Cours : thème 3 - Question 6

Question 6 : Comment les technologies répondent-elles aux besoins de collaboration ?

Notions abordées :
- réseau et intérêt des réseaux, internet, intranet, extranet ;
- architectures logiques : architecture « pair-à-pair » (*peer to peer*) et « client-serveur » ;
- serveur et services ;
- adressage et configuration réseau (adresse MAC, adresse IP, masque de sous-réseau, etc.) ;
- protocole, pile de protocoles et URL ;
- LAN, WAN, MAN, câble Ethernet, commutateur, routeur, pare-feu, proxy.

1. Introduction

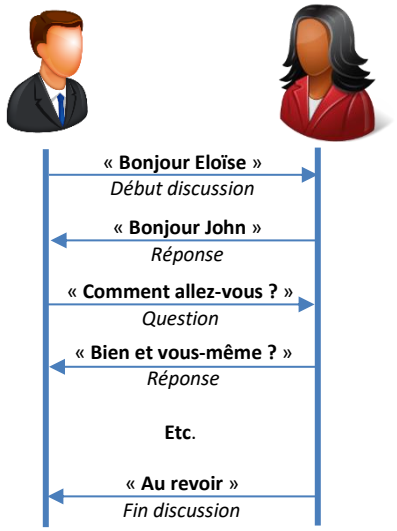
1.1. Réseau et protocole ?

Dans son acception informatique, un réseau est un ensemble d'appareils informatisés interconnectés entre eux par des liens filaires (exemple : câble Ethernet) ou non filaires (exemples : Wifi, Bluetooth).

Le seul fait que les appareils soient reliés entre eux (i.e. en réseau) ne suffit pas pour que ces appareils communiquent entre eux ! Ces liens qui les relient permettent seulement aux appareils de faire circuler de l'information sous forme d'onde ou encore d'électricité. Cependant, il faut que les appareils se comprennent ! C'est alors qu'apparaît la notion de protocole.

Un protocole, au sens informatique, est un format d'échange de données, une façon pour deux appareils de discuter entre eux. Un protocole définit les messages (requêtes et réponses) ainsi que le format des messages échangés par les interlocuteurs.

Exemple de protocole humain



1.2. Intérêt d'un réseau informatique

De manière générale, l'organisation en réseau des ressources informatiques conduit à une amélioration des performances du système d'information en permettant de :

Possibilités offertes	Gains attendus
Communiquer et partager des données	- informations plus facilement accessible, plus vite accessible et/ou toujours disponible ; - conséquences : travail plus efficace, économie de temps, de déplacement.
Partager et centraliser des ressources (données, logiciels, etc.)	- réduction des coûts ; - maintenance et évolution facilitées ; - standardisation, unification, sécurisation, etc.

En bref, les TIC (*Technologies de l'Information et de la Communication*), plus particulièrement dans le cadre d'un réseau, permettent de s'affranchir des contraintes :

D'espace	De temps	De nombre	De type d'information
Ressources humaines, matérielles ou informationnelles pouvant échanger à distance.	Utilisation de ressources disponibles en continue, circulation accélérer de l'information, etc.	Possibilité de diffuser de diffuser de l'information au plus grand nombre (sites web, visioconférence, etc.).	Possibilité de diffuser tous types d'informations : vidéos, textes, images, scènes 3D, etc.

1.4. Typologie des réseaux

On classe communément les réseaux en fonction de leur étendue géographique :
- le **réseau local** (**LAN** : *Local Area Network*) ou réseau local d'entreprise connecte en réseau des équipements d'une même organisation ;
- le **réseau distant** (**WAN** : Wilde Area Network) interconnecte des réseaux locaux entre eux ;
- le **réseau internet** (*Interconnected Networks*) interconnecte, à l'échelle mondiale, un ensemble de LAN et de WAN entre eux. C'est le réseau des réseaux. Il s'agit d'un **MAN** (*Metropolitan Area Network*).

1.5. Internet

L'internet est souvent associé au terme web. Ce dernier vient du « www » (*World Wild Web*). En ce sens, le **web** et internet désignent un ensemble de technologies permettant d'utiliser et de concevoir des services disponibles sur le réseau internet. A cet égard, on peut évoquer :
- les **RFC** (*Request For Comments*) qui sont des documents officiels décrivant des aspects techniques d'internet ;
- le **W3C** (*World Wild Web Consortium*) qui est un organisme à but non lucratif définissant et faisant évoluer de nombreux standards du web (exemple : évolution du langage JavaScript au travers des normes ECMASRIPT ou encore du langage CSS) ;
- les normes IEEE qui définissent divers standards au niveau matériel (exemple : protocole Ethernet) ;
- l'**ICANN** qui est un organisme de régulation chargé de gérer les attributions des adresses IP publiques et des noms de domaine ainsi que de gérer les serveurs DNS racines ;
- l'AFNIC qui est l'organisme rattaché à l'ICANN chargé de réguler les noms de domaine en .fr ;
- la **loi informatique et liberté de 1978** qui pose, à l'échelle française, des principes juridiques en outre en matière d'utilisation et de protection des données personnelles.

1.6. Intranet et extranet

De même que l'on parle de site internet, on parle de site intranet et de site extranet, ou plus simplement d'intranet et d'extranet :
- un **extranet** consiste en un ensemble de ressources web mises à disposition par une organisation auprès d'un public extérieur. Un extranet fournit ces ressources typiquement en accès restreint, réservé. L'accès aux ressources nécessite normalement une authentification (identifiant + mot de passe) ;
- un **intranet** consiste en un ensemble de ressources web mises à disposition au sein d'une organisation et à destination des utilisateurs du réseau interne de l'organisation. En général, il nécessite également une authentification.
- intranet et extranet utilisent les technologies d'internet, à savoir les technologies web.

2. Architectures et infrastructures réseaux

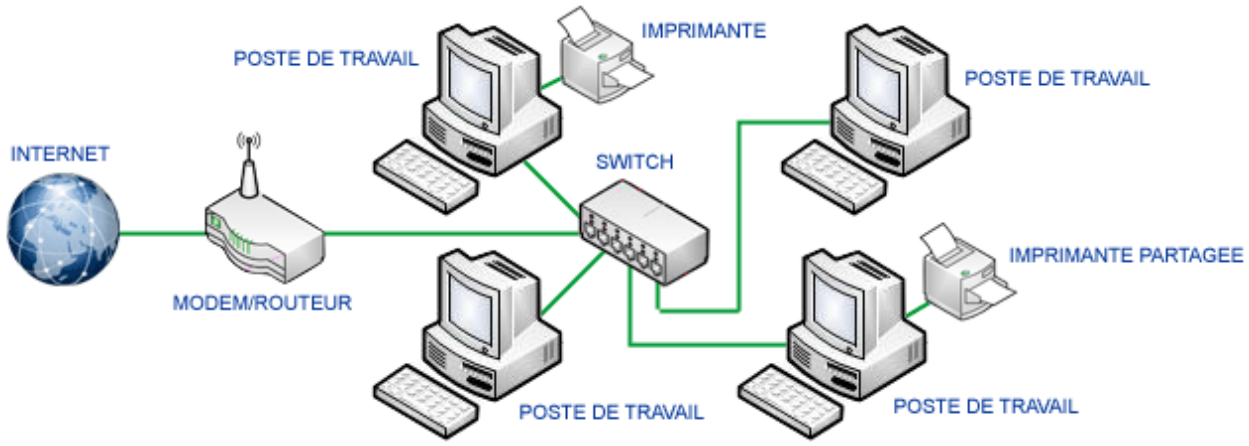
2.2. Matériels réseaux

Pour se connecter au réseau local ou encore au réseau internet, les équipements sont en outre reliés physiquement, à savoir matériellement. Plus encore, les équipements en question sont classiquement interconnectés au moyen d'équipements intermédiaires. A ce titre, le réseau fait appel à différents matériels :
- des **liens filaire (exemple : câble Ethernet) ou non filaires (exemples : Wifi, Bluetooth, etc.)** reliant les équipements entre eux ;
- un ou plusieurs **commutateurs** (***switch***) permettant aux équipements de communiquer entre eux sur le réseau local ;
- un ou plusieurs **routeurs** permettant de connecter les équipements au réseau internet et plus généralement d'interconnecter des réseaux entre eux ;
- un ou plusieurs **pare-feux** permettant de sécuriser le réseau local en empêchant certaines formes d'intrusions. On notera qu'un pare-feu peut être matériel ou logiciel. Un routeur intègre en général des fonctionnalités lui permettant de tenir le rôle de pare-feu ;
- un ou plusieurs proxys assurant entre autres choses des fonctionnalités de gestion de cache ou encore de filtrage.

Commutateur (*switch*)		**Routeur**	
Equipement intermédiaire pour connecter entre eux des équipements sur le réseau local		Equipement intermédiaire pour connecter des réseaux entre eux, en outre pour connecter au réseau internet le réseau local et ses équipements.	
Symbole :		Symbole :	

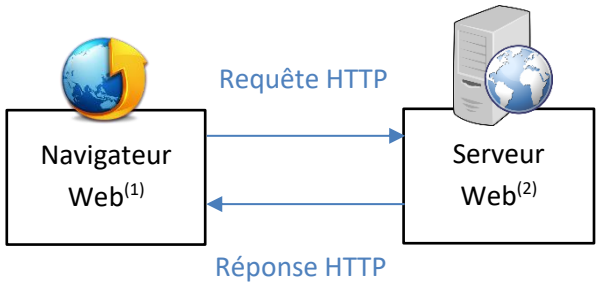
On notera qu'on utilise souvent les expressions **infrastructures informatiques** et **parc informatique** pour qualifier l'ensemble des éléments matériels du système informatique d'une organisation : matériels réseau, ordinateurs, serveurs, etc.

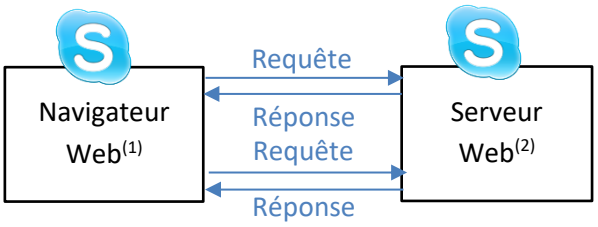
Exemple d'architecture réseau :



2.3. Architectures logiques

On parle d'architecture logique dans la mesure où il ne s'agit plus d'architecture uniquement matérielle mais d'architecture matérielle et logicielle. La communication en réseau est toujours assurée à la fois par des matériels et des logiciels. Et l'on peut distinguer principalement les architectures suivantes :

Architecture client-serveur	
Architecture au travers de laquelle le logiciel joue le rôle du client (**logiciel client** ou **partie client**) et un autre logiciel joue le rôle du serveur (**logiciel serveur** ou **partie serveur**). Le client envoie les requêtes au serveur et le serveur lui retourne les réponses. Le serveur fournit le service. Le client consomme le service. Exemples : - navigateur (client) et serveur web (serveur) ; - explorateur de fichier (client) et serveur de fichier (serveur) ; - boîte mail (client) et serveur de messagerie (serveur) ; - etc.	*Principe d'une architecture client/serveur :*  (1) Chrome, Mozilla, etc. (2) Apache, Tomcat, JBoss, etc.

Architecture paire-à-paire (P2P, *per-to-per*)	
Architecture au travers de laquelle le logiciel joue à la fois le rôle du client et celui du serveur. Autrement dit, tantôt le logiciel envoie des requêtes et reçoit des réponses, tantôt il reçoit les requêtes et envoie les réponses. Exemples : Skype (en 2017 encore), certains logiciels de téléchargement, etc.	*Principe d'une architecture per-to-per :* 

On ajoutera que le **serveur physique** est l'équipement (matériel) sur lequel se trouve le ou les logiciels serveurs. Le **client physique** est l'équipement (matériel) sur lequel se trouve le ou les logiciels clients.

2.4. Sécurité

Un système d'information est d'autant plus vulnérable qu'il est en réseau. En effet, en mettant à disposition des ressources au travers d'un réseau, ou en le connectant à internet, on peut craindre des vulnérabilités (exemple : intrusion dans le système d'information avec piratage de données sensibles, perte de connexion internet perturbant voire empêchant le travail, etc.).

Dès lors, en vue de prévenir ces risques et vulnérabilités, il convient de mettre en place des mesures proportionnées au regard de leur coût, de la probabilité de survenance des dysfonctionnements et de la gravité de ces derniers. A cet égard, on retient les critères de sécurité suivants :
- **confidentialité** : l'information ne doit être divulguée qu'aux seules personnes autorisées. On définit

typiquement des autorisations par profil d'utilisateurs. On parle de gestion de droits d'accès par rôle (RBAC) ou par utilisateur (DBAC) ;
- **intégrité** : l'information doit être préservée telle que transmise ou encore enregistrée. Elle ne doit pas être altérée au fil du temps, que l'altération soit volontaire ou accidentelle. Cela implique des choix en termes de sauvegardes (duplication/réplication ou encore systèmes de tolérance aux pannes) et de formats de stockage (formats durables) ;
- **disponibilité** : l'information doit être au maximum disponible, sans interruption, à savoir qu'on doit autant que faire se peut avoir tout le temps accès à l'information. Cela implique de mettre en place des infrastructures logicielles et/ou matérielles adaptées et proportionnées en matière de coût (redondance, plan de continuité et de reprise d'activité, systèmes de tolérance aux pannes, etc.). On parle de taux ou de degré de disponibilité. 99% de disponibilité signifie par exemple : disponible en moyenne 365x99%≈361 jours/an ;
- **imputabilité** : les ajouts, modifications, suppressions ou plus généralement les actions effectuées doivent être tracées et il doit être possible d'identifier avec certitude et exactitude l'auteur de chaque action. Il s'agit d'une forme de traçabilité de l'information. On doit éviter la répudiation, à savoir il ne doit pas être possible pour l'auteur de l'action de nier que c'est bien lui qui l'a effectuée.

3. Adressage IP et adressage réticulaire

L'adressage permet de répondre à la question « qui ? », sous-entendu l'adressage consiste en un ensemble de techniques permettant d'identifier les équipements informatiques. De fait, si un équipement doit s'adresser à un autre, il faut avant toute chose savoir à qui l'on s'adresse.

3.1. Adressage physique et logique

On qualifie d'hôte, sous-entendu hôte du réseau, tout équipement informatisé connecté au réseau considéré. Sur le réseau local, on peut considérer deux façons d'identifier un hôte, cette identification permettant de savoir à qui l'on s'adresse :

Adresse MAC	
Description : l'adresse MAC est l'adresse physique du matériel en ce qu'elle permet d'identifier un matériel informatisé de manière unique dans le monde. Autrement dit, deux matériels informatiques (téléphone, ordinateur, badgeuse, etc.) ne peuvent avoir même adresse MAC. **Exemple** : 12:A3:5F:EC:FF:04	**Format** : X:X:X:X:X:X X peut prendre les valeurs 00 à FF (en hexadécimal), soit 0 à 255 en décimal. Les 3 premiers octets identifient le fabriquant, les 3 suivants le matériel du fabriquant, soit finalement 6 octets. **Taille :** 6 octets, soit 6 x 8 = 48 bits **Nombre de possibilités :** 2^{48} adresses
Adresse IP	
Description : l'adresse IP est l'adresse logique du matériel en ce qu'elle permet uniquement d'identifier le matériel informatisé sur le réseau considéré. L'adresse IP est unique sur le réseau local considéré mais des postes sur des réseaux distincts peuvent avoir même adresse IP. **Exemple** : 192.168.1.2	**Format** : X.X.X.X X peut prendre les valeurs 0 à 255. **Taille :** 4 octets, soit 4 x 8 = 32 bits **Nombre de possibilités :** 2^{32}* adresses **Exemple :** 192.168.1.2 * 2^{32} = 4 294 967 296, ce qui est finalement assez faible.

Il convient par ailleurs de préciser qu'une adresse IP admet une représentation binaire, à savoir une représentation constituée de 0 (faux) et de 1 (vrai). On appelle un octet une succession et 8 bits, un bit étant un 0 ou un 1. Une adresse IP est constituée de 4 octets.

Bit n°	8	7	6	5	4	3	2	1
Valeur associée	2^7=128	2^6=64	2^5=32	2^4=16	2^3=8	2^2=4	2^1=2	2^0=1

Représentation binaire de l'adresse IP « 192.168.1.13 » : 11000000.10101000.00000001.00001101

$$192 = \mathbf{1}\times128 + \mathbf{1}\times64 + \mathbf{0}\times32 + \mathbf{0}\times16 + \mathbf{0}\times8 + \mathbf{0}\times4 + \mathbf{0}\times2 + \mathbf{0}\times1$$
$$168 = \mathbf{1}\times128 + \mathbf{0}\times64 + \mathbf{1}\times32 + \mathbf{0}\times16 + \mathbf{1}\times8 + \mathbf{0}\times4 + \mathbf{0}\times2 + \mathbf{0}\times1$$
$$1 = \mathbf{0}\times128 + \mathbf{0}\times64 + \mathbf{0}\times32 + \mathbf{0}\times16 + \mathbf{0}\times8 + \mathbf{0}\times4 + \mathbf{0}\times2 + \mathbf{1}\times1$$
$$13 = \mathbf{0}\times128 + \mathbf{0}\times64 + \mathbf{0}\times32 + \mathbf{0}\times16 + \mathbf{1}\times8 + \mathbf{1}\times4 + \mathbf{0}\times2 + \mathbf{1}\times1$$

3.2. Classes d'adresses IP, masque de sous-réseau, adresse du réseau et adresse de broadcast

Le **masque de sous-réseau** permet d'établir à quel réseau appartient une adresse IP. A ce sujet, nous traiterons le cas le plus simple : les masques de sous-réseau des réseaux de classe A, B et C.

En fait, une adresse IP est constituée de deux parties :
- la **partie réseau** : elle est constituée des bits communs à l'adresse IP et au masque de sous-réseau ;
- la **partie hôte** : elle est constituée de tous les bits restants.

L'adresse IP du réseau a la particularité suivante :
- sa partie réseau est la même que celle de toutes les adresse IP du réseau ;
- sa partie hôte est constituée uniquement de 0 (soit 0 en décimal).

L'**adresse IP de *broadcast*** permet de délivrer un message à tous les hôtes du réseau. Chaque réseau en possède une et une seule. Lorsqu'un hôte émet un message à destination de cette adresse IP, son message est diffusé par le commutateur à tous les hôtes du réseau, sauf à l'émetteur lui-même. Par ailleurs, l'adresse IP de *broadcast* n'est pas routable. Elle a la particularité suivante :
- sa partie réseau est la même que celle de toutes les adresse IP du réseau ;
- sa partie hôte est constituée uniquement de 1 (soit 255 en décimal).

	Classe A	**Classe B**	**Classe C**
Masque	255.0.0.0 (abrégé /8)	255.255.0.0 (abrégé /16)	255.0.0.0 (abrégé /24)
Exemple d'IP	10.21.22.23	10.21.22.23	10.21.22.23
Partie réseau	10	10.21	10.21.22
Partie hôte	21.22.23	22.23	23
IP du réseau	10.0.0.0	10.21.0.0	10.21.22.0
IP de broadcast	10.255.255.255	10.21.255.255	10. 21. 22.255
IP adressables*	2^{24}-2 = 16 777 214	2^{16}-2 = 65 534	2^8-2 = 254

** IP adressables : nombre d'adresses IP pouvant être attribuées à des postes sur le réseau.*

Important ! Communément, afin de signifier qu'un poste a pour adresse IP 10.21.22.23 et pour masque de sous-réseau 255.0.0.0, on écrite 10.21.22.23/8. Pareillement, pour les masques de sous-réseau /16 et /24, on écrit respectivement 10.21.22.23/16 et 10.21.22.23/24.

3.3. Adresses IP de bouclage

Les **adresses IP de bouclage** redirigent l'hôte du réseau (votre poste informatique par exemple) vers lui-même. On parle de ***localhost*** ou encore d'**adresses IP de *loopback***. Les adresses IP de *loopback* sont les suivantes : 127.0.0.1 à 127.255.255.255 (masque : 255.0.0.0).

Elles permettent en outre à un poste informatique de s'interroger lui-même, ce qui permet de simuler un comportement d'architecture client-serveur. En effet, jouant le rôle de client, le poste informatique peut interroger le serveur *localhost*, lequel n'est autre que le poste informatique lui-même jouant à la fois le rôle de client et de serveur. Tout se passe comme si l'on interrogeait un serveur (envoi d'une requête) et que celui-ci nous répondait (envoi d'une réponse). En fait, la requête et la réponse ne sont alors jamais « sorties » du poste informatique.

3.4. Adresses IP privées/publiques

Adresse IP publique	Adresse IP privée
Les adresses IP publiques sont uniques et permettent d'accéder à un matériel informatique au-delà du réseau local, à savoir sur internet. On parle d'adresse IP routable*. * Une adresse IP est dite routable si elle peut être utilisée telle quelle au travers du réseau internet pour identifier un hôte unique du réseau internet. Ces adresses IP sont délivrées par l'intermédiaire de l'ICANN, typiquement aux serveurs ou encore aux box.	Les adresses IP privées sont propres au réseau local. Elles ne sont jamais visibles en-dehors du réseau local et ne peuvent être utilisées que sur celui-ci. On parle d'adresse IP non routable. Il existe 3 plages d'adresses IP privées : - **classe A** : Plage : 10.0.0.0 - 10.255.255.255 Masque : 255.0.0.0 (souvent abrégé /8) - **classe B** : Plage : 172.16.0.0 - 172.31.255.255 Masque : 255.255.0.0 (souvent abrégé /16) - **classe C** : Plage : 192.168.0.0 - 192.168.255.255 Masque : 255.255.255.0 (souvent abrégé /24)

Important ! Concrètement, lorsqu'un routeur redirige une requête à destination d'internet émise par un hôte du réseau local, disposant typiquement d'une adresse IP privée, le routeur connecté à internet remplace l'adresse IP de l'hôte du réseau par sa propre adresse IP publique. Ainsi, l'hôte du réseau local est invisible sur internet. Seul le routeur connecté à internet est visible sur internet. Ce procédé fait appel à deux procédés que nous n'étudierons pas : l'*IP masquerade* et le *port forwarding*. On remarquera en revanche :

- que cette substitution d'adresse IP offre un avantage en matière de sécurité, l'invisibilité des hôtes du réseau local et l'impossibilité d'accéder directement à ces derniers ;
- que cette substitution permet à des hôtes de réseaux locaux distincts d'avoir la même adresse IP, ce sans quoi toutes les adresses IP disponibles (soit 2^{32} = 4 294 967 296) seraient déjà toutes utilisées.

3.5. Routeur et passerelle

Revenons-en encore à nos fameux routeurs. Comme nous le disions, un routeur permet d'interconnecter des réseaux entre eux et, en particulier, permet de connecter le réseau local à internet. Autrement dit, **un routeur est connecté *a minima* à deux réseaux distincts** (par exemple au réseau local et à internet).

Or, pour discuter sur un réseau, il faut une configuration IP, soit une adresse IP et le masque du réseau en question. Ainsi, **le routeur possède au minimum deux adresses IP**, chacune d'entre elles lui permettant de communiquer sur un réseau différent.

Qu'est-ce qu'une **passerelle** et quel rapport avec le routeur ? Bien, comme nous l'évoquions ci-dessus, un poste informatique sur le réseau local possède typiquement une adresse IP privée lui permettant uniquement de communiquer avec les équipements du réseau local via un commutateur. Le problème, c'est que l'on peut souhaiter communiquer avec des équipements extérieurs, par exemple un serveur web pour accéder à un site internet. Dès lors, il nous faut connaître l'équipement qui pourra rediriger notre requête vers l'extérieur si bien que son adresse IP sur le réseau local est appelée la passerelle en ce qu'elle permet de communiquer avec l'extérieur. Cette adresse IP est en général l'une des adresses IP du routeur, à savoir l'adresse IP du routeur qui se trouve sur le même réseau.

3.6. Adresse IP fixe, statique ou dynamique

Adresse IP fixe	Adresse IP statique	Adresse IP dynamique
L'adresse IP est configurée manuellement sur le poste informatique. Le poste a ainsi toujours la même adresse IP. **Inconvénient :** nécessité de configurer chacun des postes manuellement (maintenance compliquée).	L'adresse IP du poste est récupérée auprès d'un serveur DHCP. Le serveur alloue toujours la même IP au poste. **Avantage :** - la configuration de l'IP est centralisée sur le serveur DHCP ; - cette forme d'adresse IP est parfaite pour les serveurs et autres matériels dont l'adresse IP dont on doit connaître l'adresse IP à tout moment.	L'adresse IP du poste est récupérée auprès d'un serveur DHCP. Le poste reçoit une adresse IP sur le réseau pouvant variée dans le temps. **Avantage :** - la configuration de l'IP est centralisée sur le serveur DHCP ; - cette forme d'IP est parfaite pour les appareils informatiques quelconques, dont la variation d'IP est sans importance.

3.7. URL

Une **URL** (*Unified Resource Locator*) permet d'identifier une ressource sur internet et d'y accéder via un navigateur web. Elle revêt la forme suivante : **https://fr.wikipedia.org:80/wiki/Uniform_Resource_Locator**.

https	Il s'agit du protocole utilisé.
://	Il s'agit d'un simple séparateur.
fr.wikipedia.org	Il s'agit du nom de domaine. On notera que « org » est un nom de domaine. « wikipedia.org » est un sous-domaine du domaine « org », « fr.wikipedia.org » est un sous-domaine du domaine « wikipedia.org ». En fait, les **noms de domaines sont hiérarchisés**. « org » est ce qu'on appelle un **nom de domaine racine**, au même titre que « fr » ou « com ».
:80	Il s'agit du port utilisé. Ce :80 est bien souvent facultatif puisque c'est le port utilisé par défaut par le navigateur et c'est le port par défaut des serveurs web dans la mesure le port 80 correspond au protocole HTTP.
/wiki/Uniform_Resource_Locator	Il s'agit de l'**URI** (*Unified Resource Identifier*). Comme son nom l'indique, l'URI permet d'identifier, sur un serveur donné, la ressource à laquelle on souhaite accéder.

3.8. Nom de domaine

Un **nom de domaine** est un nom qu'on peut obtenir auprès de l'ICANN typiquement par l'intermédiaire d'un hébergeur web (exemple : OVH, Gandhi, etc.). On peut associer un nom de domaine à un serveur. Dès lors, plutôt que d'interroger (envoi d'une requête) un serveur au moyen de son adresse IP, l'on pourra le faire au moyen de son nom de domaine. On notera qu'il est tout à fait possible d'associer plusieurs noms de domaine à un même serveur. La **traduction** (***translation***) d'un nom de domaine vers son adresse IP est assurée par les **serveurs DNS (*Domain Name System*)** au moyen du **protocole DNS**.

4. Services et protocoles

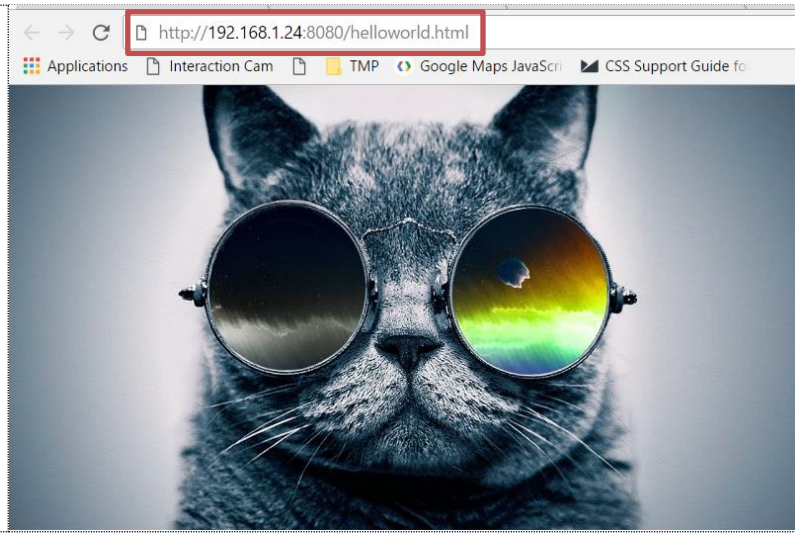
4.1. Ports

Si l'adresse IP permet d'identifier un poste informatique sur le réseau, le **couple adresse IP + port** permet d'identifier un service d'un poste informatique donné. C'est en quelque sorte une « porte d'entrée » qui permet d'accéder à l'un des services d'un poste informatique.

Exemple :

Il peut s'agir par exemple d'accéder à un serveur web. Le serveur physique a une adresse IP, mettons 192.168.1.24. Le serveur logiciel, à savoir le serveur web (exemple : *Wamp Server*), utilise un port, mettons le port 8080. Sur le réseau local, on peut alors accéder au serveur web grâce à l'URL http://192.168.1.24:8080.

Sur le serveur web, on peut créer une ressource, mettons une page web « helloworld.html ». Ça y est ! Sur le réseau local, on peut accéder à la page web grâce à l'URL : http://192.168.1.24:8080/helloworld.html.



Un ordinateur a **65536 ports attribuables**. Autrement dit, un ordinateur peut mettre à disposition jusqu'à 65536 services.

Quant au protocole HTTP, il est « normalement » associé au port 80. Du moins, c'est le port standard, par défaut. Ainsi, un serveur web, *WampServer* dans l'exemple ci-dessus, est typiquement démarré sur le port 80. On dit qu'il écoute sur le port 80. Et on dit qu'il écoute dans la mesure où il attend de recevoir des requêtes pour y répondre. Rien n'empêche toutefois, comme dans l'exemple ci-dessus, de démarrer le serveur web sur un autre port (en l'occurrence le port 8080) !

4.2. Pile de protocole

Nous ne cessons d'évoquer le terme protocole. Comprenez qu'en matière de réseau, de ce fait en matière de communication entre appareils informatisés, les protocoles interviennent à tous les niveaux.

En effet, les appareils ont besoin de communiquer pour diverses raisons. Aussi, les protocoles répondent à diverses problématiques de communication.

Effectivement, on catégorise les protocoles par niveaux. On parle d'ailleurs plus volontiers de **couches** que de niveaux. On appelle ces couches le **modèle TCP/IP** ou encore la **pile de protocoles TCP/IP** :
- **accès réseau** : c'est la couche la plus basse, le plus proche du matériel. Elle englobe tous les protocoles permettant la communication directe entre matériels informatisés par câble ou encore par ondes. Les messages transmis sont appelés des **trames** ;
- **internet** : c'est la couche qui s'occupe du routage des messages sur le ou les réseaux. En d'autres termes, elle se préoccupe du bon acheminement des messages à leur destinataire. Les messages sont appelés des **paquets** ;
- **transport** : c'est la couche qui s'occupe de la communication entre logiciels (services) sur le ou les réseaux (exemples : sites internet, skype, etc.). Les messages sont appelés des **segments** ;
- **application** : c'est la couche la plus haute. Elle regroupe les protocoles fournissant des services (exemples : service de partage de fichier, services mail, etc.).

Citons quelques-uns des protocoles les plus répandus (du plus bas au plus haut) :

Couche	Protocole	Service associé
Accès réseau	Ethernet	Le protocole Ethernet est utilisé pour la communication matérielle, à l'échelle des câbles (des câbles Ethernet). Il décrit la manière de transmettre les signaux binaires sur un fil reliant deux appareils.
	Wifi	Le protocole Wifi assure la même fonctionnalité que le protocole Ethernet, une communication matérielle, mais décrit cette fois-ci la manière de transmettre les signaux binaires par ondes radios, sans lien filaire.
IP	Protocoles IP	Suite de protocoles qui, entre autres, scinde les messages en paquets et en assure l'acheminement au travers du réseau.
Transport	TCP	Le protocole TCP permet à un ou plusieurs logiciels de se connecter à un autre logiciel et d'échanger des données. Ce protocole dispose de fonctionnalités permettant d'assurer l'intégrité des données transmises et de s'assurer que les données ont effectivement été transmises.
	UDP	Le protocole UDP permet à un ou plusieurs logiciels d'échanger des données sans maintenir de connexion entre les logiciels. La transmission des données est plus rapide mais moins sure qu'en TCP.
Application	HTTP ou HTTPS HyperText Transfer Protocol	Le protocole HTTP permet en outre de communiquer avec un serveur web en vue d'accéder à ses ressources. HTTPS est la version sécurisée (cryptée) du protocole HTTP.
	SMTP Simple Mail Transfer Protocol	Le protocole SMTP permet le transfert de courriers électroniques d'un serveur de courrier à un autre. Autrement dit, il permet typiquement d'envoyer/diffuser des mails.
	IMAP POP3	Les protocoles IMAP et POP3 permettent la consultation (côté client) des courriers électroniques stockés sur serveurs respectivement IMAP et POP.

Application	FTP ou SFTP File Transfer Protocole	Le protocole FTP permet l'échange de fichiers entre clients FTP et serveur FTP. On parle de serveur de fichiers. SFTP en est la version sécurisée (cryptée).
	DNS	Le protocole DNS assure la conversion des noms de domaines en adresses IP. Pour ce faire, les serveurs DNS utilisent en outre des tables de correspondances qui associent un nom de domaine à une adresse IP et inversement.
	DHCP Dynamic Host Configuration protocol	Serveur DHCP (permettant aux hôtes d'un réseau d'obtenir une adresse IP sur le réseau sur demande. On parle d'adresse IP dynamique).

Pour conclure, on comprendra bien que les protocoles d'une couche ont recours à un ou aux protocoles de la couche d'en-dessous. Par exemple, HTTP (couche application) utilise par défaut le protocole UDP (couche transport). D'où le fait que l'on ait recours à l'expression pile de protocoles.