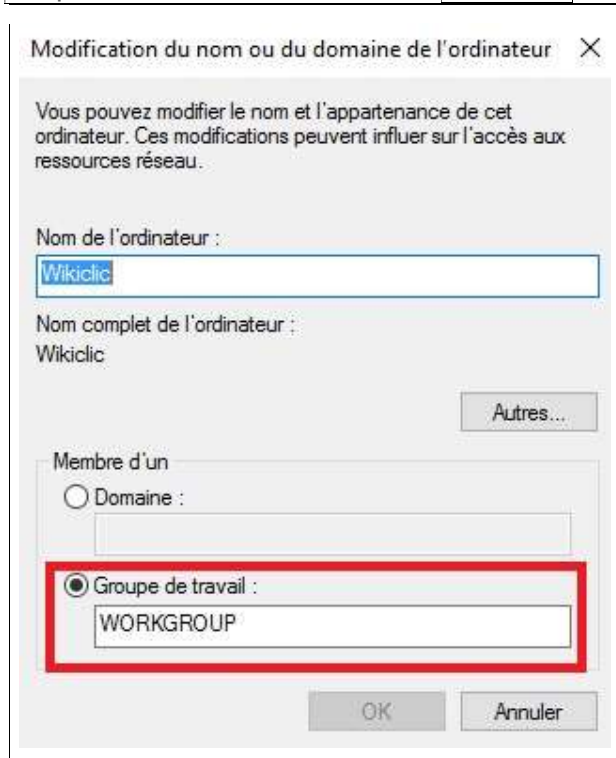
The screenshot shows the Windows 10 'System' settings window. The left sidebar contains links to 'Gestionnaire de périphériques', 'Paramètres d'utilisation à distance', 'Protection du système', and 'Paramètres système avancés'. The main content area is titled 'Informations système générales' and includes sections for 'Édition Windows' (showing 'Windows 10 Professionnel'), 'Système' (showing processor, RAM, and system type), and 'Paramètres de nom d'ordinateur, de domaine et de groupe de travail'. In the 'Paramètres de nom' section, the 'Groupe de travail' is set to 'WORKGROUP'. A red rectangular box highlights the 'Groupe de travail' field, and a red arrow points from the text 'Voici le groupe de travail que vous devez spécifier' to this field. Other fields include 'Nom de l'ordinateur' (Wikiclic), 'Nom complet' (Wikiclic), and 'Description de l'ordinateur'. At the bottom, there is a section for 'Activation de Windows' and a product ID.

Comme vous le voyez, le nom de votre réseau (ou de votre groupe de travail) est affiché sur la fenêtre des propriétés.

Pour le changer, cliquez sur "**Modifier les paramètres**" pour accéder à la fenêtre ci-dessous :



Cliquez ensuite sur le bouton "**Modifier**" :



Il suffit ensuite de saisir le nom que vous voulez puis de valider et de redémarrer votre PC pour que la modification soit réalisée.

Il est possible aussi de changer le nom de votre ordinateur sur le réseau en saisissant le nom dans la zone "**Nom de l'ordinateur**".

Par exemple, si je veux créer un réseau portant le nom de groupe "**Ma maison**" avec mon PC comme étant le serveur principal avec le nom "**chef suprême**", je devrai saisir ces informations de la façon suivante :

Modification du nom ou du domaine de l'ordinateur X

Vous pouvez modifier le nom et l'appartenance de cet ordinateur. Ces modifications peuvent influencer sur l'accès aux ressources réseau.

Nom de l'ordinateur :
Chef suprême

Nom complet de l'ordinateur :
Chef suprême

Autres...

Membre d'un

☐ Domaine :

☒ Groupe de travail :
MA MAISON

OK Annuler

Configurer les adresses IP

Comme nous l'avons déjà vu:

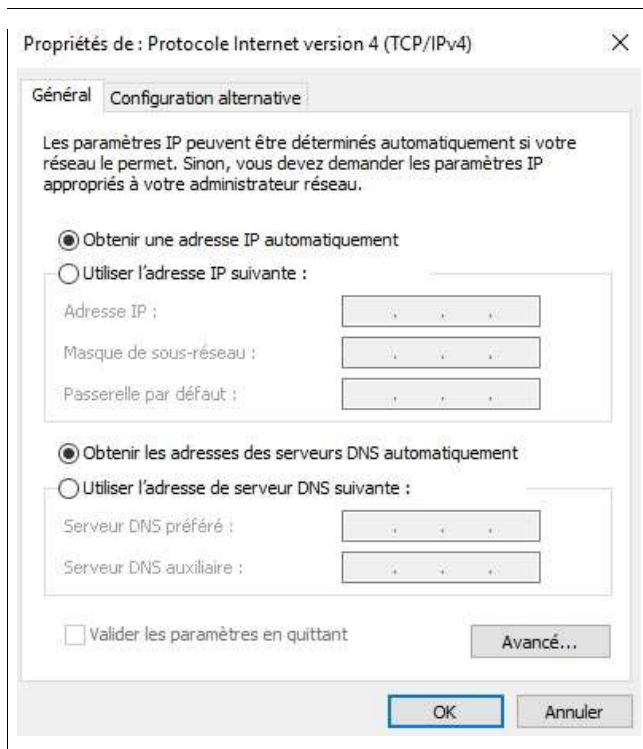
Chaque périphérique sur le réseau a une adresse IP qui peut être dynamique ou fixe.

Pour un réseau domestique, donc avec un nombre de périphériques reliés limité, il est plus pratique de laisser le système gérer cet aspect avec l'option **DHCP**.

Mais, pour éviter des erreurs de partage ou quelques problèmes d'accès, il est préférable de fixer ses propres adresses IP.

Pour cela, procédons comme suit :

Accéder au protocole TCP/IP v4 (comme on l'a expliqué dans la section "**adresse IP fixe**") :



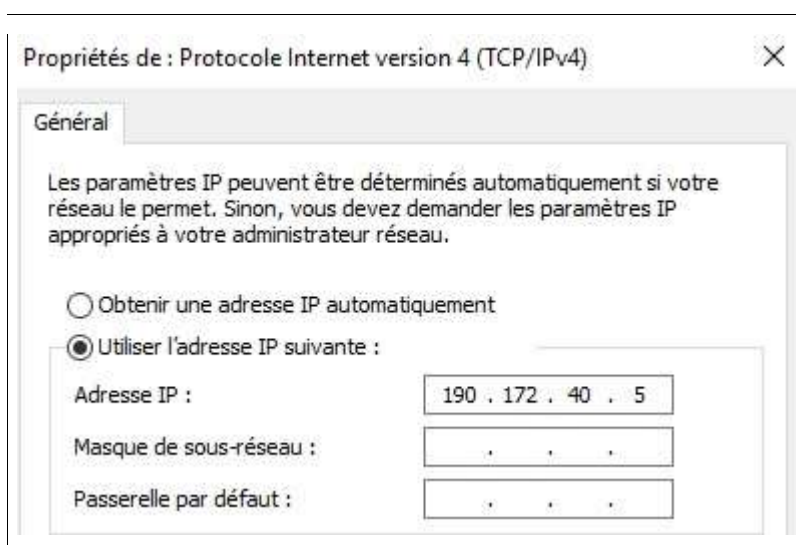
Cocher ensuite "Utiliser l'adresse IP suivante" pour saisir les adresses IP . Ces adresses doivent être choisies selon la méthode suivante:

Si une adresse IP est de la forme xxx.xxx.xxx.xxx avec chaque nombre entre 1 et 255, nous aurons des adresses comme 190.172.40.15

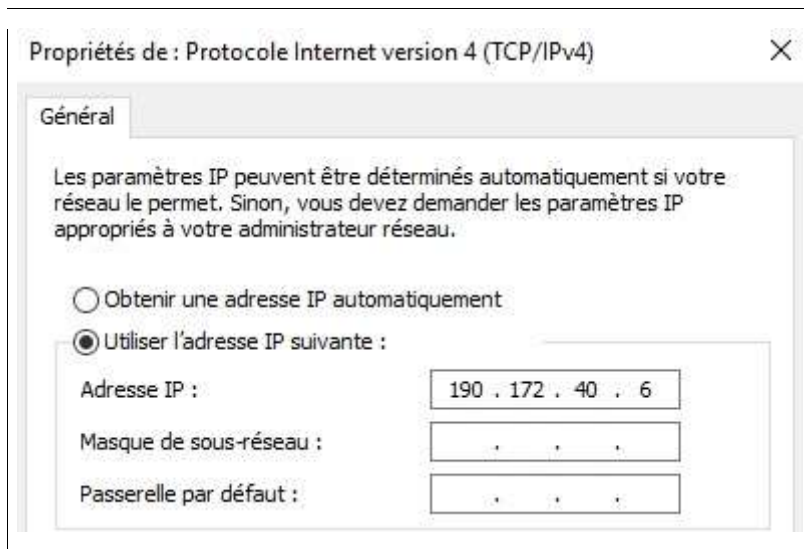
Pour relier plusieurs périphériques au même groupe; il suffit de donner pour chaque IP les mêmes 3 premiers chiffres et changer seulement le dernier.

Par exemple, pour relier 3 ordinateurs au groupe "**Ma maison**" avec des adresses IP fixes j'aurai:

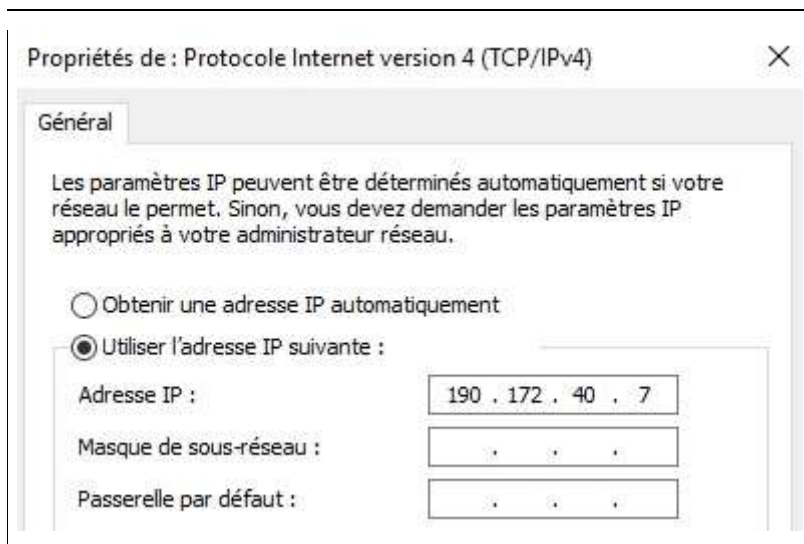
Pour l'ordinateur N°1:



Pour l'ordinateur N°2 :



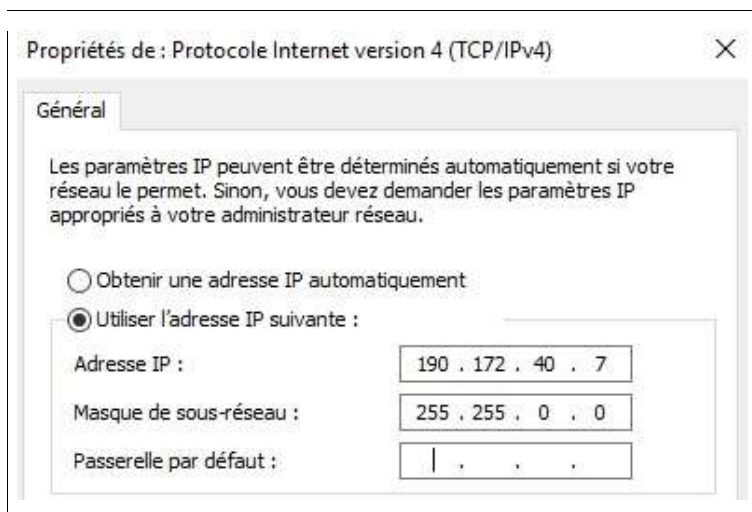
Et pour l'ordinateur N°3:



Et les autres paramètres , à quoi ça sert ?

Et bien, **le masque sous réseau** facilite la communication entre les adresses IP d'un même groupe.

Pour un réseau domestique comme celui qu'on a pour but de créer dans ce cours, il suffit de cliquer dans la zone "Masque de sous réseau" pour qu'il soit généré automatiquement avec la valeur 255.255.0.0 :



Pour votre réseau personnel, tous les autres paramètres peuvent rester vides.

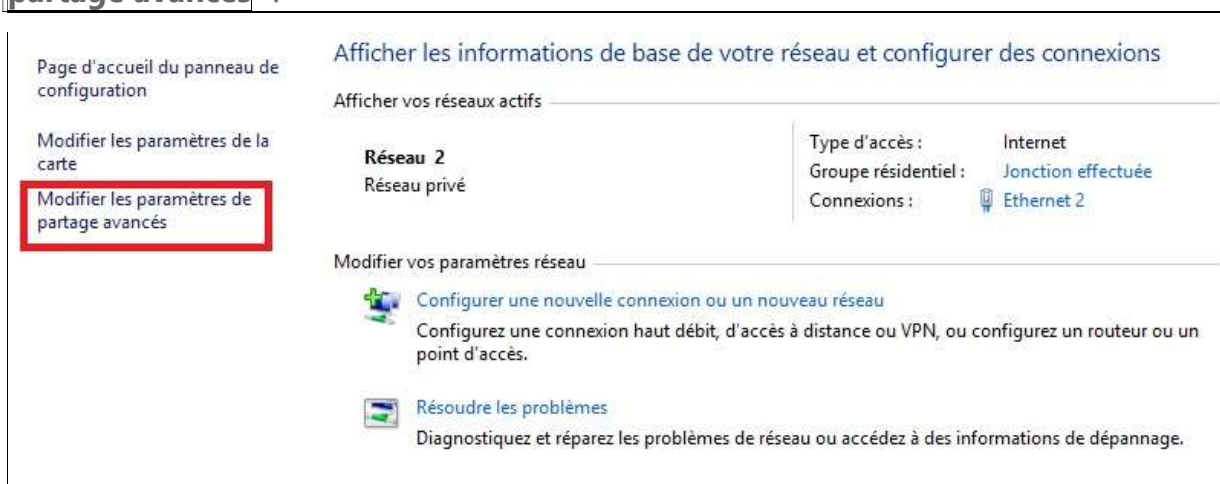
Après le redémarrage des ordinateurs de votre groupe, ils seront tous connectés avec chacun une adresse IP fixe et connue.

En fait, procéder à cette méthode et fixer les IP permet vraiment d'avoir une gestion plus efficace et d'éviter la plupart des problèmes usuels.

En plus de créer un groupe résidentiel pour faciliter le partage de données et la gestion des périphériques et médias.

Les réglages supplémentaires à réaliser, sont surtout nécessaires pour accélérer les accès et éviter des messages concernant les droits d'administrateurs et autres problèmes.

Accédez aux paramètres avancés en cliquant sur l'option "**Modifier les paramètres de partage avancés**" :



Attention, les paramètres à venir sont exclusivement réservés à l'utilisation d'un réseau personnel dont les membres sont dignes de confiance.

Dans l'interface qui s'affiche procédez à l'activation des options suivantes :

- Pour la rubrique "Privé" :

Privé (profil actuel) 

Recherche du réseau

Quand la découverte du réseau est activée, cet ordinateur peut voir les autres ordinateurs et périphériques du réseau, et peut lui-même être vu par les autres ordinateurs du réseau.

- ☒ Activer la découverte de réseau
 - ☒ Activez la configuration automatique des périphériques connectés au réseau.
- ☐ Désactiver la découverte de réseau

Partage de fichiers et d'imprimantes

Lorsque le partage de fichiers et d'imprimantes est activé, toute personne sur le réseau peut accéder aux fichiers et aux imprimantes que vous avez partagés à partir de cet ordinateur.

- ☒ Activer le partage de fichiers et d'imprimantes
- ☐ Désactiver le partage de fichiers et d'imprimantes

Connexions du Groupement résidentiel

En général, Windows gère les connexions aux autres ordinateurs du groupe résidentiel. Mais si vous avez le même compte d'utilisateur et le même mot de passe sur tous vos ordinateurs, vous pouvez configurer le Groupement résidentiel pour utiliser votre compte.

- ☒ Autoriser Windows à gérer les connexions des groupes résidentiels (recommandé)
- ☐ Utiliser les comptes d'utilisateurs et les mots de passe pour se connecter à d'autres ordinateurs

○ Pour la rubrique "Invité" :

Invité ou public 

Recherche du réseau

Quand la découverte du réseau est activée, cet ordinateur peut voir les autres ordinateurs et périphériques du réseau, et peut lui-même être vu par les autres ordinateurs du réseau.


- ☒ Activer la découverte de réseau
- ☐ Désactiver la découverte de réseau

Partage de fichiers et d'imprimantes

Lorsque le partage de fichiers et d'imprimantes est activé, toute personne sur le réseau peut accéder aux fichiers et aux imprimantes que vous avez partagés à partir de cet ordinateur.

- ☒ Activer le partage de fichiers et d'imprimantes
- ☐ Désactiver le partage de fichiers et d'imprimantes

○ Pour la rubrique "Tous les réseaux" :

Tous les réseaux 

Partage de dossiers publics

Lorsque le partage des dossiers Public est activé, les utilisateurs du réseau, y compris les membres du groupe résidentiel, peuvent accéder aux fichiers des dossiers Public.

- ☒ Activer le partage afin que toute personne avec un accès réseau puisse lire et écrire des fichiers dans les dossiers Public
- ☐ Désactiver le partage des dossiers Public (les personnes connectées à cet ordinateur peuvent continuer d'accéder à ces dossiers)

Diffusion de contenu multimédia

Lorsque la diffusion de contenu multimédia est activée, les utilisateurs et périphériques du réseau peuvent accéder à la musique, aux images et aux vidéos sur cet ordinateur. Ce dernier peut également trouver des fichiers multimédias sur le réseau.

[Choisir les options de diffusion de contenu multimédia...](#)

Connexions de partage de fichiers

Windows utilise le chiffrement 128 bits pour mieux protéger les connexions de partage de fichiers. Certains périphériques ne prennent pas en charge le chiffrement 128 bits et doivent utiliser le chiffrement 40 ou 56 bits.

- ☒ Utiliser le chiffrement 128 bits pour mieux protéger les connexions de partage de fichiers (recommandé)
- ☐ Activer le partage de fichiers pour les périphériques qui utilisent le chiffrement 40 ou 56 bits

Partage protégé par mot de passe

Lorsque le partage protégé par mot de passe est activé, seules les personnes disposant d'un compte d'utilisateur et d'un mot de passe sur cet ordinateur peuvent accéder aux fichiers partagés, aux imprimantes connectées à l'ordinateur et aux dossiers publics. Pour donner accès à d'autres personnes, vous devez désactiver le partage protégé par mot de passe.

- ☒ Activer le partage protégé par mot de passe
- ☐ Désactiver le partage protégé par mot de passe

Conclusion

Toutes ces notions, sont bien sûr destinés à débiter en apprenant les notions de bases des réseaux et du partage de fichiers, ce qui vous permettra de mieux gérer vos réseaux domestiques et surtout de dépanner toutes les pannes simples sans avoir à attendre un professionnel ou une connaissance pour résoudre un problème banal.