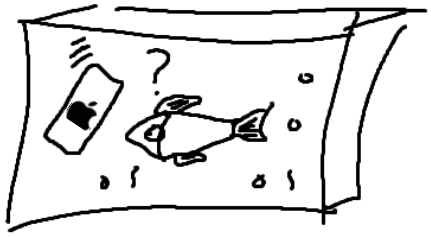
RÉSEAUX, ROUTAGE ET VPN

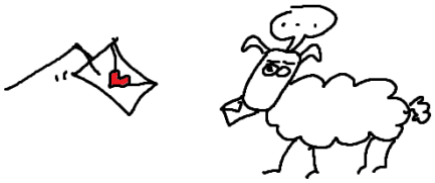
I - Introduction

Le besoin de communiquer induit forcément un besoin de communication entre les machines. Le tout est de :

- se mettre d'accord sur des moyens **compatibles** de communiquer



- faire en sorte que la communication est bien passée



- garantir des mêmes outils pour communiquer, quelque soit l'âge des machines.

On élabore un protocole de communication en fonction des technologies et besoins de l'époque (1974) : le **protocole IP**.

On convient pour commencer de permettre aux machines de se localiser, par le biais d'une adresse, appelée **adresse IP**. Celles que nous manipulons datent de 1979, ce sont les adresses IPv4 (Internet Protocol version 4). La version 6 actuellement en pleine expansion ne sera pas abordée ici ; il faut juste savoir que les deux versions cohabitent aujourd'hui.

La gestion d'adresses se fait par le biais de **cartes réseaux** (Ethernet, Wifi, Bluetooth...) présentes sur toute machine connectée. Tout comme une voiture, une carte réseau a une « immatriculation » qui lui est propre, appelée « adresse MAC » (Media Access Control). Ainsi, chaque machine sera localisable par d'autres de manière unique.

Des machines connectées forment un réseau ; il faut donc prévoir aussi de communiquer entre les réseaux, d'où la notion de **routage**.

II - Adressage IPv4

a) Qu'est-ce qu'une adresse IPv4 ?

Une machine travaille de base sur un système binaire. C'est tout naturellement que son adresse IPv4 est une suite de bits, au nombre de 32 exactement. Pourquoi 32 ? parce que les prévisions de l'époque n'allaient pas au delà de 2^{32} machines inter-connectées (soit de l'ordre de 4 milliards) :

1 0 1 1 0 1 0 1 0 1 1 0 1 0 0 0 1 0 0 0 0 0 1 1 0 1 0 1 1 1 0 1

Nous n'allons pas interconnecter jusqu'à 4 milliards de machines en un seul réseau mondial (bonjour la vie privée), mais plutôt interconnecter des réseaux de machines. Ainsi l'adresse IPv4 comportera une partie « adresse du réseau », les bits de poids forts (les plus à gauche), et une partie « numéro de la machine dans le réseau », les bits restants, de poids faible donc :

1 0 1 1 0 1 0 1 0 1 1 0 1 0 0 0 1 0 0 0 0 0 1 1 0 1 0 1 1 1 0 1

Partie réseau Partie machine

b) Répartition des bits entre réseau et machine

Toute adresse IPv4 est obligatoirement accompagnée d'un filtre, permettant de distinguer les bits « réseau » des bits « machine » : il s'appelle **masque de sous-réseau** (**subnet mask**), et se compose comme l'adresse IPv4 de 32 bits. On demande à l'ordinateur d'appliquer la table de vérité « AND » entre l'adresse IPv4 et le masque. Par exemple un masque réservant 24 bits pour la partie réseau (et donc 8 bits pour la partie machine) aura comme suite de bits :

1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0

On parle alors d'un **masque de 24 bits**.

Il s'en suit l'opération AND suivante :

1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0

& 1 0 1 1 0 1 0 1 0 1 1 0 1 0 0 0 1 0 0 0 0 0 1 1 0 1 0 1 1 1 0 1

1 0 1 1 0 1 0 1 0 1 1 0 1 0 0 0 1 0 0 0 0 0 1 1 **0 0 0 0 0 0 0 0**

Résultat : on obtient l'adresse réseau sans la partie machine, qui elle est réduite de fait à 0.

On distingue 3 grandes catégories de réseaux, appelées **classes (A, B ou C)** selon le masque attribué :

Type de réseau	Masque	Nombre max de machines
réseau de classe A	masque de 8 bits	2^{24} ≈ 16 millions
réseau de classe B	masque de 16 bits	2^{16} ≈ 65 000
réseau de classe C	masque de 24 bits	2^{8} = 256

Le **réseau domestique** par défaut est de classe C (à moins d'avoir une famille *très* nombreuse...).

Un réseau d'entreprise de grande taille sera de classe B ; un fournisseur d'accès Internet attribuera les adresses publiques des routeurs (box) de ses abonnés en classe C.

c) Nomenclature

Pour éviter de se trimbaler les 32 bits en permanence, on les range en 4 octets (4 × 8 bits) puis on convertit chacun des octets en base 10. Par exemple :

1 1 0 0 0 0 0 0 1 0 1 0 1 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 1 0 0 0

11000000 . 10101000 . 00000001 . 00001000

192 . 168 . 0 . 8

De même pour le masque :

masque de 24 bits

1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0

1111111 . 11111111 . 11111111 . 00000000

255 . 255 . 255 . 0

d) Conclusion

Une machine qui se connecte à un réseau suivant le protocole IPv4 sera dotée :

- D'une adresse IPv4 sur 4 octets
- D'un masque de sous-réseau **propre au réseau** auquel la machine se connecte, définissant quelles sont la partie réseau et la partie machine de l'adresse.

Remarque : on peut aussi manuellement définir, pour un réseau, un masque de **23 bits** :

1111111 . 11111111 . 1111111**0** . 00000000

255 255 254.0

On ne travaille plus dans un réseau de classe C, ni même B ou A. L'intérêt ? on peut brancher jusqu'à 256×2 = 512 machines, donc augmenter légèrement la capacité d'une infrastructure, sans pour autant basculer dans une classe trop grosse. 65 000 connexions possibles pour un réseau de classe C, dans un réseau gérant 300 machines par exemple, n'est pas forcément sans risque...

III - Addons

a) DHCP

Dynamic Host Configuration Protocol (DHCP, protocole de configuration dynamique des hôtes) est un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station ou d'une machine, notamment en lui attribuant automatiquement une adresse IP et un masque de sous-réseau. (Wikipédia)

Il y a deux manières d'attribuer une adresse IP à une machine :

- manuellement, directement dans les paramètres IPv4 de la carte réseau
- automatiquement, par le biais d'un service géré par un serveur déjà membre du réseau.

Dans le premier cas, on parle d'**adressage statique**, dans le deuxième d'**adressage dynamique**.

b) DNS

Le **Domain Name System**, généralement abrégé **DNS**, qu'on peut traduire en « système de noms de domaine », est le service informatique distribué utilisé pour traduire les noms de domaine Internet en adresse IP ou autres enregistrements. (Wikipédia)

Le service DNS, géré non pas par un mais par une multitude de serveurs à travers le monde, est défini dans les paramètres IPv4 de la machine (statiquement ou dynamiquement) par **l'adresse IP d'un service DNS existant**. Chaque fournisseur d'accès renseigne sur ses routeurs les IPs de ses propres serveurs DNS ; Google possède son serveur DNS, d'IP 8.8.8.8. Le 9.9.9.9 est un service DNS indépendant, proposé par FDN (French Data Network), FAI associatif depuis 1992.

c) adresses réservées

Pour un masque de 24 bits, on peut prétendre à 256 machines, par exemple de l'adresse 192.168.0.0 à l'adresse 192.168.0.255. Ce n'est pas tout à fait vrai : il y a au moins 2 adresses particulières réservées, pour des questions de **broadcast** (= diffusion) :

- L'adresse **192.168.0.0** est réservée pour définir l'adresse réseau. Les 3 premiers octets étant pour le réseau auquel la machine est connectée, le 192.168.0.0 permet aux appareils (notamment aux routeurs, que nous étudierons après) de définir ce réseau. Ainsi un routeur, connecté d'un côté au **192.168.0** et de l'autre à Internet, définira l'adresse **192.168.0.0** comme « chemin » vers tout appareil branché sur ce réseau. C'est une adresse réservée à la redirection d'informations à l'intérieur du réseau en question.
- L'adresse 192.168.0.255 est aussi réservée, pour du multicast (=multi-diffusion). Lorsqu'un appareil se branche au réseau et qu'il est paramétré en adressage dynamique (par un service DHCP), il envoie dans le réseau une demande d'adressage, ne sachant pas qui lui répondra ; on dit qu'il « crie » une requête à qui l'entendra. L'adresse qu'il utilise alors est le **192.168.0.255**. De même, on peut allumer un ordinateur par le réseau avec la commande créée par la package « SysInternals » nommé WOLCMD (Wake On Line), comme suit :

  wolcmd D43D7EB723EA 192.168.0.255 255.255.255.0 7

  l'exécutable (sur un autre ordinateur du réseau) appelle l'adresse MAC de la carte réseau de l'ordinateur à réveiller en lui précisant l'adresse multicast 192.168.0.255, en attendant qu'une adresse réseau lui soit attribué (le « 7 » après la notification du masque est le numéro de port utilisé par le protocol que suit WOLCMD).

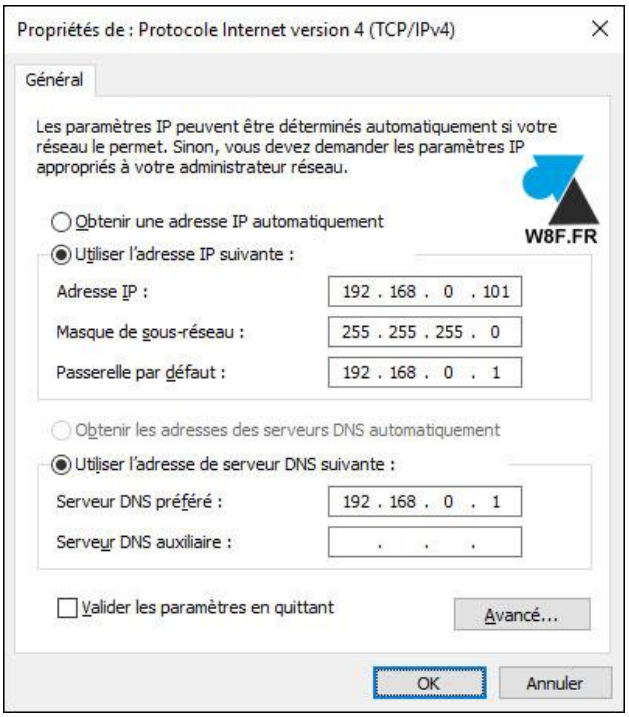
d) Passerelle, passerelle par défaut

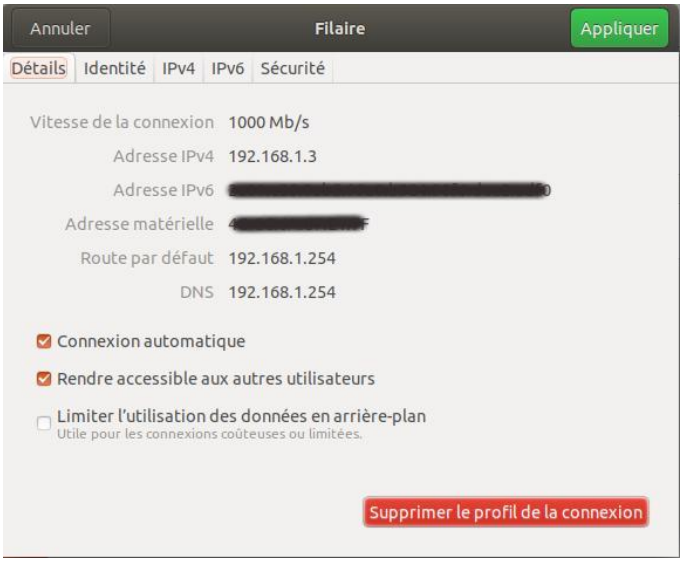
Nous en venons à la partie « interconnexion entre les réseaux ».

Un routeur gère la circulation d'informations entre les différents réseaux auxquels il est connecté, un peu comme les panneaux de ville à un carrefour. Lorsqu'un appareil souhaite communiquer vers une adresse IPv4 qui n'est pas dans le réseau, il doit **savoir qui pourra faire sortir sa requête du réseau**, le routeur en l'occurrence (chez soi, la box par exemple). les paramètres réseau de l'appareil notifient l'adresse IPv4 du routeur qui permet de sortir, le routeur sert donc de **passerelle**. Sans passerelle, tu restes chez toi.

e) Conclusion

Les paramètres réseau IPv4 d'une carte réseau ressemblent généralement à ça :





Sur Windows

Sur Linux

IV - LE ROUTAGE

Comment faire transiter les paquets envoyés à travers plusieurs réseaux ? comment un appareil peut-il faire une requête sur Internet tout en restant privé ? Imaginez une lettre de demande d'allocations familiales. Vous la postez, le facteur fait le reste, mais il ne va pas l'apporte lui-même en mains propres à la secrétaire qui gérera votre demande (elle risque de passer sa vie à le voir H24... !).

De même, le courrier retour reste dans votre boîte aux lettres et ne vous est pas apporté dans votre salle de bain alors que vous prenez tranquillement votre douche... Et même si vous n'êtes pas là, le courrier reste en attente dans votre boite aux lettres.

Tout fonctionne comme la gestion du courrier postal.

a) Le protocole TCP

[SLIDE CI-JOINT : TCP IP NSI]

b) Le protocole UDP

[SLIDE CI-JOINT : UDP]

c) Différence entre TCP et UDP

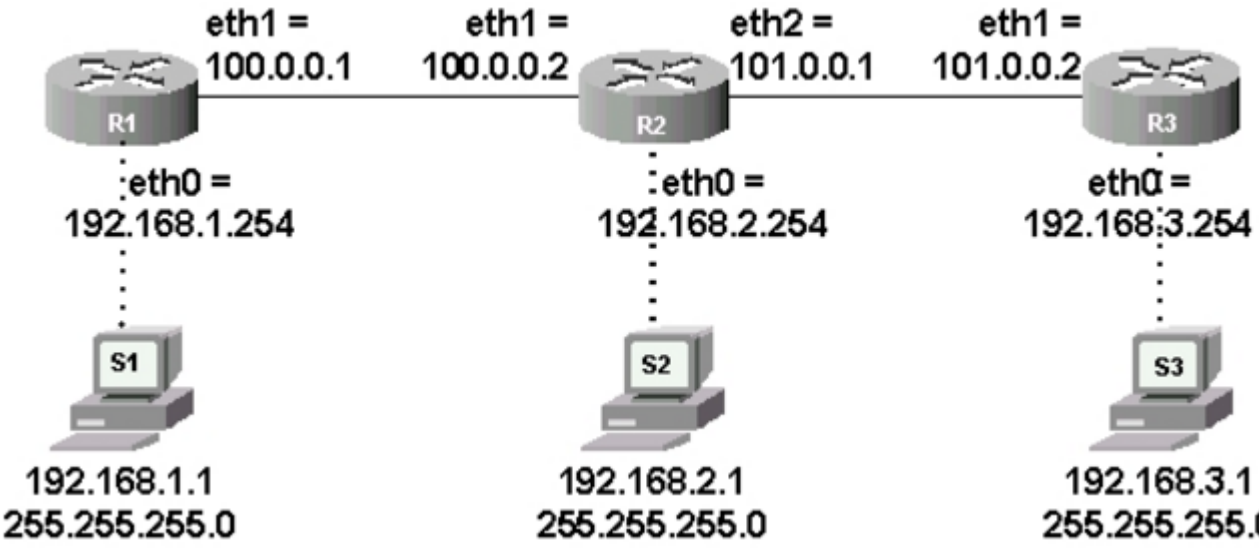
Le TCP garantit l'intégrité du message envoyé ;

L'UDP est utilisé pour des flux directs (streaming, VoIP, DNS...) à courte distance ou ne nécessitant pas le renvoi de paquets perdus. On imagine mal un match de foot ou une conversation téléphonique dont les quelques dixièmes de seconde de coupures éparpillées dans le temps ressurgissent à la fin du match ou de la conversation !

V - TABLES DE ROUTAGE - ADRESSES PUBLIQUES ET PRIVÉES

a) Ce qui se passe à l'intérieur d'un routeur : la table de routage

Prenons un exemple concret, 3 réseaux locaux reliés entre eux :



Chaque routeur possède deux connexions, une pointant vers un réseau local (192.168.X.X) et une autre pointant vers « l'extérieur ». On distingue alors deux types de réseaux, **les réseaux privés et les réseaux publics.** Nous verrons cette différence ultérieurement.

l'ordinateur S1 (192.168.1.1) souhaite communiquer avec S2 (192.168.2.1). Une commande, sur un terminal de S1, lui permet de savoir si son destinataire est joignable : la commande *ping* :

ping 192.168.2.1

la requête part de S1. Comme le 192.168.2.1 n'est pas dans le réseau local de S1, la requête part directement vers la passerelle enregistrée sur S1 : le routeur R1 (192.168.1.254). R1 doit impérativement posséder une base de connaissance pour savoir vers qui faire passer la requête : c'est la table de routage du routeur.

Chaque routeur en possède une, voici son fonctionnement :

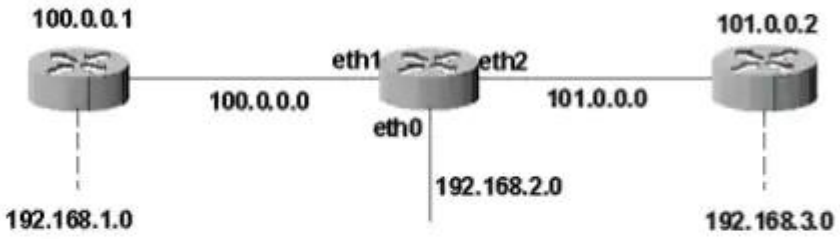
TABLE DE ROUTAGE DE R1

Adresse à joindre	Masque	Passerelle	Interface de R1	Métrique
192.168.1.254	*255.255.255.255*	*127.0.0.1*	*127.0.0.1*	*0*
100.0.0.1	*255.255.255.255*	*127.0.0.1*	*127.0.0.1*	*0*
192.168.1.0	**255.255.255.0**	**192.138.1.254**	**192.168.1.254 (= eth0)**	**0**
100.0.0.0	**255.0.0.0**	**100.0.0.1**	**100.0.0.1 (= eth1)**	**0**
192.168.2.0	255.255.255.0	100.0.0.2	100.0.0.1 (= eth1)	1

On a donc, comme les panneaux de la circulation routière, la route toute indiquée !

De même, le routeur R2 aura la table suivante :

Table de routage



Réseau	Masque	Moyen de l'atteindre	Métrique
192.168.2.0	255.255.255.0	eth0	0
100.0.0.0	255.0.0.0	eth1	0
101.0.0.0	255.0.0.0	eth2	0
192.168.1.0	255.255.255.0	100.0.0.1	1
192.168.3.0	255.255.255.0	101.0.0.2	1

Un routeur = un carrefour = une table de routage indiquant la direction à prendre.

b) De routeur en routeur : simulation sur le logiciel FILIUS

J'utilise personnellement un outil interactif de simulation réseau assez connu : **FILIUS**.

Grâce à Filius, on peut :

- créer un réseau ou un ensemble de réseau
- paramétrer chaque appareil : ordinateurs, routeurs, commutateurs, tables de routage
- simuler des applications : terminal, serveur DHCP, serveur DNS, serveur WEB...
- analyser les paquets qui transitent, examiner les trames TCP lors d'un envoi de paquets (à l'image de Nmap)
- suivre en direct par une animation en couleur le trajet d'une requête à travers les appareils.

Enjoy : c'est par là https://ent2d.ac-bordeaux.fr/disciplines/sti-college/2019/09/25/filius-un-logiciel-de-simulation-de-reseau-simple-et-accessible/

c) Les réseaux privés

Quelle différence entre un réseau privé et un réseau public, puisque les routeurs permettent de passer de l'un à l'autre ? La différence réside dans le **choix de l'adresse du réseau** : dans le fonctionnement global du routage Internet, il y a des plages entières d'adresses définies comme étant **privées**, **qui ne sont pas utilisable sur internet**, par exemple le réseau de votre entreprise ou le réseau domestique. Un réseau privé est un réseau qui utilise les **plages d'adresses IP non accessibles depuis Internet**.

Les adresses IP privées se trouve dans les classes A, B et C.

Voici les plages d'adresse IP privé selon les classes :

– Les adresses privées de la classe A : 10.0.0.0 à 10.255.255.255 (comprend 16 millions d'adresses)
– Les adresses privées de la classe B : 172.16.0.0 à 172.31.255.255 (comprend 65535 adresses)
– Les adresses privées de la classe C : 192.168.0.0 à 192.168.255.255 (comprend 256 adresses)

d) Conclusion

Le routage, essentiellement présent sur les routeurs, permet le bon acheminement de la communication à travers plusieurs réseaux interconnectés. Devant une telle complexité de fonctionnement et de normes, beaucoup de notions sont automatisées, comme le remplissage des tables de routages des routeurs, par communication tacite entre les routeurs voisins les uns des autres. Les différents services comme le DHCP, le DNS, les pare-feu, permettent d'obtenir le minimum viable, comme un réseau domestique. Plus les applications à l'intérieur d'un réseau se multiplieront (serveur WEB, SGDB, serveur FTP, protocoles de sécurisation...), plus il y aura besoin de connaissances afin de rendre ce réseau stable, c'est-à-dire fiable et fonctionnel.

V - les VPN : la base

a) fonctionnement

Un VPN crée une connexion sécurisée entre vous et internet. Lorsque vous vous connectez à internet par l'intermédiaire d'un VPN, l'intégralité de votre trafic de données est envoyée via un tunnel virtuel chiffré. Cela présente de multiples avantages :

- Vous serez plus anonyme sur internet : votre adresse IP et votre localisation ne seront plus visibles par n'importe qui.
- Vous serez plus en sécurité sur internet : le tunnel chiffré vous protégera des pirates et des cybercriminels et votre appareil ne sera plus aussi vulnérable aux attaques.
- Vous serez plus libre sur internet : en utilisant des adresses IP différentes, vous pourrez accéder à des sites web et à des services en ligne qui seraient autrement bloqués.

b) Les VPN proposés sur Internet

Les serveurs VPN offrant leurs services sur Internet sont le plus souvent payants. Et pour cause, pour créer un tunnel VPN il faut passer par un **serveur VPN**. Votre ordinateur se connecte donc à ce serveur, qui renvoie les requêtes vers leurs destinations prévues. Le destinataire (serveur web, ...) ne verra que l'adresse IP du serveur VPN et ne saura rien de qui envoie les requêtes. Cela necessite, pour plusieurs milliers de connexions, du matériel et de la capacité d'accueil...

c) Les VPN locaux

Vous pouvez créer votre propre serveur VPN, ou en acheter un, si votre box ne fait pas déjà office de serveur VPN. Le tout est de situer ce serveur de façon à être directement connecté à Internet, par une adresse IP publique. Ça ne sert donc à rien de prendre un vieil ordinateur ou une Raspberry, d'y installer l'appli qu'il faut et de la brancher sur votre réseau domestique... Puisqu'alors votre box est de fait en pleine ligne de mire !

Certains F.A.I. proposent un **service VPN sur leur box**, comme la Livebox Pro ou la Freebox Revolution (anciennement Freebox Pro). Dans les paramétrages de ladite box, un onglet VPN est à paramétrer. Vous pouvez alors depuis l'extérieur connecter votre ordinateur à cette box ; le résultat est que votre ordinateur, que vous soyez aux Seychelles, aux Baléares si le ciel est dégagé ou en plein Manhattan, sera considéré comme appartenant au réseau local de la box. Ainsi, toutes les requêtes que vous faîtes passeront par la box et **auront officiellement comme point de départ la box** et non votre ordinateur.

d) VPN : 100% sécurisé ?

Les protocoles utilisés (principalement le PPTP, Point-to-Point Tunneling Protocol) datent quand même un p'tit peu (le PPTP est décrit depuis 1999 dans la RFC2637).

Layer 2 Tunneling Protocol (L2TP) et IPsec sont des protocoles inspirés de PPTP et chargés de le remplacer. Cependant, le protocole PPTP continue d'être utilisé car il est implémenté nativement sur les machines Windows depuis Windows 2000. Toute machine Microsoft est donc capable de mettre en place un tunnel PPTP avec une machine distante sans devoir ajouter de mécanisme supplémentaire.

La sécurisation du VPN réside dans les protocoles utilisés pour l'utiliser, notamment en termes d'authentification. Comme tout appareil transmettant des données, tel une borne WiFI, il est toujours possible de percer la sécurité d'un serveur VPN. La réussite dépendra des moyens mis en œuvre : maîtrise et connaissances des failles potentielles, puissance matérielle surtout en terme de rapidité (pour des attaques de force brute par exemple), intention, ciblage... La discussion rentre dans un cadre bien plus général, celui de la cyber-sécurité.

e) Conclusion

La technicité développée dans l'utilisation d'un VPN est de nos jours ordinaire : faire transiter des données de manière sécurisée, d'où l'aspect crypté, anonymisé et exigeant une authentification dans son fonctionnement.

Ce qui définit l'importance du VPN est surtout la pertinence de son usage : accès à des sites que le lieu de résidence ne permet pas, ne pas laisser de traces, simple accès à distance à un réseau local sont diverses raisons parmi tant d'autres d'opter pour une connexion VPN.
