Formation Cisco :

Vous l'aurez compris, un réseau est un ensemble de périphériques, de protocoles et de supports qui travaillent ensemble pour permettre la communication d'un périphérique à un autre. Que cela soit une communication locale entre deux postes de la même maison, ou un appel vidéo en ligne entre la France et les États-Unis, utilisant ainsi la puissance d'Internet.

Bien entendu, le réseau n'est pas constitué uniquement de périphériques utilisateurs et utilise des équipements, protocoles et supports spécialisés pour communiquer. Nous aurons l'occasion d'en parler dans les prochaines pages de ce cours.

Travailler à l'aide d'un réseau

En utilisant les réseaux, un salarié est aujourd'hui capable de travailler à distance et de s'intégrer au réseau interne de l'entreprise à l'aide de sa connexion domestique. Ce mode de travail permet au salarié de mieux concilier sa vie privée et professionnelle, en évitant les déplacements physiques.

Un rapport datant de 2012, adressé au Ministre chargé de l'Industrie, de l'Énergie et de l'Économie numérique mentionnait que plus de **12 %** des salariés télétravaillaient au moins huit heures par mois.

Au-delà de cette statistique, ces technologies sont une formidable occasion de permettre à des personnes en situation d'handicap de s'intégrer pleinement et de travailler comme n'importe quel autre salarié.

Communiquer à l'aide d'un réseau

Aujourd'hui, il est très simple de se mettre en contact avec n'importe quelle autre personne sur la planète, tant que ces personnes ont un accès à Internet.

Avant l'arrivée de supports rapides tels que l'ADSL ou maintenant la fibre optique, les communications étaient limitées à la messagerie instantanée ou à des interactions très basiques.

De nos jours, nous pouvons échanger de façon orale et visuelle par le biais d'outils de communication tels que Skype, WhatsApp et Facebook.

Se divertir à l'aide d'un réseau

N'importe quel joueur peut interagir et communiquer avec un autre à l'aide d'un réseau local ou d'Internet.

La démocratisation et le déploiement global d'Internet ont conduit à une ouverture incroyable des possibilités de jeu et de collaboration entre les joueurs.

Apprendre à l'aide d'un réseau

Tout le monde peut aujourd'hui apprendre et partager sa connaissance à l'aide d'outils comme Wikipédia.

Dans un modèle plus traditionnel, l'interaction élève / professeur est aujourd'hui enrichie par ses technologies. Ainsi, un professeur de mathématiques peut montrer à un élève connecté en ligne comment résoudre une équation à l'aide d'un tableau blanc numérique.

Le suivi pédagogique des élèves peut également être complété par ses outils.

    - **onnectivité globale :** La connexion à Internet s'effectue en majeure partie en France grâce aux technologies ADSL, qui utilisent la ligne cuivre France Telecom comme support de communication. La bande passante que peut offrir cette connexion dépend de la technologie de synchronisation utilisée ainsi que de la longueur de la ligne. Le débit descendant est bien souvent supérieur au débit ascendant sur ces lignes.
        - Avec la modernisation des réseaux et des infrastructures, nous voyons de plus en plus de déploiement des supports fibre optique à usage domestique, permettant une perte minimale et ainsi un débit descendant / ascendant largement plus avantageux.

- **Les réseaux de petits bureaux / bureaux à domicile** sont similaires aux installations domestiques, à la nuance que l'entreprise peut choisir de ne pas utiliser une ligne ADSL classique, mais SDSL, permettant d'avoir un débit ascendant / descendant symétrique. Parfois, les réseaux de petits bureaux comptent plus de périphériques connectés comparés aux réseaux domestiques.

- **Les moyens et grands réseaux** représentent des installations d'entreprises, reliées (ou non) à Internet, qui peuvent aller d'un déploiement unique au siège social de l'entreprise à de grandes architectures reliant les filiales et antennes nationales au siège.
    - **Composants :** Des équipements réseau d'entreprise, sécurisés et redondants. Le réseau étant de nos jours un besoin incontournable de l'entreprise, l'installation doit être résiliente et dotée de mécanismes automatiques ou manuels de reprise d'activité.
    - **Mode de connexion :** Les employés peuvent se connecter, selon la politique de sécurité de l'entreprise en filaire ou en sans-fil. Ils ont également la possibilité de se connecter au réseau interne de l'entreprise de leur domicile, via une technologie nommée VPN (*Virtual Private Network*).
    - **Connectivité globale :** La connectivité entre les sites de l'entreprise et Internet est assurée par des connexions redondantes et à très haut débit, type fibre optique.

- **Les réseaux mondiaux** sont des architectures qui s'étendent sur toute la surface du globe et permettent la communication internationale. Elles prennent bien souvent la forme de câbles sous-marins déployés pour interconnecter par exemple, la France avec le Royaume-Uni. Ces connexions sont déployées et maintenues par des opérateurs (Orange, Level3, Tata, ...). Ces connexions permettent à des multinationales d'interconnecter différents bureaux ensemble et permettre une communication sécurisée entre ceux-ci.

Évidemment, la taille du réseau impacte la stratégie de déploiement de celui-ci ainsi que les divers besoins en connectivité globale.

Activité : trouver un câble sous-marin et en analyser les caractéristiques

Prérequis pour cette activité :

- Un ordinateur doté d'un navigateur web

Etapes de l'activité :

1. Connectez-vous sur l'ordinateur.
2. Lancer votre navigateur et dirigez-vous vers le site internet suivant : http://www.submarinecablemap.com (Liens vers un site externe.)Liens vers un site externe.
3. Cherchez un câble sous-marin nommé Apollo dont l'une des terminaisons se trouve à Lannion, en Bretagne, France
4. Notez les caractéristiques du cable et le chemin qu'il emprunte

Après avoir effectué ces manipulations de votre côté, répondez à ces questions :

Question : qui est le propriétaire de ce câble ?

Question : quelle est l'année de mise en service de ce câble ?

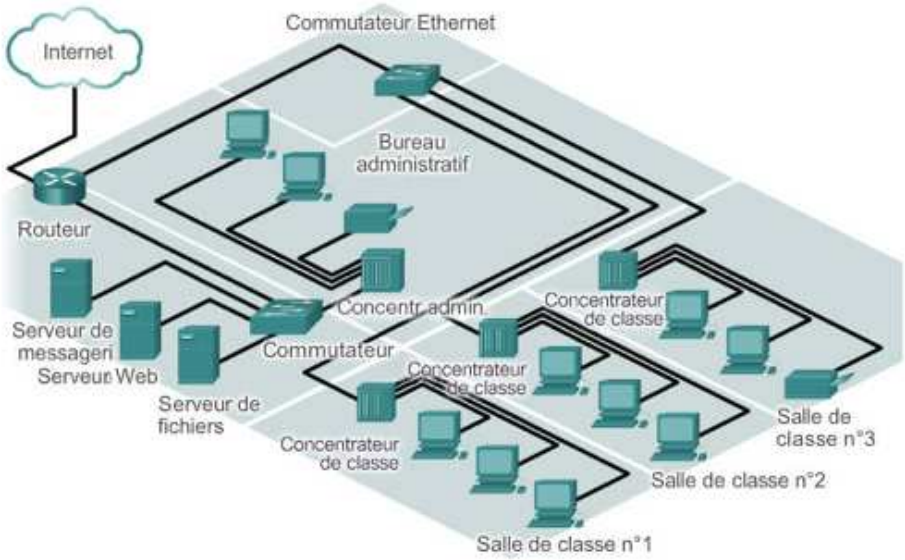
Question : quels sont les autres points de terminaisons de ce câble ?

Question : quelle est la longueur de ce câble ?

Les plans de topologie visent à exprimer, en utilisant des symboles communément admis, l'état de l'architecture réseau, tant sur le plan physique que logique.

Ils sont une donnée essentielle pour documenter l'architecture réseau, analyser son fonctionnement et effectuer des dépannages. Ces éléments sont également important dans des projets d'évolution d'architecture, permettant d'identifier en un coup d'oeil les éléments critiques et potentiels impacts d'une modification de la topologie.

Topologie physique :



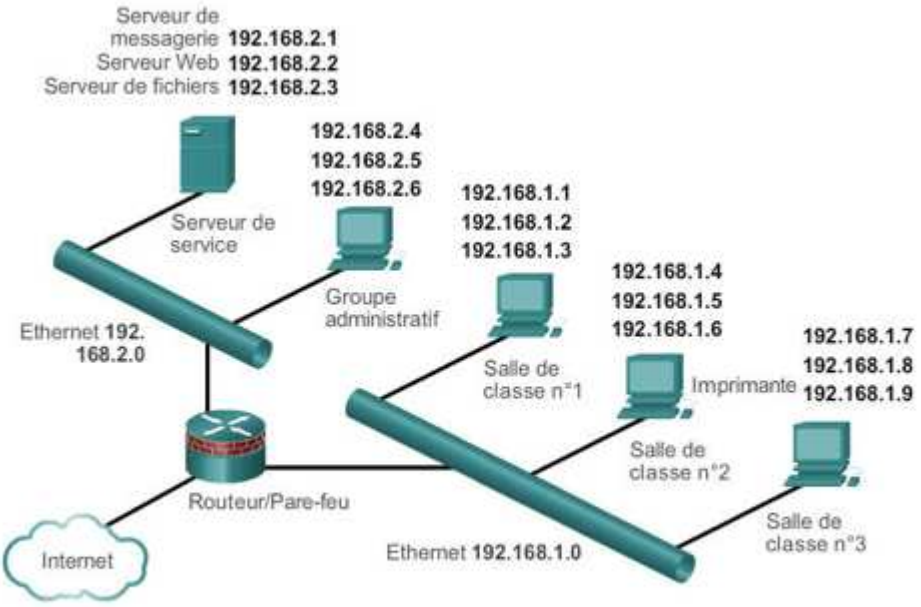
Cette topologie est communément appelée "topologie de niveau 2", en référence à la couche 2 - **Liaison de données** - du modèle OSI - *Open Systems Interconnection*.

Ce schéma vise à décrire les éléments suivants :

- La disposition physique des périphériques et équipements réseaux
- Le câblage physique des périphériques et équipements réseaux

En aucun cas sur ce schéma ne sont mentionnés les adresses IP ou sous-réseaux, c'est l'objet de la topologie logique.

Topologie logique :

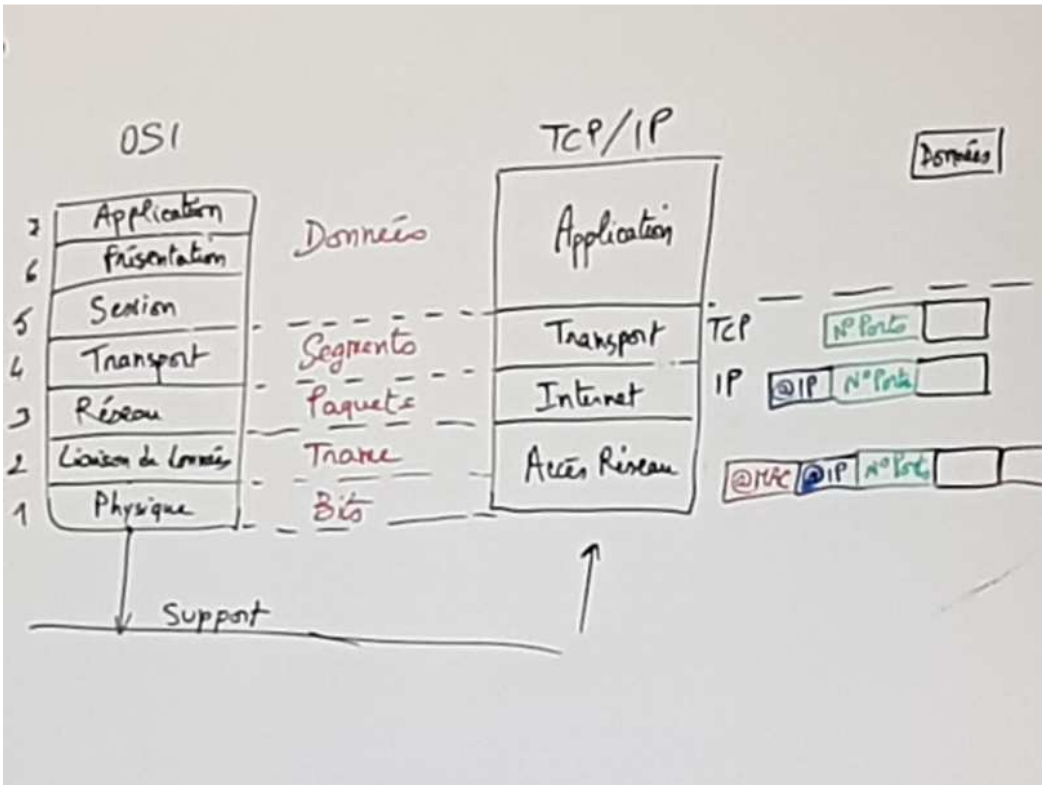


Cette topologie est communément appelée "topologie de niveau 3", en référence à la couche 3 - **Réseau** - du modèle OSI.

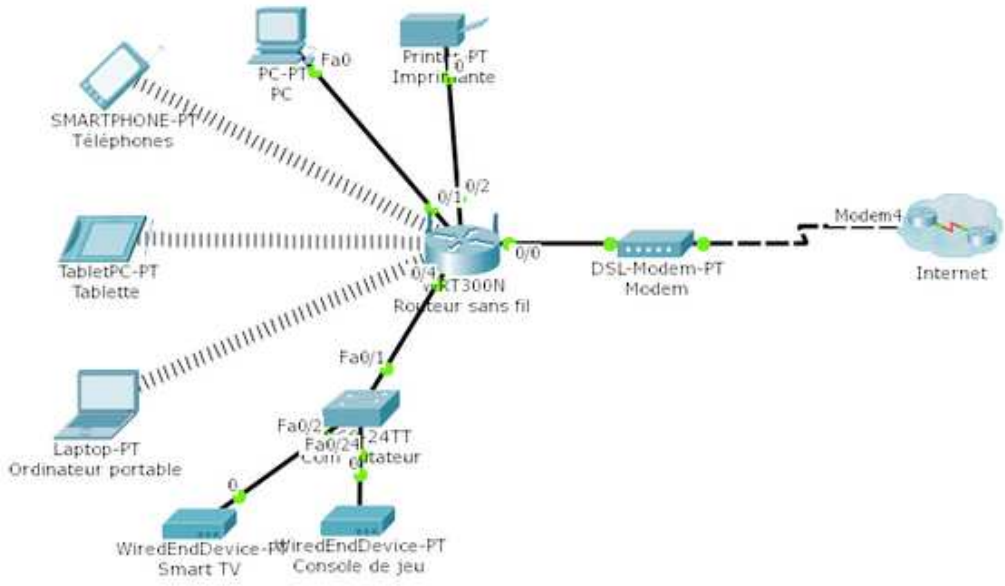
Ce schéma vise à décrire les éléments suivants :

- Les périphériques et équipements réseaux de niveau 3 ou plus
  - Les commutateurs et concentrateurs travaillant en couche inférieures, ils ne sont logiquement pas mentionnés
- Les sous-réseaux configurés et utilisés
- L'association des postes de travail avec les sous-réseaux présentés
- Les adresses IP associées aux périphériques réseaux
- Si applicable, la relation du réseau local à Internet

L'objectif de ce schéma n'est pas d'exposer le placement physique ni le câblage des équipements. Ainsi, deux postes dans le même sous-réseau peuvent sembler proches alors qu'ils ne se trouvent pas nécessairement dans la même salle de classe.



Topologie d'un réseau domestique



Le schéma de topologie ci-dessus représente l'architecture d’un réseau domestique typique.

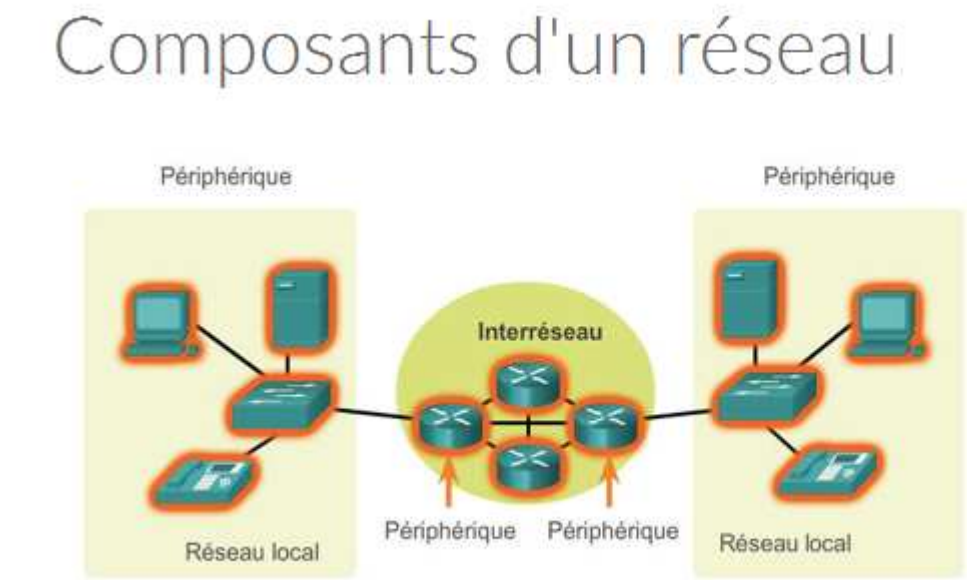
Celui-ci comprend les périphériques et installations domestiques suivantes :

- **Des périphériques finaux**
  - Une tablette
  - Un ordinateur fixe
  - Un ordinateur portable
  - Un téléphone intelligent
  - Une imprimante
  - Une TV connectée

- Une console de jeu

- **Des équipements réseaux**
  - Un commutateur (*fourni dans le bundle académique*)
  - Un routeur et point d'accès (*fourni dans le bundle académique*)
  - Un modem

Avec ce type d'exemple, vous pourrez démontrer aux élèves comment un réseau fonctionne à **l'aide de l'outil de simulation Packet Tracer ainsi qu'en réel avec les équipements physiques dont vous serez dotés.**



---

il existe trois types de composants d'un réseau :

- les périphériques
- les supports de transmissions
- les services

Les périphériques se divisent en deux familles :

- **les périphériques finaux, source ou destination d'un trafic réseau.** Ils sont pour la plupart le point où l'humain peut communiquer avec la machine, par le biais d'une interface humain-machine. Néanmoins, certains périphériques finaux n'interagissent pas directement avec son utilisateur. C'est le cas par exemple des capteurs ou des caméras connectées. **Dans l'image ci-dessus, les postes fixes, les téléphones IP et les serveurs sont des périphériques finaux.**

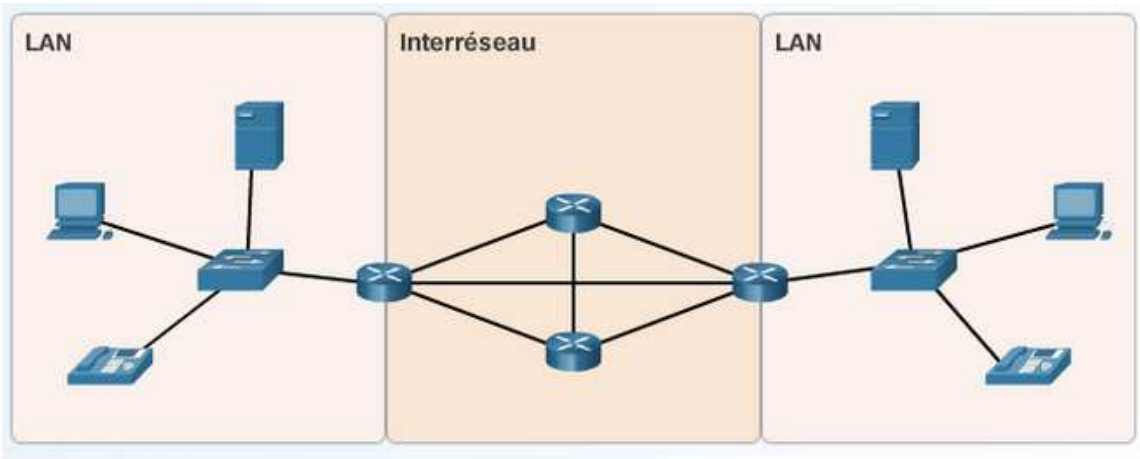
- **les périphériques réseaux intermédiaires, équipements de l'infrastructure réseau.** Les périphériques réseaux ne sont pas visibles directement de la perspective de l'utilisateur, ils oeuvrent néanmoins pour connecter les hôtes et les réseaux ensemble. **Dans l'exemple, les commutateurs (dans le réseau local) et les routeurs (dans l'interréseau) sont des périphériques réseaux.**

Les supports de transmission relient les périphériques ensemble, représentant sur le schéma **des lignes continues de couleur noire**, ce qui signifie l'utilisation d'un support de connexion type

réseau local LAN (Local Area Network). Veuillez noter qu'en fonction de la nature du support de transmission, le mode de représentation peut également changer.

Les services ne figurent pas sur le schéma directement. Ce sont les applications qui peuvent utiliser l'architecture réseau et servir les utilisateurs directement ou indirectement, par le biais des périphériques finaux. Nous pourrions citer par exemple un service Web qui s'exécuterait sur les serveurs du réseau local permettant la consultation de page Web au sein du réseau interne. Ou bien encore la téléphonie sur IP rendue possible grâce aux techniques Voice Over IP (VoIP) et à l'utilisation de téléphones IP. De la perspective des utilisateurs, les services rendent possible les usages du réseau tout en restant transparents.

Qu'est-ce qu'un routeur?



Un routeur **interconnecte** des réseaux locaux ensemble. Il est installé en règle générale en lien direct avec d'autres routeurs, permettant de former **l'interréseau** et ainsi remplir son rôle principal.

Un routeur permet en outre, de connecter des périphériques locaux à Internet.

Plusieurs types de routeurs sont disponibles selon le contexte d'installation. Ci-dessous, vous trouverez des exemples d'équipements en fonction de l'environnement de déploiement :

- routeur et point d'accès Wi-Fi
  - *"box"* opérateur
  - Cisco RV215W Wireless-N VPN Router (fourni avec le cours)

Qu'est-ce qu'un commutateur ?

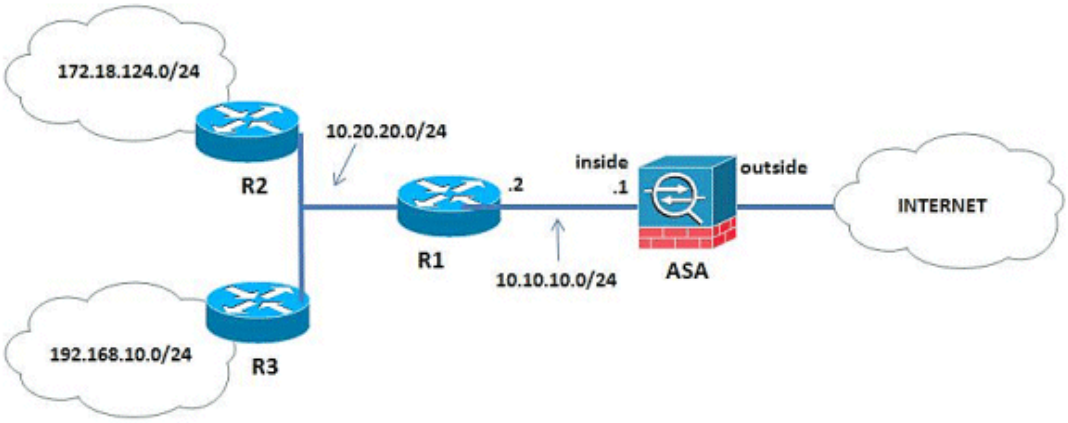
Un commutateur **connecte** des périphériques locaux ensemble. Il est installé en règle générale au sein du réseau local (*LAN - Local Area Network*).

Certains commutateurs spécialisés peuvent jouer le rôle de routeur (les commutateurs de niveau 3) ou alimenter des équipements locaux (les commutateurs PoE - Power over Ethernet), tels que des téléphones et caméras IP.

Plusieurs types de commutateurs sont disponibles selon le contexte d'installation. Ci-dessous, vous trouverez des exemples d'équipements en fonction de l'environnement de déploiement :

- commutateur intégré
  - *"box"* opérateur
  - Cisco RV215W Wireless-N VPN Router (fourni avec le cours)
- commutateur domestique / TPE / PME
  - Cisco SF302-08 8-Port 10 100 Managed Switch with Gigabit Uplinks (fourni avec le cours)

Qu'est-ce qu'un pare-feu?



Il est important de protéger les ordinateurs individuels et les serveurs reliés au réseau, mais il convient également de contrôler le trafic en direction et en provenance du réseau.

Le pare-feu est l'un des outils de sécurité les plus efficaces pour protéger les utilisateurs internes du réseau des menaces externes. Un pare-feu se trouve entre deux réseaux, ou plus, et contrôle le trafic entre eux tout en contribuant à éviter les accès non autorisés. Les pare-feu emploient diverses techniques pour déterminer les accès autorisés à un réseau ou les accès à interdire. Ces techniques sont les suivantes :

- **Filtrage des paquets** : interdit ou autorise l'accès selon les adresses IP ou MAC.
- **Filtrage des applications** : interdit ou autorise l'accès à des types d'applications spécifiques en fonction des numéros de ports.
- **Filtrage d'URL** : interdit ou autorise l'accès à des sites Web en fonction d'URL ou de mots clés spécifiques.
- **Inspection dynamique de paquets** : les paquets entrants doivent constituer des réponses légitimes aux requêtes d'hôtes internes. Les paquets non sollicités sont bloqués, sauf s'ils sont expressément autorisés. L'inspection de paquets peut éventuellement reconnaître et filtrer des types d'attaques spécifiques telles que le déni de service.

Les pare-feu peuvent prendre en charge une ou plusieurs possibilités de filtrage, parmi celles décrites. En outre, les pare-feu effectuent souvent une traduction d'adresses réseau. Ce mécanisme consiste à traduire (ou convertir) une adresse IP ou un groupe d'adresses IP internes en une adresse IP publique externe envoyée sur le réseau. Cela permet de dissimuler les adresses IP internes aux utilisateurs externes.

Les pare-feu sont disponibles sous plusieurs formes, comme décrit ci-dessous :

- **Pare-feu matériel** - Un pare-feu matériel est intégré à un périphérique matériel dédié appelé appareil de sécurité.

- **Pare-feu basé sur un serveur** : un pare-feubasé sur un serveur est constitué d'une application de pare-feu qui s'exécute sur un système d'exploitation tel que Linux ou Windows.

- **Pare-feu intégré** : un pare-feu intégré est mis en œuvre par l'ajout d'une fonction de pare-feu à un périphérique existant, comme un routeur.

- **Pare-feu personnel** - Un pare-feu personnel se trouve sur un ordinateur hôte et n'est pas conçu pour une mise en œuvre sur un réseau local. Il peut être disponible par défaut dans le système d'exploitation ou obtenu auprès d'un vendeur externe.

Plusieurs types de pare-feu sont disponibles selon le contexte d'installation. Ci-dessous, vous trouverez des exemples d'équipements en fonction de l'environnement de déploiement :

- pare-feu intégré
  - *"box"* opérateur
  - Cisco RV215W Wireless-N VPN Router
- pare-feu domestique / TPE / PME
  - Cisco ASA 5505 Adaptive Security Appliance
- pare-feu d'entreprise
  - Cisco ASA 5555-X Adaptive Security Appliance

La représentation générique d'un pare-feu dans un schéma de topologie est la suivante :

Supports de transmission

Différents supports de transmissions existent pour échanger des informations entre périphériques: le cuivre, la fibre optique et les technologies sans-fil.

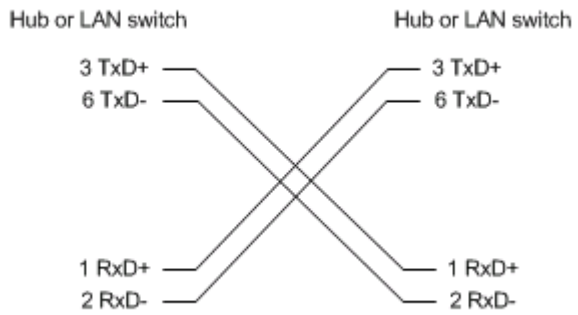
Les critères de choix parmi ses technologies impliquent souvent :

- la portée maximale du signal
- la bande passante disponible
- le coût d'implémentation
- la sensibilité aux perturbations environnementales

Des normes existent pour concevoir des câbles Ethernet avec des connecteurs RJ45.

La construction d'un câble droit constitue une connexion commune aux deux extrémités du câble. Comme vous pourrez le remarquer sur le schéma ci-dessus, le câble croisé inverse, sur une des extrémités les paires n°2 et 3.

Un poste de travail se connectera à un commutateur avec un câble **droit**. Deux routeurs, commutateurs ou postes de travail seront en revanche liés par un câble **croisé**.

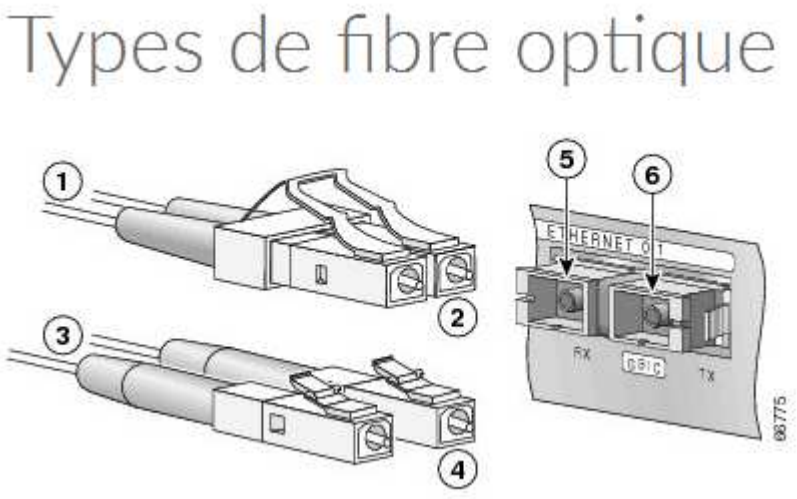


Vous pouvez par ailleurs vous poser la question du **Pourquoi?** Prenons l'exemple de deux postes fixes liés ensemble par un câble Ethernet **droit**. Les postes utilisent une manière commune pour transmettre et recevoir l'information à travers la connexion Ethernet. Dans une connexion FastEthernet, les pins utilisés pour transmettre sont les numéros **1 et 2 (TX+/TX-)** et pour la réception les **3 et 6 (RX+/RX-)**.

Or, si deux postes utilisent un câble **droit** pour se connecter, les postes s'enverront mutuellement l'information sur les mauvais pins. Il faut donc **croiser** le câble pour permettre aux pins de transmission (**TX**) de correspondre aux pins de réception (**RX**) du destinataire. Et réciproquement.

Selon le scénario de déploiement, il est donc utile de prévoir des câbles de différents types.

Sachez néanmoins que les commutateurs modernes sont aujourd'hui capables de gérer les connexions incorrectes en utilisant des technologies telles que l'Auto-MDIX (Liens vers un site externe.)Liens vers un site externe.et d'assurer néanmoins une connectivité avec un câble non adapté.



La fibre optique consiste en un câble très fin de verre ou de plastique dans lequel va transiter de la lumière pour coder une information. Ces câbles sont bien entendu gainés et protégés pour éviter toute exposition à une lumière autre que celle transmise par les deux équipements connectés.

La fibre permet souvent de faire **transiter l'information plus rapidement qu'avec les supports cuivre traditionnels. De plus, quand une liaison cuivre peut attendre une distance maximale de 100 mètres, la fibre optique peut offrir une portée supérieure à 50 kilomètres, en fonction de la technologie de transmission et des supports utilisés.**

Par ailleurs, les câbles sous-marins qui constituent Internet utilisent pour la plupart des fibres optiques pour interconnecter les pays et continents.

Pour information, il existe deux types de fibre optique, **monomode** ou **multimode**.

Problèmes de mise en œuvre	Cuivre	Fibre optique
Bande passante	10 Mbit/s – 10 Gbit/s	10 Mbit/s – 100 Gbit/s
Distance	Relativement courte (de 1 à 100 mètres)	Relativement longue (de 1 à 100 000 mètres)
Résistance aux perturbations électromagnétiques et radioélectriques	Faible	Élevée (résistance totale)
Résistance aux risques électriques	Faible	Élevée (résistance totale)
Coûts des supports et des connecteurs	Le plus faible	Le plus élevé
Compétences requises pour l'installation	Le moins	Le plus
Précautions à prendre pour la sécurité	Le moins	Le plus

Types de transmission sans fil

Wi Fi	• **Normes IEEE 802.11**
	• **Aussi appelé Wi-Fi**
	• **CSMA/CA**
	• **Avec des variantes :**
	  • **802.11a : 54 Mbit/s, 5 GHz**
	  • **802.11b : 11 Mbit/s, 2,4 GHz**
	  • **802.11g : 54 Mbit/s, 2,4 GHz**
	  • **802.11n : 600 Mbit/s, 2,4 et 5 GHz**
	  • **802.11ac : 1 Gbit/s, 5 GHz**
	  • **802.11ad : 7 Gbit/s, 2,4 GHz, 5 GHz et 60 GHz**

Bluetooth®	• Norme IEEE 802.15 • Vitesse jusqu'à 3 Mbit/s • Jumelage de périphériques sur des distances de 1 à 100 mètres
Wi MAX	• Norme IEEE 802.16 • Vitesse jusqu'à 1 Gbit/s • Utilise une topologie point à multipoint pour fournir un accès à large bande sans fil

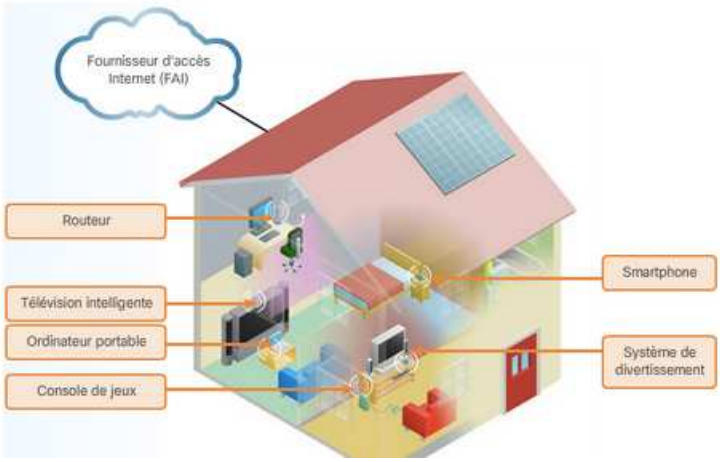
Plusieurs standards de transmission existent pour assurer une transmission sans-fil.

Les normes, vitesses théoriques et capacités des standards sont mentionnés dans le tableau ci-dessus pour information.

Exemples de transmissions sans-fil

Pour bien différentier chaque technologie sans-fil et son contexte d'utilisation, citons quelques usages.

Wi-Fi



La connexion sans-fil d'un domicile est bien souvent partagée en utilisant la technologie Wi-Fi.

Celle-ci permet aux appareils domestiques de se connecter au réseau local et par extension, à Internet.

Bluetooth

La technologie Bluetooth permet à plusieurs périphériques proches de communiquer et d'échanger sans fil. Pour cela, les appareils forment un réseau personnel, aussi appelé PAN (*Personal Area Network*).

Dans ce cadre, il est souvent question de transfert de données direct, d'un appareil à un autre, sans intermédiaire.

Les exemples d'applications sont nombreux :

- connexion d'une oreillette sans-fil à un téléphone intelligent
- transfert de données entre deux ordinateurs / smartphones
- manettes de consoles de jeux

WiMAX

La technologie WiMAX consiste à apporter l'accès à Internet par le biais d'antennes, sur le même principe des antennes cellulaires utilisés par les téléphones mobiles.

Cette technologie est particulièrement utile dans les zones non-denses où les lignes cuivres et les installations locales ne peuvent pas desservir les habitations dans de bonnes conditions.

Normes Wi-Fi

Norme	Débit maximal	Fréquence	Rétro-compatible
802.11a	54 Mbit/s	5 GHz	Non
802.11b	11 Mbit/s	2,4 GHz	Non
802.11g	54 Mbit/s	2,4 GHz	802.11b
802.11n	600 Mbit/s	2,4 GHz ou 5 GHz	802.11b/g
802.11ac	1,3 Gbit/s (1 300 Mbit/s)	2,4 GHz et 5,5 GHz	802.11b/g/n
802.11ad	7 Gbit/s (7 000 Mbit/s)	2,4 GHz, 5 GHz et 60 GHz	802.11b/g/n/ac

Pour information, le tableau ci-dessus décrit les normes sans-fil les plus répandues (à l'exception du 802.11ad).

Comme vous pouvez le voir, les vitesses ont pu augmenter avec les progrès techniques et l'utilisation de bandes de fréquence différentes. Au point d'arriver aujourd'hui à dépasser la limite du Gigabit en transmission sans-fil avec la norme 802.11ac. Une vidéo de la taille de **4 gigaoctets** serait ainsi transférée en l'espace d'un peu plus de ... **25 secondes.**

Concernant la technologie Wi-Fi, les débits théoriques et bandes de fréquences dépendant de la norme utilisée pour communiquer entre le client et le point d'accès.

Notez que pour utiliser une norme en particulier, le client et le point d'accès doivent être mutuellement compatible avec cette dernière.

Cependant, selon les situations, la rétro-comptabilité avec d'autres normes est possible. Par exemple, un point d'accès 802.11ac peut offrir de la connectivité aux clients 802.11b/g/n.

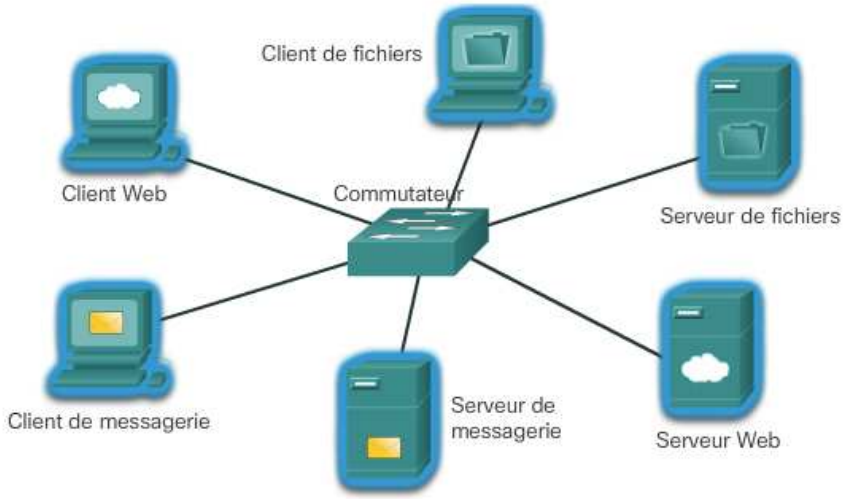
Pour information, le tableau ci-dessus décrit les normes sans-fil les plus répandues (à l'exception du 802.11ad).

Comme vous pouvez le voir, les vitesses ont pu augmenter avec les progrès techniques et l'utilisation de bandes de fréquence différentes. Au point d'arriver aujourd'hui à dépasser la limite du Gigabit en transmission sans-fil avec la norme 802.11ac. Une vidéo de la taille de **4 gigaoctets** serait ainsi transférée en l'espace d'un peu plus de ... **25 secondes.**

Concernant la technologie Wi-Fi, les débits théoriques et bandes de fréquences dépendant de la norme utilisée pour communiquer entre le client et le point d'accès.

Notez que pour utiliser une norme en particulier, le client et le point d'accès doivent être mutuellement compatible avec cette dernière.

Client / serveur

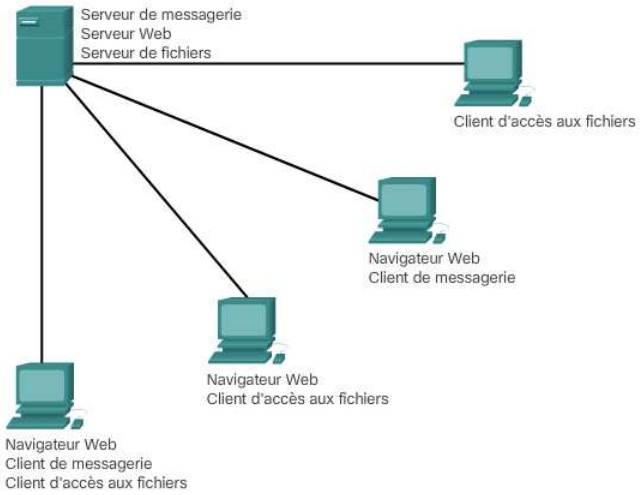


Tous les ordinateurs connectés à un réseau et qui participent directement aux communications réseau sont des hôtes ou des périphériques finaux. Les hôtes peuvent envoyer et recevoir des messages sur le réseau. Dans les réseaux actuels, les périphériques finaux peuvent jouer le rôle de client, de serveur, ou les deux. Les logiciels installés sur l'ordinateur déterminent le rôle qu'il tient au sein du réseau.

Les serveurs sont des hôtes équipés des logiciels leur permettant de fournir des informations, comme des messages électroniques ou des pages Web, à d'autres hôtes sur le réseau. Chaque service nécessite un logiciel serveur distinct. Par exemple, un hôte nécessite un logiciel de serveur Web pour pouvoir offrir des services Web au réseau.

Les clients sont des ordinateurs hôtes équipés d'un logiciel qui leur permet de demander des informations auprès du serveur et de les afficher. Un navigateur Web, tel qu'Internet Explorer, est un exemple de logiciel client.

Client / serveur - suite

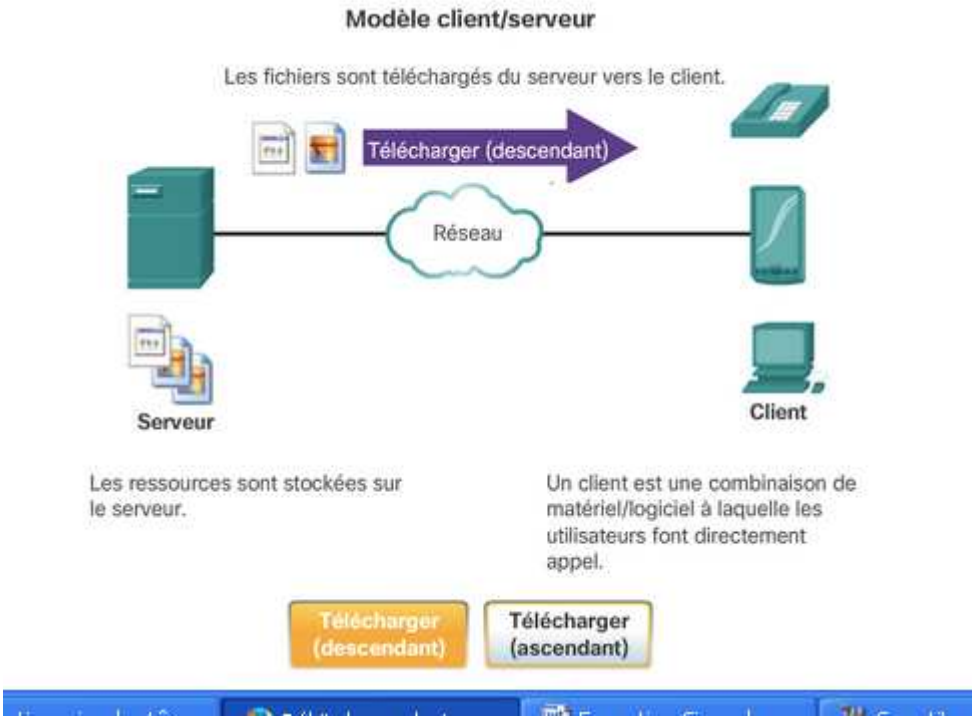


Un ordinateur équipé d'un logiciel serveur peut fournir des services à un ou plusieurs clients en même temps.

De plus, un seul ordinateur peut exécuter différents types de logiciel serveur. Chez les particuliers et dans les petites entreprises, il peut arriver, par nécessité, qu'un ordinateur fasse office à la fois de serveur de fichiers, de serveur Web et de serveur de messagerie.

Un seul ordinateur peut également exécuter différents types de logiciel client. Un logiciel client doit être installé pour chaque type de service requis. Un hôte équipé de plusieurs clients peut se connecter à plusieurs serveurs en même temps. Par exemple, un utilisateur peut consulter sa messagerie électronique et une page Web en même temps qu'il utilise la messagerie instantanée et écoute la radio sur Internet.

Débit descendant



De la perspective de chaque périphérique connecté sur un réseau, chacun peut envoyer et recevoir des informations.

Lorsque qu'un client demande à télécharger un fichier stocké sur un serveur, ce dernier s'éxecute en **envoyant** les informations au client qui **télécharge** la donnée. La distinction entre ces deux termes est importante. Ainsi, quand le serveur envoie la donnée, il utilise sa **bande passante disponible d'envo**i alors que le client utilise **sa bande passante disponible de réception.**

Vous pouvez vous poser la question de la vitesse de téléchargement qui s'applique ici. Là aussi, cela dépend de ce qui sépare ces deux postes.

Scénario 1 :

Imaginons que ces deux périphériques soient connectés en réseau local. Dans cette situation, le débit utilisable sera celui de la connexion locale qui lie les deux postes ensemble.

Attention, en cas de vitesse de connexion asymétrique entre ces deux postes, la vitesse la plus basse limitera le débit de transfert entre ces deux entités. Par exemple, si le serveur négocie une vitesse d'interface de **10 mégabits par seconde** quand le client a négocié une vitesse de **100 mégabits par seconde**, la vitesse maximale de transfert sera **limitée à 10 mégabits par seconde** entre ces deux postes, même si le client peut télécharger plus vite. Le facteur limitant ici étant la **vitesse d'émission du serveur,** non la vitesse de réception du client.

La communication étant ici purement locale, en aucun cas, le débit Internet ne sera utilisé. Il n'est donc pas pertinent de l'aborder dans cet exemple.

Scénario 2 :

Imaginons que ces deux périphériques soient physiquement séparés par Internet. Le serveur est hébergé chez un prestataire de service, dans le *cloud*. Le client accède au serveur par le biais d'Internet avec sa connexion domestique, une ligne ADSL qui possède les attributs suivants :

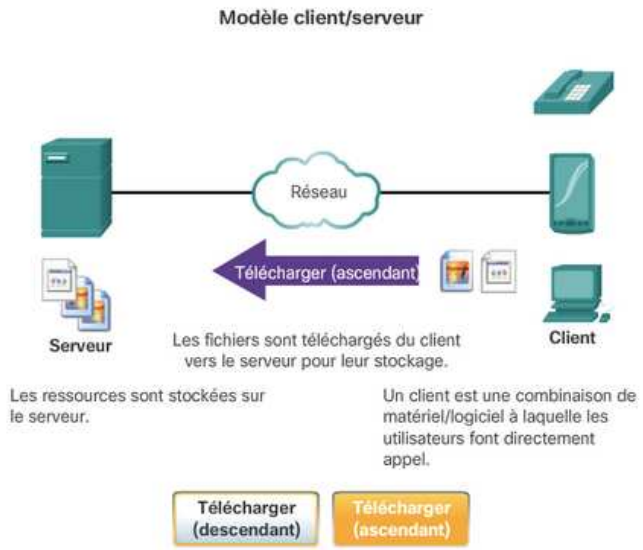
Le fichier étant téléchargé du serveur au client, la bande passante ici qui compte est bien à la fois la vitesse d'émission du serveur ainsi que la vitesse de réception de la ligne ADSL.

Bien que le prestataire de services où le serveur est hébergé garantit un débit symétrique de **10 Gigabits par seconde**, le facteur limitant ici est la vitesse de réception de la ligne. Ainsi, le client ne pourra pas télécharger à plus de **5243 kilobits par seconde** soit **655,375 kilooctets par seconde.**

Dans les deux scénarios, nous identifions un facteur limitant dans le réseau, entre le client et le serveur. Nous appelons communément cela **un goulot d'étranglement**.

De manière générale, si l'on veut étudier la vitesse théorique atteignable entre deux points, celle-ci sera **égale ou inférieure à la valeur vitesse la plus basse sur le chemin par lequel transite l'information.**

Débit ascendant



Lorsque qu'un client souhaite envoyer un fichier sur un serveur, le client s'éxecute en **envoyant** les informations au serveur qui **télécharge** la donnée. La distinction entre ces deux termes est importante. Ainsi, quand le client envoie la donnée, il utilise sa **bande passante disponible d'envo**i alors que le serveur utilise **sa bande passante disponible de réception.**

Vous pouvez vous poser la question de la vitesse d'envoi qui s'applique ici. Là aussi, cela dépend de ce qui sépare ces deux postes.

Scénario 1 :

Imaginons que ces deux périphériques soient connectés en réseau local. Dans cette situation, le débit utilisable sera celui de la connexion locale qui lie les deux postes ensemble.

Attention, en cas de vitesse de connexion asymétrique entre ces deux postes, la vitesse la plus basse limitera le débit de transfert entre ces deux entités. Par exemple, si le serveur négocie une vitesse d'interface de **10 mégabits par seconde** quand le client a négocié une vitesse de **100 mégabits par seconde**, la vitesse maximale de transfert sera **limitée à 10 mégabits par seconde** entre ces deux postes, même si le client peut envoyer plus vite. Le facteur limitant ici étant la **vitesse de réception du serveur,** non la vitesse d'émission du client.

La communication étant ici purement locale, en aucun cas, le débit Internet ne sera utilisé. Il n'est donc pas pertinent de l'aborder dans cet exemple.

Scénario 2 :

Imaginons que ces deux périphériques soient physiquement séparés par Internet. Le serveur est hébergé chez un prestataire de service, dans le *cloud*. Le client accède au serveur par le biais d'Internet avec sa connexion domestique, une ligne ADSL qui possède les attributs suivants :

Le fichier étant téléchargé du client au serveur, la bande passante ici qui compte est bien à la fois la vitesse de réception du serveur ainsi que la vitesse d'émission de la ligne ADSL.

Bien que le prestataire de services où le serveur est hébergé garantit un débit symétrique de **10 Gigabits par seconde**, le facteur limitant ici est la vitesse d'émission de la ligne. Ainsi, le client ne pourra pas envoyer à plus de **878 kilobits par seconde** soit **109,75 kilooctets par seconde.**

Dans les deux scénarios, nous identifions un facteur limitant dans le réseau, entre le client et le serveur. Nous appelons communément cela **un goulot d'étranglement.**

De manière générale, si l'on veut étudier la vitesse théorique atteignable entre deux points, celle-ci sera **égale ou inférieure à la valeur vitesse la plus basse sur le chemin par lequel transite l'information.**

Activité : évaluer le débit d'une connexion Internet

Prérequis :

- Un ordinateur équipé d'un navigateur Internet

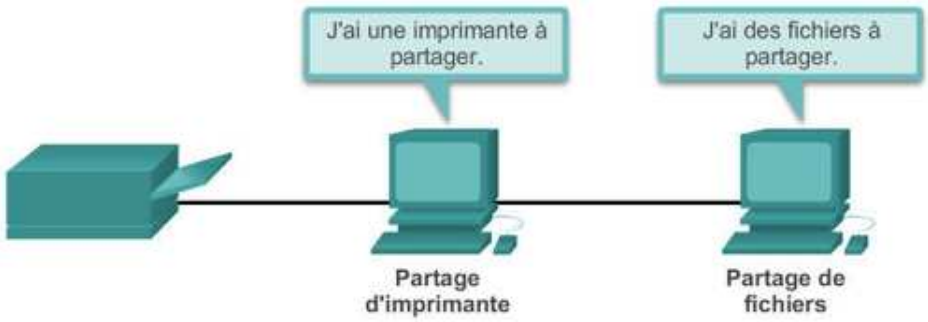
Etapes de l'activité :

1. Connectez vous sur le site suivant : http://www.speedtest.net/fr/

2. - Cliquez sur le bouton "**Démarrer le test**"
3. - Puis, laissez le test de débit se dérouler.

4. - Un rapport s'affiche alors avec votre vitesse ascendante et descendante.

Peer-to-peer



Le paradigme *peer-to-peer* (P2P) rend possible pour un périphérique réseau de devenir simultanément client et serveur, dans le but de partager ses ressources locales.

Dans l'exemple ci-dessus, le premier poste partage une imprimante directement connectée. Le deuxième poste partage des fichiers. Dans ces deux cas, les postes sont des serveurs.

Cependant, cela n'empêche à aucun moment les serveurs de devenir client pour accéder aux données partagées. Ainsi, le deuxième poste peut accéder à l'imprimante du premier poste. Le premier poste peut également accéder aux fichiers que l'autre poste a partagé.

Plus proche de nous, Microsoft a décidé d'implémenter ce mécanisme pour le téléchargement des mises à jour du système d'exploitation Windows 10. Ainsi, si votre poste dispose de la mise à jour stockée localement, ce dernier sera en capacité de la partager avec d'autres ordinateurs souhaitant télécharger ces fichiers.

Là, aussi, le poste agit en tant que serveur lorsqu'il propose des fichiers à d'autres ordinateurs.

Types de réseaux

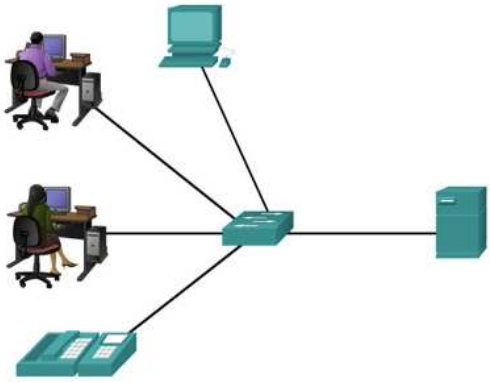
Il existe plusieurs types d'infrastructures réseau. Les modèles les plus répandus sont :

- Le réseau local (**LAN -** *Local Area Network*)
- Le réseau local sans fil (**WLAN -** *Wireless Local Area Network*)
- Le réseau étendu (**WAN -** *Wide Area Network***)**

Autres types de réseau :

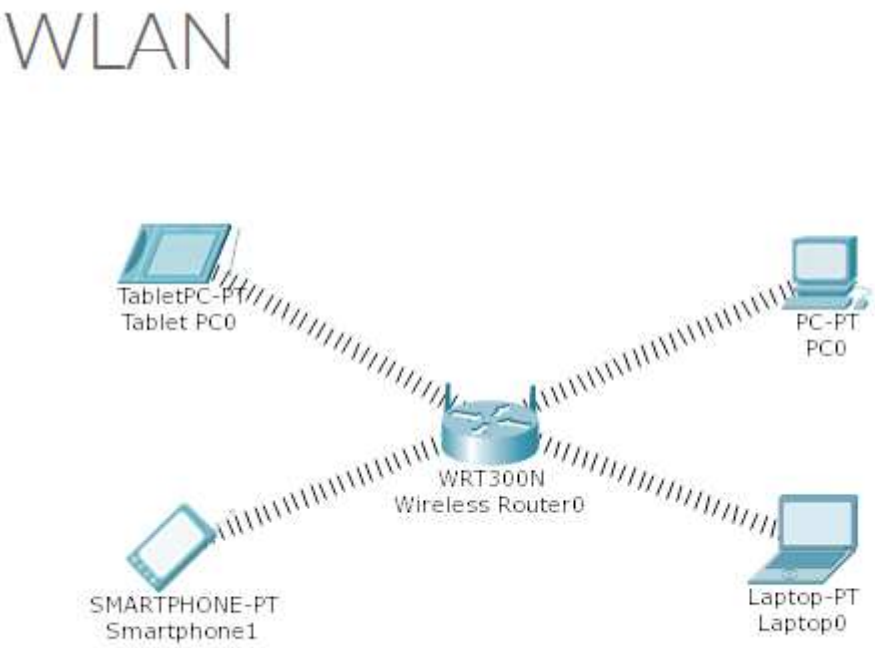
- Le réseau métropolitain (**MAN -** *Metropolitan Area Network*)
- Le réseau de stockage (**SAN -** *Storage Area Network*)

LAN



Le réseau local ou LAN (*Local Area Network*) est un réseau installé au sein d'une habitation, un collège, d'une entreprise.

Ce réseau a une portée exclusivement locale.

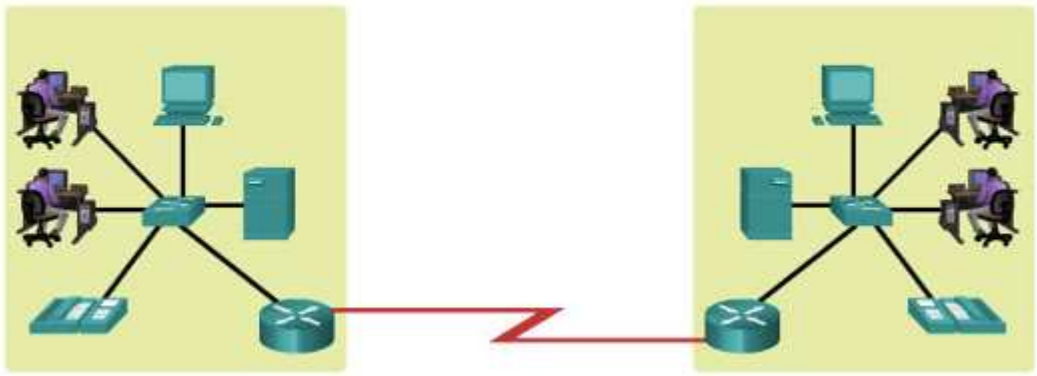


Le réseau local sans-fil ou WLAN (*Wireless Local Area Network*) est un réseau installé au sein d'une habitation, un collège, d'une entreprise.

Il permet la connectivité des clients en utilisant les technologies sans-fil Wi-Fi et ainsi permet l'intégration des équipements au sein du réseau local.

Ce réseau a une portée exclusivement locale.

WAN

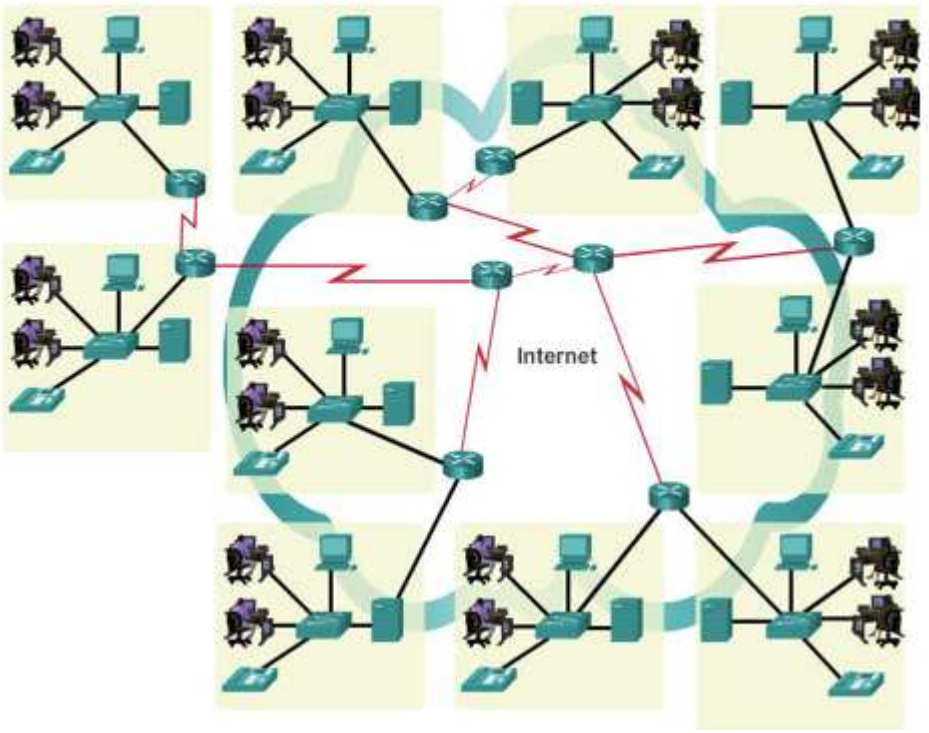


Le réseau étendu ou WAN (*Wide Area Network*) est un réseau reliant deux points séparés geographiquement.

Ce réseau permet une communication des deux réseaux locaux (*LAN*) grâce au lien distant (WAN) qui connecte les deux routeurs des deux réseaux locaux respectifs.

Un lien WAN peut également connecter l'entreprise et son réseau local aux réseaux opérateur et à Internet.

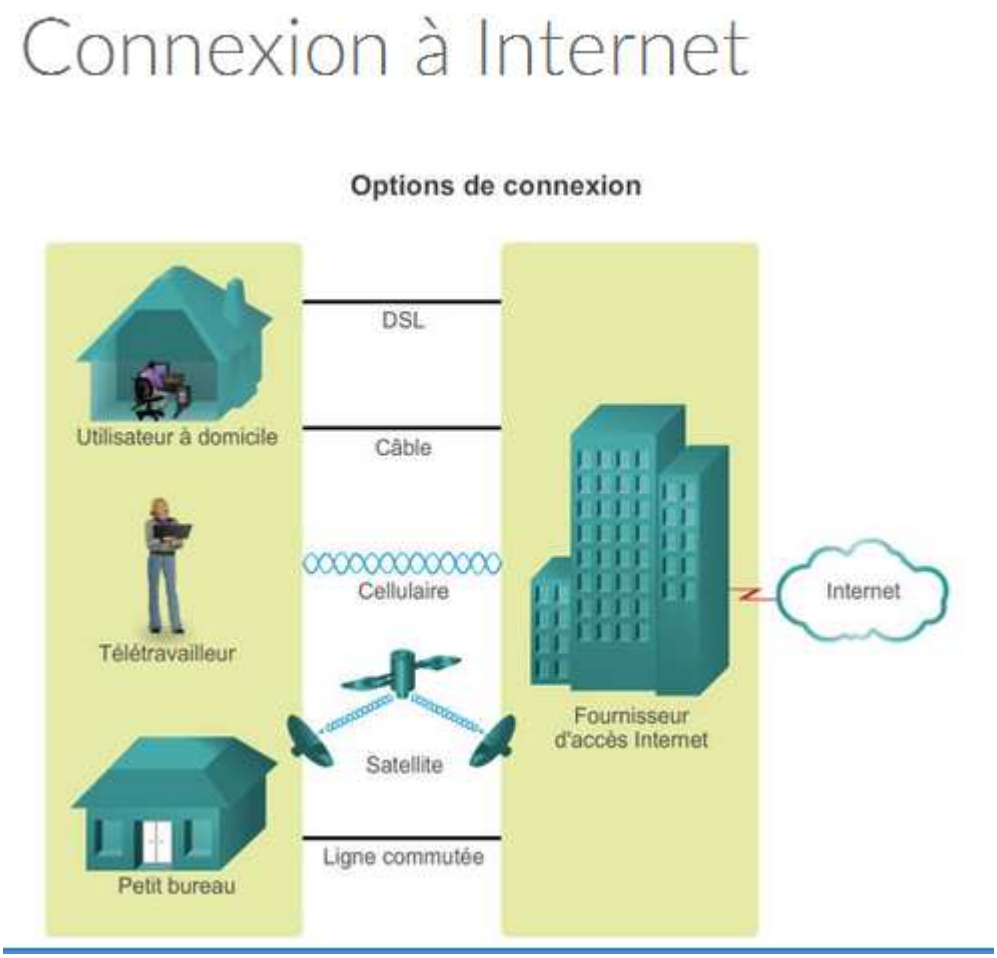
Internet



Internet est le réseau des réseaux.

Internet interconnecte les réseaux locaux, et de façon plus large, le monde. Ce lien est rendu possible par la présence de liens mondiaux, notamment les câbles sous-marins que nous avons abordé en début de module.

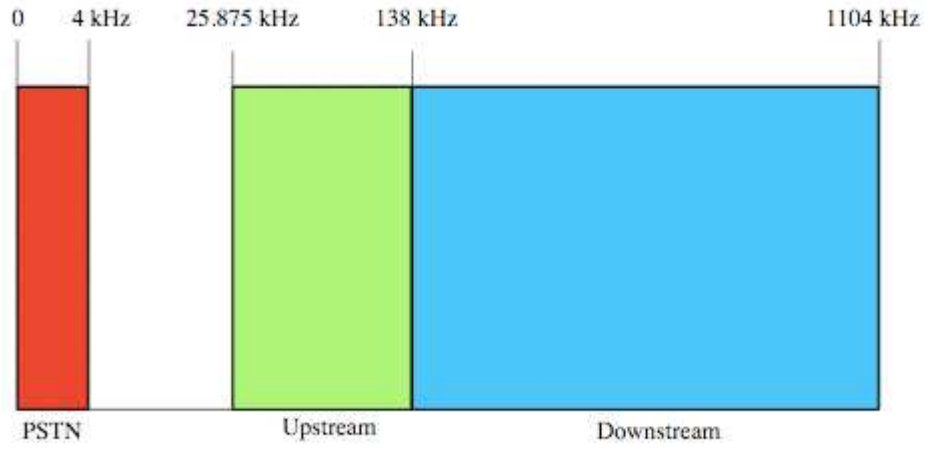
Internet est un média universel connecté par les opérateurs. Le rôle de ces opérateurs est de faire transiter l'information de sa source à sa destination, sans aucun traitement particulier, que cela soit en termes de priorité ou de contenu. On appelle ce principe la **neutralité du Net.**



Plusieurs options sont disponibles pour connecter un domicile ou une entreprise à Internet.

Parmi les plus fréquents en France, l'installation d'une ligne ADSL qui utilise la ligne cuivre support France Télécom pour se connecter au réseau de l'opérateur. Ce qui a permis son essor en France et dans le monde est la capacité de cette technologie à s'intégrer aux lignes téléphoniques traditionnelles sans y apporter des changements physiques importants côté utilisateur.

Dans le détail, l'isolation des signaux se fait par modulation de fréquence pour séparer le réseau téléphonique traditionnel (**en rouge**), le signal montant (**en vert**) et le signal descendant (**en bleu**).



Source : Wikipédia

L'inconvénient de cette technologie est que le débit exploitable de la ligne dépend fortement de la longueur de la ligne, entre le domicile de l'abonné et le répartiteur opérateur, nommé DSLAM (*Digital Subscriber Line Access Multiplexer*). Plus la ligne est longue, plus le signal est atténué. Par conséquence, le débit de synchronisation devient moins important.

Bien que des techniques ont été développées pour supporter une plus grande bande passante pour les lignes dites courtes, c'est à dire proche du répartiteur, la ligne ne peut pas être longue de plus de 5 kilomètres pour supporter l'usage de ces technologies.

L'abonné peut également choisir de se connecter à Internet via le support câble, avec un câblo-opérateur.

Dans les zones où ces technologies ne sont pas supportées, l'utilisateur peut se connecter à Internet via les réseaux satellite, cellulaires ou plus rarement, avec une ligne commutée et un modem classique.

Règles pour communiquer entre humains

Imaginez un monde où chacun parlerait son propre langage et selon ses propres règles. Il serait très difficile de communiquer ensemble et de se comprendre.

Nous avons établi, depuis les premières intéractions humaines des moyens standardisés pour communiquer entre humains.

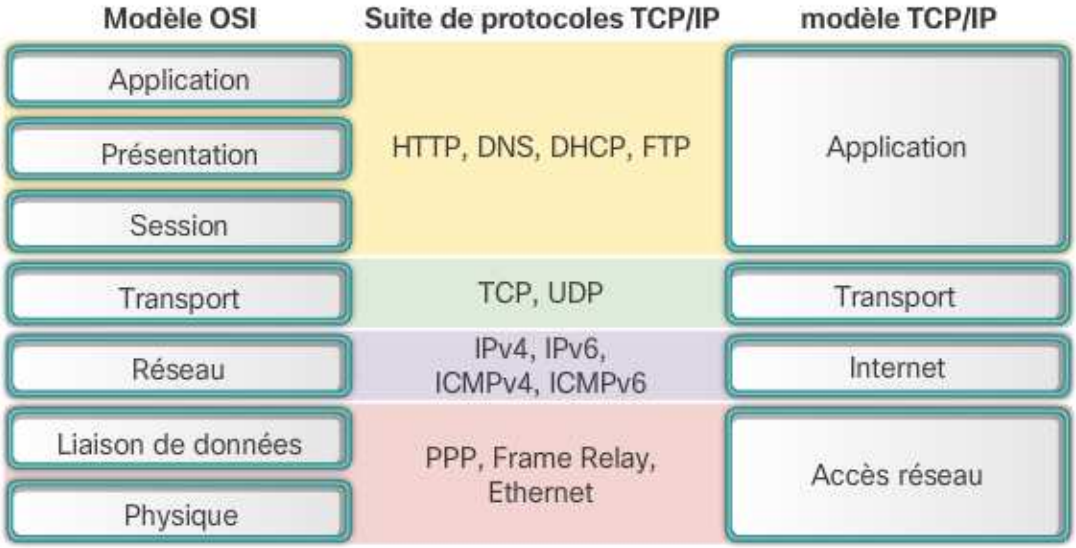
Sans même parfois en avoir conscience, nous obéissons aux paramètres suivants quand nous communiquons :

- Expéditeur et destinataire identifiés
- Mode de communication (face-à-face, lettre, photographie, ...)
- Même langue et syntaxe
- Vitesse et rythme d'élocution
- Confirmation que le message a bien été reçu ou accusé de réception

Ainsi, quand nous nous adressons à quelqu'un, nous utilisons un algorithme pour communiquer avec cette personne.

1. Nous annoncons au destinataire que nous allons lui communiquer une information
2. Le destinataire est en attente de votre message
3. Vous commencez à parler. En parlant, vous émettez un signal physique qui sera reçu grâce à l'écoute du destinataire
4. Votre message est interprété par votre destinataire
5. Vous pouvez vous assurer que le message a bien été reçu, en demandant par exemple au destinataire de répéter l'information

Modèle TCP/IP et OSI



On utilise souvent un modèle sous forme de couches, tel que le modèle TCP/IP pour aider à visualiser l'interaction entre les différents protocoles. Ce modèle illustre le fonctionnement des protocoles intervenant dans chaque couche, ainsi que leur interaction avec les couches supérieures et inférieures.

L'utilisation d'un modèle en couches présente certains avantages pour décrire des protocoles et des opérations sur un réseau. L'utilisation d'un modèle en couches :

- Aide à la conception d'un protocole, car des protocoles qui fonctionnent à un niveau de couche spécifique disposent d'informations définies à partir desquelles ils agissent, ainsi que d'une interface définie par rapport aux couches supérieures et inférieures.

- Il encourage la concurrence, car les produits de différents fournisseurs peuvent fonctionner ensemble.

- Il permet d'éviter que des changements technologiques ou fonctionnels dans une couche ne se répercutent sur d'autres couches, supérieures et inférieures.

- Il fournit un langage commun pour décrire les fonctions et les fonctionnalités réseau.

Il existe deux types de modèles de réseau de base :

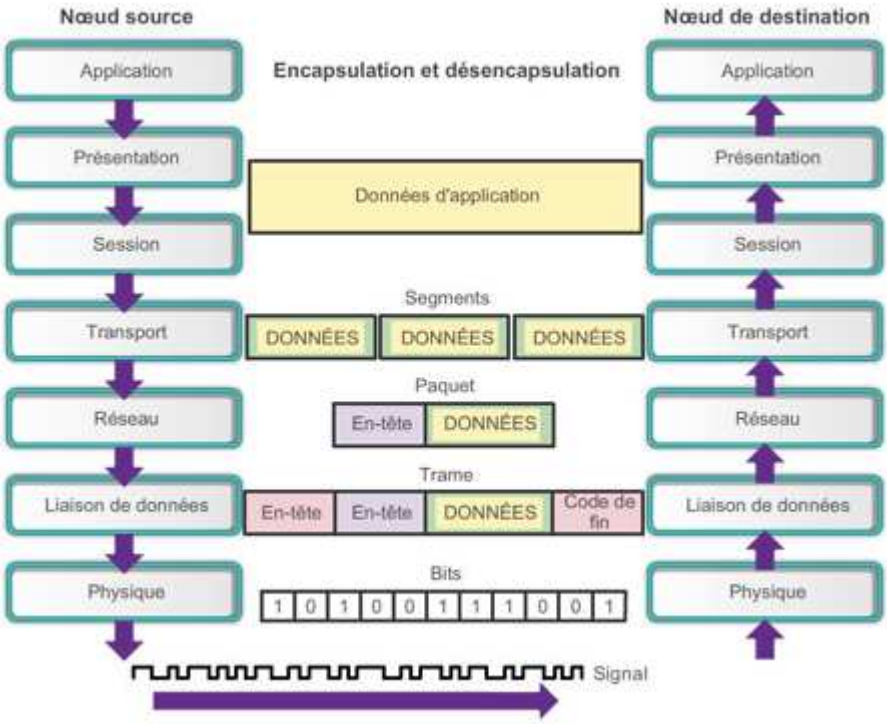
- **Le modèle de protocole**, qui suit la structure d'une suite de protocoles donnée. L'ensemble hiérarchique des protocoles associés dans une suite représente généralement toutes les fonctionnalités requises à l'interface entre le réseau humain et le réseau de données. Le modèle TCP/IP est un modèle de protocole, car il décrit les fonctions qui interviennent à chaque couche des protocoles au sein de la suite TCP/IP.

- **Le modèle de référence** assure la cohérence de tous les types de protocoles et services réseau en décrivant les opérations à effectuer à chaque couche, mais n'indique pas leur mise en œuvre. Un modèle de référence n'est pas destiné à être une spécification d'implémentation, ni à fournir un niveau de détail suffisant pour définir précisément les services de l'architecture réseau. Le principal objectif d'un modèle de référence est d'assurer une compréhension plus claire des fonctions et des processus impliqués.

Le modèle OSI (*Open Systems Interconnection*) est le modèle de référence interréseau le plus connu. Il est utilisé pour la conception de réseaux de données, des spécifications d'opérations et la résolution des problèmes.

Comme l'illustre la figure, les modèles OSI et TCP/IP sont les principaux modèles utilisés en matière de fonctionnalités réseau. Les concepteurs des protocoles, services ou périphériques réseau peuvent créer leurs propres modèles représentant leurs produits. Enfin, les concepteurs doivent communiquer avec l'industrie en associant leurs produits ou leurs services aux modèles OSI ou TCP/IP ou aux deux.

Envoi des données du client au serveur



La collaboration des couches du modèle TCP/IP et OSI pour transmettre l'information de l'application éméttrice de l'information jusqu'à l'application destinataire est essentielle et s'organise autour de deux processus : **l'encapsulation** et la **désencapsulation.**

L'encapsulation

L'encapsulation a pour but de préparer une information **avant** son envoi sur un réseau.

Ainsi, l'information applicative est **transformée** successivement dans les formats suivants :

1. **Segments** (à la couche 4, Transport)
2. **Paquet** (à la couche 3)
3. **Trame** (à la couche 2)
4. **Bits** (à la couche 1)

Comme discuté précédemment dans ce cours, la création d'un **segment** part de la segmentation de l'information envoyée. Une fois l'information segmentée, une en-tête de niveau 4 est ajoutée, formant le segment. Les informations de l'en-tête serviront au destinataire pour intérpréter les segments reçus, les réordonner dans le bon ordre et router l'information vers la bonne application.

La création d'un **paquet** est realisée en ajoutant une en-tête de niveau 3, contenant notamment l'adresse IP de la source et du destinataire.

La création d'une **trame** est réalisée en encadrant les informations précédentes autour d'une en-tête et d'une fin de trame. On y rajoute ici si nécessaire, les informations contenant la source et la destination de l'information, au niveau 2, comme les adresses MAC pour **Ethernet**.

La trame est ensuite transmise sur le réseau sous forme de bits.

La désencapsulation

Une fois l'information reçue par le destinataire commence le processus de désencapsulation, qui consiste à **traiter** la donnée reçue.

Le destinataire va lire successivement la trame, paquet, segment avant de délivrer l'information à l'application destinataire. À chaque étape de ce processus, le destinataire peut effectuer des vérifications pour s'assurer de l'intégrité de l'information et la destination de celle-ci.

Couche 2 - **Liaison de données**

- vérification de l'intégrité de la trame
- vérification du destinataire de la trame

Couche 3 - **Réseau**

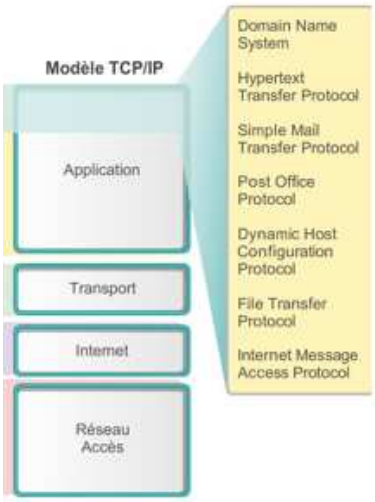
- vérification du destinataire du paquet
- vérification de l'intégrité de l'en-tête réseau

Couche 4 - **Transport**

- vérification de l'intégrité du segment
- réordonnancement et reconstitution de l'information segmentée
- renvoi de l'information si des segments manquent ou sont corrumpus

Successivement, le destinataire enlève les en-têtes de couches pour à la fin, ne délivrer que l'information à destination de l'application cible.

Couche Application



La couche **Application** fournit l'interface entre les applications que nous utilisons pour communiquer et le réseau sous-jacent par lequel nos messages sont transmis. Les protocoles de couche application sont utilisés pour échanger des données entre les programmes s'exécutant sur les hôtes source et de destination.

Un des protocoles application les plus connus est **HTTP** (*Hypertext Transfer Protocol*). Il permet le plus souvent à l'utilisateur de consulter des pages locales ou publiques, à l'aide d'un navigateur web, comme Firefox.

Dans le modèle OSI, cette couche se divise en trois :

- couche **application**
- couche **presentation**
- couche **session**

La couche **présentation** remplit trois fonctions principales :

- Codage et conversion des données de la couche application
- Compression des données
- Chiffrement des données pour la transmission et déchiffrement de celles reçues par le périphérique de destination.

La couche **session** est responsable des tâches suivantes :

- Crée et gère les communications entre les applications source et de destination
- Gère l'échange d'informations pour initier les dialogues, les maintenir actifs et redémarrer les sessions si nécessaire

Couche Transport

La couche **Transport** permet aux données applicatives d'être traitées pour faciliter leur transport sur le réseau.

Cette couche a les responsabilités suivantes :

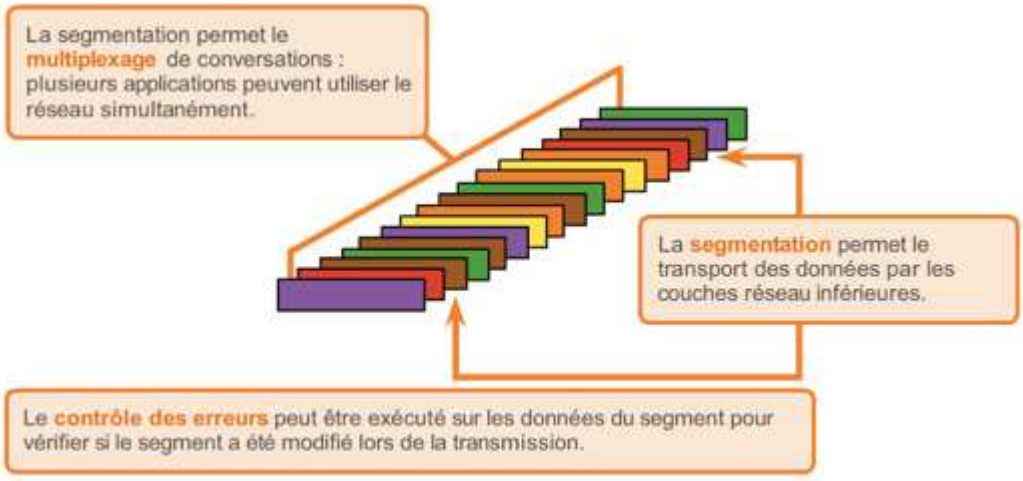
- Segmentation des données
- Réassemblage de segments
- Fiabilisation de l'échange de données
- Contrôle de flux
- Lien entre une application et une communication réseau

Segmentation des données

La couche **Transport** segmente les données en provenance de la couche application pour favoriser le **multiplexage** de l'information.

Le multiplexage consiste à mélanger les flux applicatifs pour permettre à chaque application qui souhaite transmettre d'éviter d'attendre qu'une communication soit terminée pour transmettre à son tour. Les informations étant découpées en segments, on ne transfère donc pas la donnée entière en une seule fois, on transfère un segment concernant l'application A, puis B et ainsi de suite. Jusqu'au moment où le dernier segment de l'information est envoyé par l'application.

Grâce à ce mécanisme, plusieurs applications peuvent communiquer de façon simultanée sur le réseau. Sans ce mécanisme, vous ne seriez pas capable de consulter une page web en communiquant en même temps avec une autre personne sur un logiciel de visioconférence.



Les couches inférieures (Internet / Accès Réseau) utiliseront ces segments pour continuer l'envoi de l'information sur le réseau.

Réassemblage de segments

Les segments envoyés sur le réseau n'ont pas la garantie d'arriver dans l'ordre au destinataire.

Or, le reassemblage d'une donnée ne peut se faire que dans l'ordre dans laquelle elle a été segmentée pour éviter la corruption de données.

Si le protocole de couche implémente cette fonctionnalité, en l'occurrence TCP, les segments sont numérotés pour garantir le reassemblage de l'information correct par la couche Transport lors de la réception de l'information par le destinataire. Nous aborderons TCP dans le détail dans les pages suivantes.

Fiabilisation de l'échange de données

Cette couche permet également de fiabiliser l'échange de données, selon le protocole utilisé.

Un segment perdu entre la source et le destinataire peut ainsi être renvoyé, sans pour autant renvoyer tous les segments échangés concernant l'information segmentée.

Là aussi, le protocole de couche TCP implémente cette fiabilité.

De plus, la couche Transport est également capable de détecter des altérations de segmen durant l'envoi de l'information sur le réseau. Ainsi, un segment corrompu pourra également être envoyé à nouveau au destinataire si nécessaire.

Contrôle de flux

Le contrôle de flux permet de convenir d'une vitesse convenable d'envoi et de réception entre l'expéditeur et le destinataire.

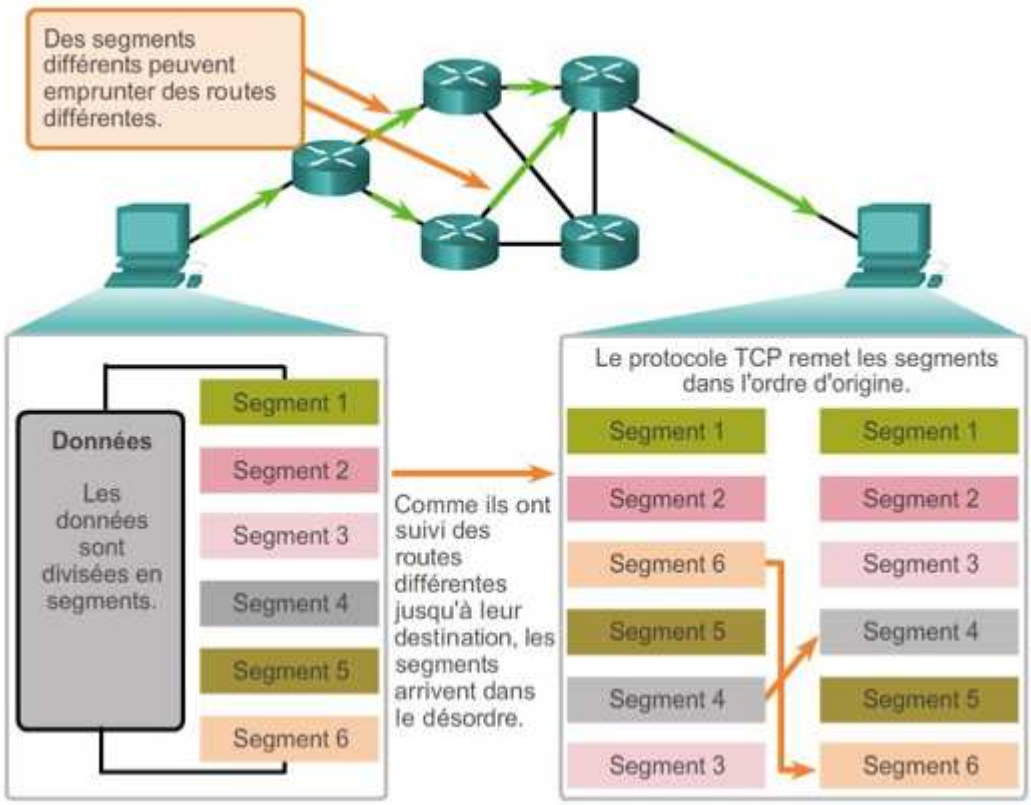
Cela permet ainsi à un expéditeur de ne pas surcharger le destinataire, avec une information envoyée à une vitesse trop rapide.

Identification d'un flux applicatif

Un flux est décrit comme une communication applicative unique entre un client et un serveur.

Quand vous communiquez avec un serveur web, vous ouvrez un flux entre votre ordinateur et le serveur. Quand vous envoyez un message électronique, vous ouvrez un autre flux.

Grâce aux **numéros de ports** présents dans l'en-tête de cette couche, les postes source et destinataire peuvent identifier le **flux** d'application lié à l'échange et ainsi délivrer l'information à l'application concernée.



TCP est un protocole **orienté connexion.**

Cela signifie qu'avant tout échange de données, les ordinateurs souhaitant échanger des données doivent **établir** une connexion. Lorsque l'échange de données est terminé, la connexion entre ces deux entités est alors **stoppée**.

Les ordinateur utilisent des instructions pour communiquer leur souhait de mettre en place ou de terminer une connexion à travers 3 étapes successives, nommées couramment le ***three-way handshake (connexion en trois étapes).***

Au délà de ces mécanismes, TCP implémente pleinement les mécanismes de fiabilité de transfert de l'information. Ainsi, cela permet de :

- **Assurer l'expéditeur que l'information a bien été reçue par le destinataire**
  - Le destinataire envoie des accusés de réception pour les informations reçues
  - En cas de non-réception, le destinataire demande à l'expéditeur de lui envoyer une nouvelle copie de ce segment.

- **Assurer l'expéditeur que l'information a été reçue dans le même état qu'envoyé**
  - Lors de la réception, le client calcule la somme de contrôle(checksum) du segment. Il la compare ensuite à la valeur contenue dans l'en-tête TCP l'intégrité du segment. Si les deux valeurs correspondent, le segment est considéré comme intact.
  - En cas de corruption du segment, le destinataire demande à l'expéditeur de lui envoyer un nouvel exemplaire de ce segment.

- **Reassembler les données dans l'ordre dans lequel elles ont été segmentées**
  - Même si les segments ne sont pas reçus dans l'ordre, TCP va ici ordonner les segments avant de pouvoir envoyer les données à la couche application.
  - Cela implique également que TCP doit **attendre** d'avoir reçu tous les segments de la donnée **avant** de la réorganiser et la transférer à la couche application.

- **Contrôler le flux d'information pour éviter que l'expéditeur envoie la donnée trop vite au destinataire**

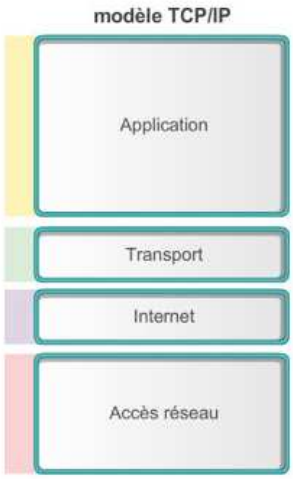
Le protocole TCP est utilisé lorsque l'on veut garantir une délivrance exacte des données, au prix de la surcharge de traitement liée notamment aux mécanismes de fiabilité.

Il est par exemple utilisé pour le protocole permettant aux utilisateurs d'afficher des pages à l'aide d'un navigateur web, HTTP.

UDP

UDP est très utilisé dans les communications voix à travers IP (VoIP), pour les jeux en ligne ainsi que pour les appels vidéos en ligne

Couche réseau / Internet



La couche **réseau** (appelée **Internet** dans le modèle TCP/IP) implémente le protocole Internet Protocol, aussi appelé couramment avec son équivalent abregé, **IP**.

La couche réseau a les rôles suivants :

- Adressage des périphériques finaux
- Encapsulation
- Routage
- Désencapsulation

La couche r**éseau** permet d'identifier la source et la destination de l'information, par le biais des adresses IP **source** et **destination**. Il est donc normal que chaque poste communiquant sur un réseau possède sa propre adresse IP locale ou globale.

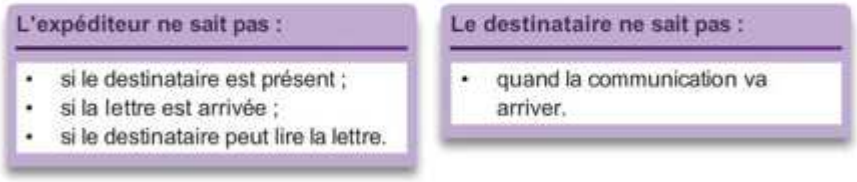
Lors d'une communication, les adresses IP **source** et **destination** présentes dans l'en-tête du paquet restent intactes et ne sont modifiées en aucun cas durant la transmission de l'information.

Si la communication devrait sortir du réseau local, les routeurs (*qui, rappelez-vous, interconnectent les réseaux*) examineront l'adresse IP de destination pour router le paquet vers la bonne direction. Une fois cette information obtenue, chaque routeur prendra sa **décision de routage** en fonction du

contenu de sa **table de routage,** c'est à dire du chemin le plus efficace dont il dispose pour s'approcher de la destination.

<u>Exemple avec La Poste</u>

Une lettre est envoyée.



Imaginez que l'adresse IP source soit l'expéditeur d'une lettre et que l'adresse IP de destination soit le destinataire de votre lettre.

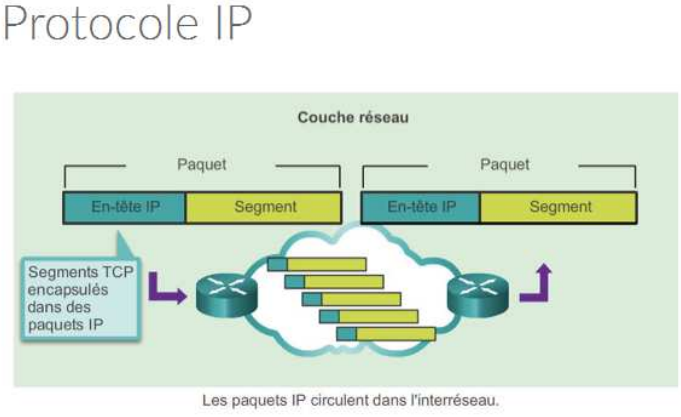
Avant d'envoyer votre lettre, vous identifiez clairement la source et la destination du message en la mentionnant sur l'enveloppe d'envoi.

Lorsque vous postez votre lettre, vous déléguez en quelque sorte l'activité de "routage" et de délivrance de la lettre à La Poste.

Dans le processus de routage de votre courrier, quelle information regarde le service postal pour router votre courrier vers sa destination? **L'adresse du destinataire !**

En outre, il serait étrange que La Poste modifie, en cours de transmission, l'adresse de l'expéditeur ou du destinataire. De plus, vous le voyez bien, le travail de La Poste n'est pas de **modifier** ces informations mais de s'en **servir** pour que votre courrier arrive à bon port.

Les mêmes principes s'appliquent ici à la couche **réseau**.



Les paquets IP circulent dans l'interréseau.

Le protocole IP (*Internet Protocol*) est le service de couche réseau mis en œuvre par la suite de protocoles TCP/IP.

Il a été conçu pour ne pas surcharger les réseaux. Il fournit uniquement les fonctions requises pour transférer un paquet d'une source à une destination en passant par un système interconnecté de réseaux. Ce protocole n'est pas destiné au suivi et à la gestion du flux de paquets. Ces fonctions sont effectuées par d'autres protocoles d'autres couches, si nécessaire.

Les principales caractéristiques du protocole IP sont les suivantes :

- **Sans connexion** – aucune connexion avec la destination n'est établie avant d'envoyer des paquets de données. La connexion sera gérée au niveau de la couche Transport si le protocole **TCP** est utilisé.

- **Acheminement au mieux (peu fiable)** – la livraison des paquets n'est pas garantie. Rappelez-vous à ce sujet que la fiabilité est implémentée au niveau de la couche Transport avec **TCP**, si nécessaire.

- **Indépendant du support** – le fonctionnement est indépendant du support transportant les données.

Notation binaire et théories

Les ordinateurs ne communiquent pas en utilisant un langage intelligible par l'homme. Ainsi, les ordinateurs communiquent, interprètent, traitent et exécutent en utilisant le langage binaire.

Dans les réseaux informatiques, le principe reste le même. Outre les mécanismes d'envoi et de réception de l'information, celle-ci est transmise en utilisant le codage binaire.

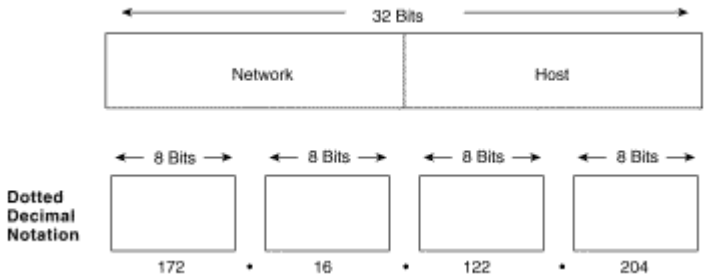
Basiquement, à quoi correspond la notation binaire ? Celle-ci est en réalité codée en utilisant l'élement le plus petit de cette notation, **un bit.** Un bit peut prendre deux valeurs, **0 ou 1**.

Comme vous vous en doutez, cette valeur unique n'a pas de sens sans une application plus précise. Par exemple, pour la taille d'un fichier, nous ne comptons pas en **bits** mais en **octets**.

Un **octet** est un groupe de **8 bits,** qui peuvent, eux aussi, prendre une valeur individuelle de **0 ou 1**. Un octet peut ainsi être codé en **256** combinaisons différentes, soit l'équivalent de 2^8, qui se lit ***2*** **exposant** ***8*** ou ***2*** **à la puissance** ***8*** (le nombre de bits composant un octet).

La valeur décimale d'un octet peut être évaluée à l'aide des rangs de puissance de 2.

Adresse IP



Une adresse IPv4 est composée de **4 octets**, chacun donc composés de **8 bits**. Elle est donc codée au total sur **32 bits.**

Celle-ci permet aux ordinateurs de posséder une adresse pour identifier la source et la destination d'un message. Elle permet également aux équipements intermédiaires, comme les routeurs, de relayer l'information jusqu'au destinataire.

Comme vous l'avez vu dans la page précédente, un octet peut prendre une valeur décimale de 0 à 255, ce qui est également le cas des quatre octets qui composent une adresse IP.

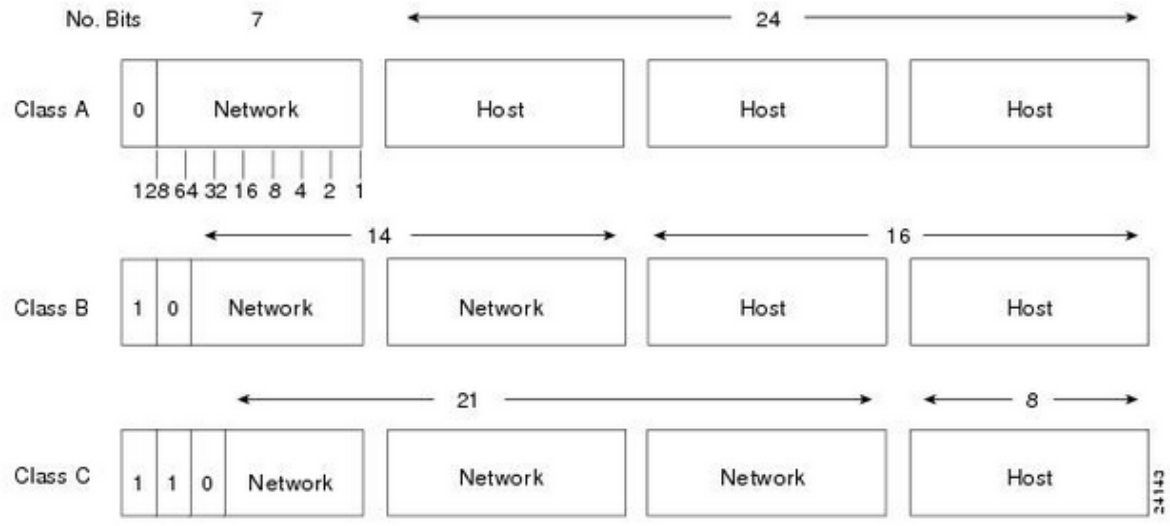
En notation décimale, une adresse est souvent notée à l'aide de la valeur décimale de chaque octet, séparée d'un point. Par exemple, l'adresse suivante :

192.168.1.1

Cependant, une adresse IP ne suffit plus pour identifier l'étendue précise d'un réseau.

Découvrons dans la page suivante le deuxième élement qui est souvent lié à l'adresse IP !

Masque de sous-réseau



De nos jours, une adresse IP seule n'a pas beaucoup de signification. Un masque de sous-réseau est utilisé pour identifier la partie **réseau** et la partie **hôte** d'une adresse IP.

La partie **réseau** identifie le réseau local configuré et utilisé par les postes. La partie **hôte** correspond aux adresses utilisées par les hôtes sur ce réseau pour communiquer.

La partié **réseau** est déterminée grâce au masque de sous-réseau, lui aussi codé sur **4 octets** et donc **32 bits.**

Un masque de sous-réseau se représente sous la forme suivante :

255.255.255.0

Cette information permet à l'ordinateur de déterminer si la communication qu'il va effectuer s'adresse à un hôte local ou à un hôte qui ne se trouve pas sur son propre réseau local.

La comparaison s'effectue de la façon suivante :

- L'hôte compare la partie **réseau** de son adresse assignée avec celle du destinataire du message
    - Si il y a correspondance, **le message est envoyé sur le réseau local**
    - **Si il n'y a pas correspondance, l'hôte considère que le destinataire du message se trouve en dehors de son réseau local. Il adresse donc l'information à sa passerelle par défaut.**

En fonction de la destination du message, le comportement de l'expéditeur du message ne sera donc pas le même.

Si l'on reprend notre exemple de masque de sous-réseau, les périphériques considèreront que les autres adresses IP, dont les trois premiers octets ont une valeur identique à son adresse IP, comme faisant partie intégrante du même sous-réseau. **Pourquoi ?** Tout simplement car le dernier octet du masque à une valeur décimale de 0, signifiant que cet octet peut varier de 0 à 255 sans pour autant sortir du sous-réseau d'origine.

Obtention d'une adresse IP

Les informations d'adresse IP peuvent être entrées manuellement sur le PC, ou attribuées automatiquement à l'aide du protocole DHCP (*Dynamic Host Configuration Protocol*). Le protocole DHCP permet aux périphériques finaux de disposer d'informations IP configurées automatiquement.

Le protocole DHCP est une technologie utilisée sur presque tous les réseaux d'entreprise. Le meilleur moyen de comprendre pourquoi le DHCP est tellement répandu est de prendre en compte tout le travail supplémentaire qui doit être effectué sans celui-ci.

Le protocole DHCP permet la configuration automatique des adresses IPv4 pour chaque périphérique final sur un réseau utilisant DHCP. Imaginez que chaque fois que vous vous connectez au réseau, vous devez entrer manuellement l'adresse IP, le masque de sous-réseau, la passerelle par défaut, et le serveur DNS. Multipliez cette opération par le nombre d'utilisateurs et de périphériques sur le réseau : vous avez saisi le problème.

Le protocole DHCP est un exemple de technologie fonctionnant de manière optimale. L'un des principaux objectifs de toute technologie est de faciliter les opérations. Grâce au protocole DHCP,

les utilisateurs entrent dans la zone couverte par un réseau donné, connectent un câble Ethernet ou activent une connexion sans fil, et les informations IPv4 nécessaires à la communication sur le réseau leur sont attribuées automatiquement.

Comme l'illustre la figure, pour configurer le protocole DHCP sur un ordinateur Windows, vous devez sélectionner « Obtenir une adresse IP automatiquement » et « Obtenir les adresses des serveurs DNS automatiquement ». Votre ordinateur reçoit automatiquement les informations en provenance d'un pool d'adresses IP et les informations IP associées sont configurées sur le serveur DHCP.

Il est possible d'afficher les paramètres de configuration IP d'un PC Windows à l'aide de la commande **ipconfig** à l'invite de commande. Le résultat affiche l'adresse IP, le masque de sous-réseau et la passerelle que le PC a reçu du serveur DHCP.

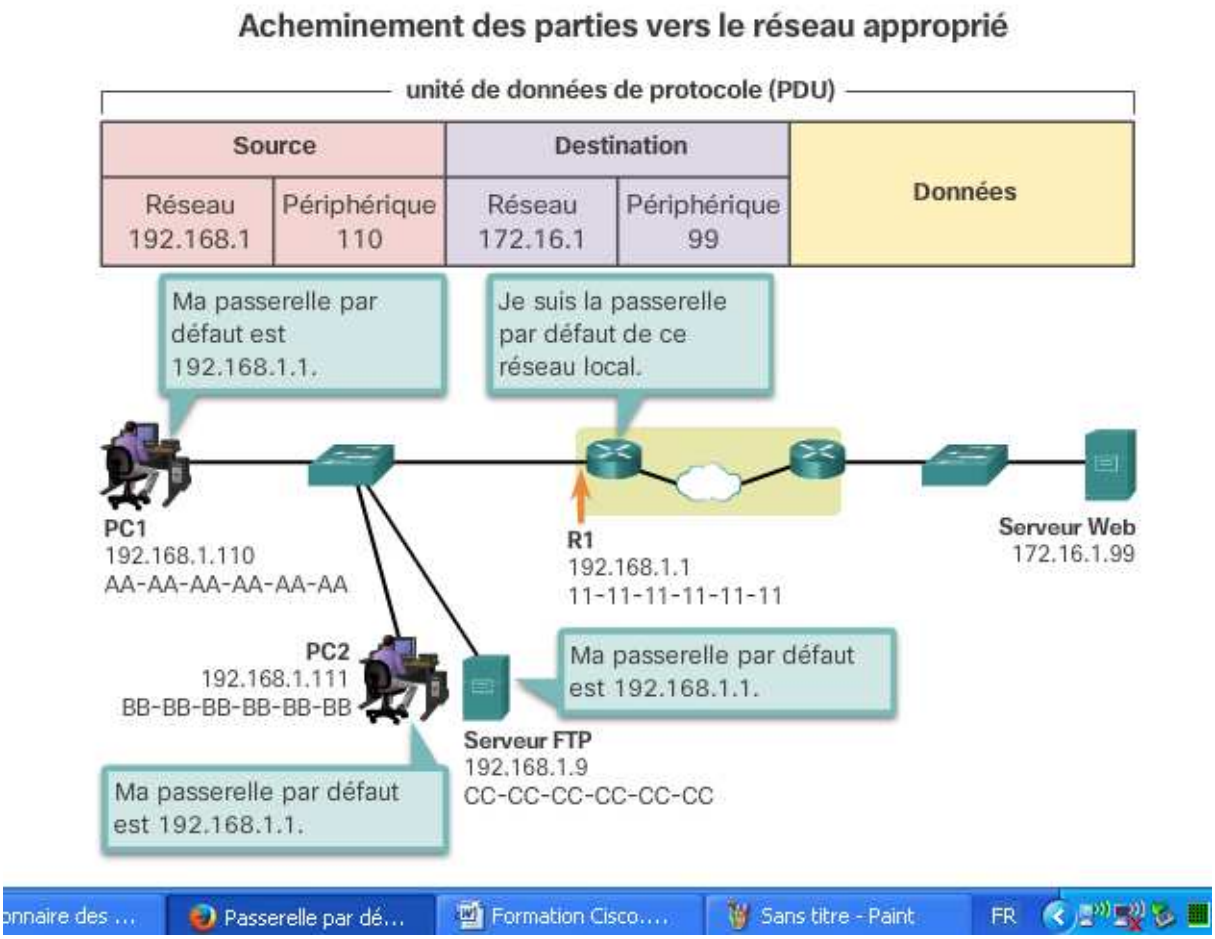
masque de sous-réseau de son ordinateur

Pré-requis : avoir un ordinateur exécutant Windows 7 ou supérieur

Etapes de l'activité :

1. Connectez-vous à l'ordinateur
2. Appuyez sur les touches + R pour lancer la console d'exécution puis tapez la commande **cmd**
3. La console devrait s'afficher. Saisissez alors la commande **ipconfig** pour afficher les paramètres réseaux de votre ordinateur.

Passerelle par défaut



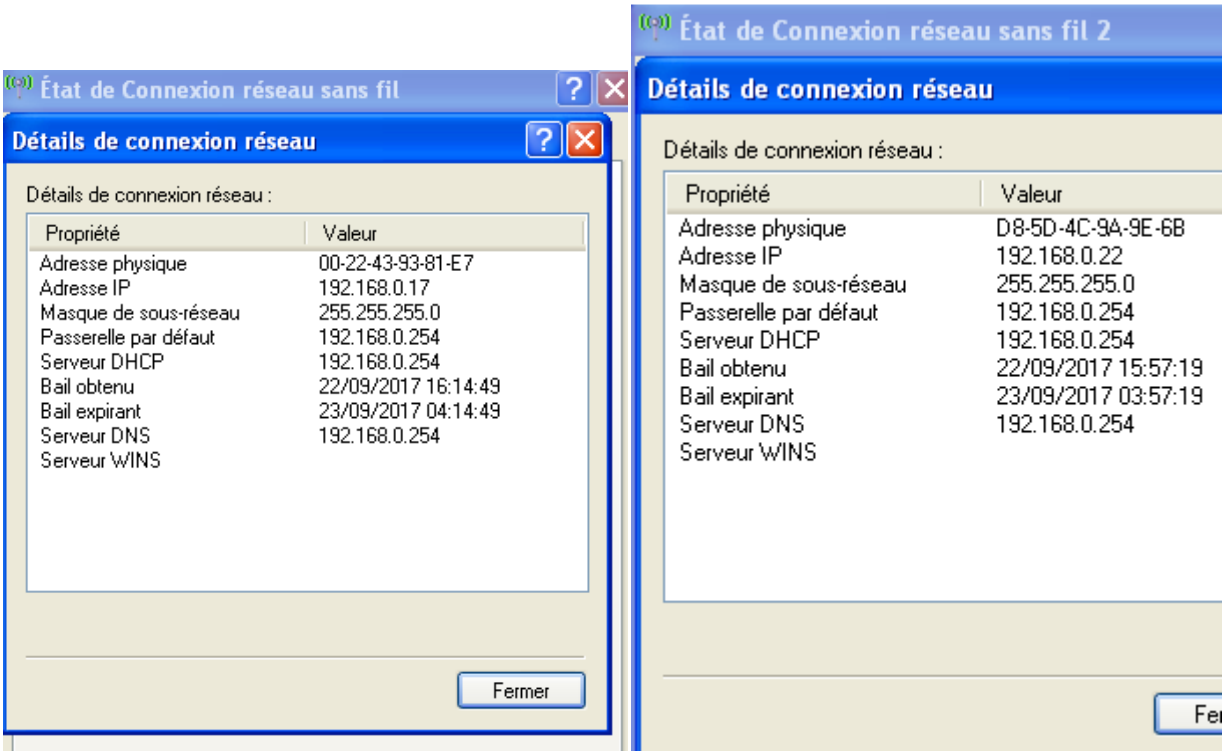
La méthode utilisée par un hôte pour envoyer des messages à une destination sur un réseau distant est différente de celle qu'il utilise pour envoyer des messages à une destination sur le même réseau local. Lorsqu'un hôte doit envoyer un message à un autre hôte du même réseau, il transfère directement le message. Un hôte utilisera le protocole ARP pour connaître l'adresse MAC de l'hôte de destination. Il inclut l'adresse IP de destination dans l'en-tête du paquet et encapsule le paquet dans une trame contenant l'adresse MAC de la destination, puis le transfère.

Lorsqu'un hôte doit envoyer un message à un réseau distant, il doit utiliser le routeur, également appelé « passerelle par défaut ». La passerelle par défaut est l'adresse IP d'une interface d'un routeur se trouvant sur le même réseau que l'hôte expéditeur.

Il est important que l'adresse de la passerelle par défaut soit configurée sur chaque hôte du réseau local. Si aucune adresse de passerelle par défaut n'est configurée dans les paramètres TCP/IP de l'hôte ou si une passerelle par défaut incorrecte est spécifiée, les messages adressés aux hôtes des réseaux distants ne peuvent pas être acheminés.

Sur la figure, les hôtes du réseau local utilisent R1 comme passerelle par défaut et son adresse 192.168.1.1 est configurée dans leurs paramètres TCP/IP. Si la destination d'une unité de données de protocole se trouve sur un autre réseau IP, les hôtes envoient les unités de données de protocole à la passerelle par défaut sur le routeur qui devra à son tour les transmettre.

Usuellement, dans un réseau domestique, la passerelle par défaut est le routeur de l'opérateur Internet, désignée de façon générique par le mot "box".



Activité : Vérifier que l'ordinateur peut contacter sa passerelle

Pré-requis : avoir un ordinateur exécutant Windows 7 ou supérieur

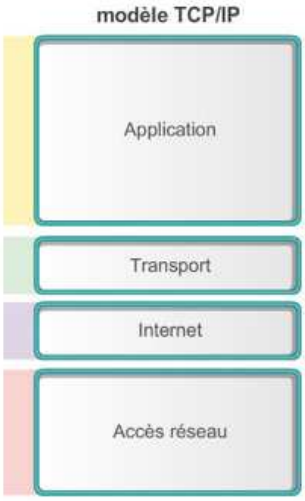
Etapes de l'activité :

1. Connectez-vous à l'ordinateur

2. Appuyez sur les touches + R pour lancer la console d'exécution puis tapez la commande **cmd**
3. La console devrait s'afficher. Saisissez alors la commande **ping X.X.X.X** (où les X sont remplacés par l'adresse IP de votre passerelle par défaut).

```
C:\Documents and Settings\benmrad>ping 192.168.0.254

Envoi d'une requête 'ping' sur 192.168.0.254 avec 32 octets de données :

Réponse de 192.168.0.254 : octets=32 temps=10 ms TTL=64
Réponse de 192.168.0.254 : octets=32 temps=2 ms TTL=64
Réponse de 192.168.0.254 : octets=32 temps=3 ms TTL=64
Réponse de 192.168.0.254 : octets=32 temps=8 ms TTL=64

Statistiques Ping pour 192.168.0.254:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 2ms, Maximum = 10ms, Moyenne = 5ms

C:\Documents and Settings\benmrad>_
```

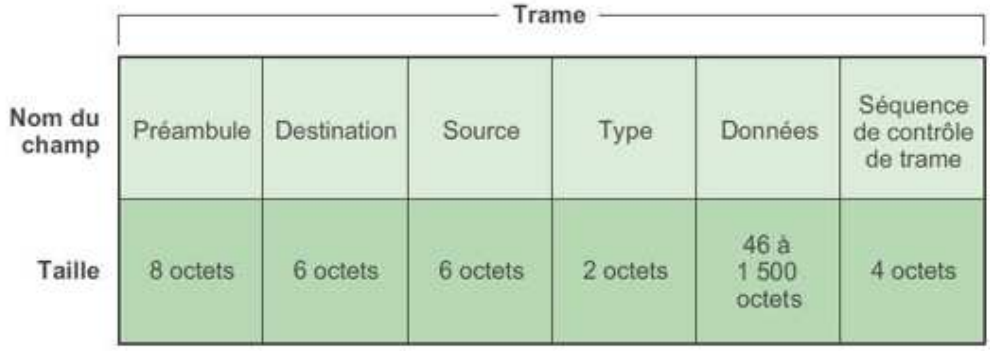
Couche Accès Réseau



La couche d'accès réseau du modèle TCP/IP représente dans le modèle OSI deux couches séparées, la couche **Liaison de données** et la couche **Physique**.

La couche **Liaison de données** a pour responsabilité de préparer l'envoi des données à travers le média de transmission. Selon le protocole et le média utilisé, le résultat du traitement de cette couche, la trame, peut être formatée de façon différente. Celle-ci a également le rôle de délimiter l'information envoyée des méthodes de signalement utilisées pour signaler le début et la fin de la trame transmise.

Par exemple, un élément envoyé sur un réseau local utilisera majoritairement la norme **Ethernet.**



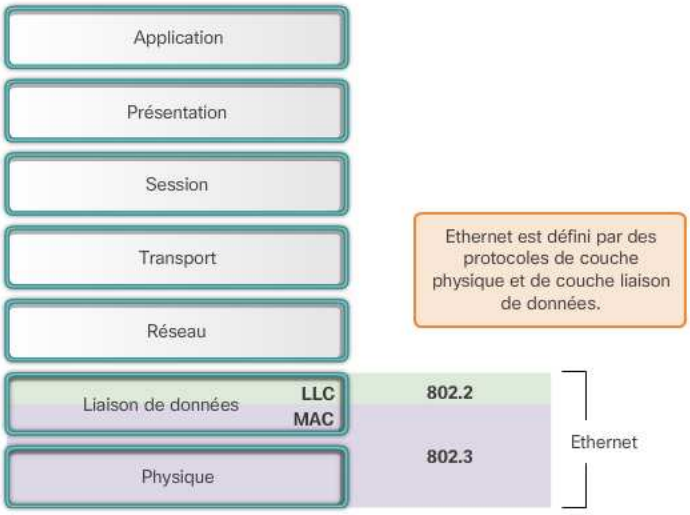
Cette couche assure également l'intégrité de l'information envoyée, ainsi que de sa destination.

Le poste destinataire de l'information est ainsi capable avec **Ethernet** de vérifier l'intégrité de l'information transmise, à l'aide d'un mécanisme de vérification de sommes de contrôle.

Également, si le protocole utilisé est **Ethernet**, le poste destinataire pourra identifier si l'information lui est destiné ou non et d'où celle-ci provient, grâce aux adresses de couche 2 liées au protocole Ethernet, **les adresses MAC.**

La couche **Physique** est responsable de transmettre la trame, convertie en bits à travers le média de transmission.

ETHERNET



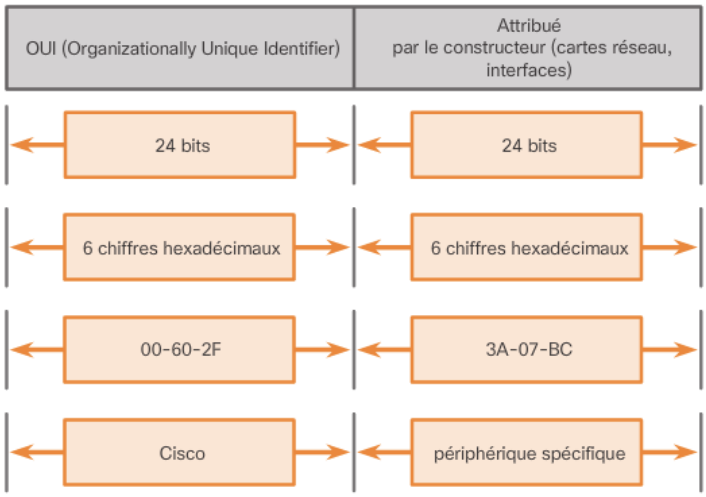
Ethernet est la technologie LAN la plus répandue aujourd'hui.

Ethernet fonctionne au niveau de la couche liaison de données et de la couche physique. Ethernet est une famille de technologies réseau définies par les normes IEEE 802.2 et 802.3. Ethernet prend en charge des bandes passantes de données de :

- 10 Mbit/s
- 100 Mbit/s
- 1 000 Mbit/s (1 Gbit/s)
- 10 000 Mbit/s (10 Gbit/s)
- 40 000 Mbit/s (40 Gbit/s)
- 100 000 Mbit/s (100 Gbit/s)

Comme illustré à la Figure 1, les normes Ethernet définissent à la fois les protocoles de la couche 2 et les technologies de la couche 1 du modèle OSI. Pour les protocoles de couche 2 du modèle OSI, tout comme pour chacune des normes IEEE 802, Ethernet s'appuie sur les deux sous-couches distinctes de la couche liaison de données pour fonctionner : les sous-couches LLC et MAC.

Adresses MAC



Comme nous l'avons vu précédemment, la topologie logique sous-jacente d'Ethernet est un bus à accès multiple. Chaque périphérique réseau est connecté au même support partagé et tous les nœuds reçoivent toutes les trames transmises.

La question est donc la suivante : si tous les périphériques reçoivent toutes les trames, comment chaque périphérique peut-il déterminer si elles lui sont destinées sans devoir passer par tout le processus de traitement et de désencapsulation pour accéder à l'adresse IP ? La question devient encore plus problématique dans les grands réseaux dont le volume de trafic est élevé et où un grand nombre de trames sont transférées.

Pour éviter la surcharge excessive liée au traitement de chaque trame, un identifiant unique appelé adresse MAC a été créé. Il permet d'identifier les nœuds source et de destination sur un réseau Ethernet. Quel que soit le type de réseau Ethernet utilisé, l'adressage MAC fournit une méthode d'identification des périphériques au niveau inférieur du modèle OSI. Vous vous souvenez sûrement que l'adressage MAC est ajouté dans l'unité de données de protocole de la couche 2. Une adresse MAC Ethernet est une valeur binaire de 48 bits constituée de 12 chiffres hexadécimaux (4 bits par chiffre hexadécimal).

Structure de l'adresse MAC

Les adresses MAC doivent être uniques au monde. La valeur de l'adresse MAC est un résultat direct des règles mises en application par l'IEEE auprès des revendeurs pour garantir l'attribution d'adresses uniques à chaque périphérique Ethernet, et ce, à l'échelle mondiale. Les règles établies par l'IEEE exigent de chaque revendeur de périphérique Ethernet qu'il s'enregistre auprès de l'IEEE. **L'IEEE attribue au constructeur un code de 3 octets (24 bits) appelé OUI (Organizationally Unique Identifier).**

L'IEEE demande aux constructeurs de respecter deux règles simples représentées sur la figure :

- Toutes les adresses MAC attribuées à une carte réseau ou à un autre périphérique Ethernet doivent utiliser, comme 3 premiers octets, l'identifiant OUI attribué au revendeur correspondant.

Toutes les adresses MAC qui ont le même identifiant OUI doivent recevoir une valeur unique (référence du revendeur ou numéro de série) dans les 3 derniers octets.

Décimal	Binaire				Hexadécimal
	8	4	2	1	
0	0	0	0	0	0
1	0	0	0	1	1
2	0	0	1	0	2
3	0	0	1	1	3
4	0	1	0	0	4
5	0	1	0	1	5
6	0	1	1	0	6
7	0	1	1	1	7
8	1	0	0	0	8
9	1	0	0	1	9
10	1	0	1	0	A
11	1	0	1	1	B
12	1	1	0	0	C
13	1	1	0	1	D
14	1	1	1	0	E
15	1	1	1	1	F

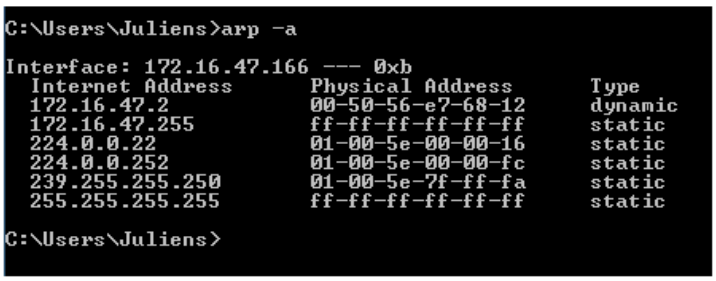
Activité : Identifier les associations MAC/IP du réseau local

Pré-requis : avoir un ordinateur exécutant Windows 7 ou supérieur

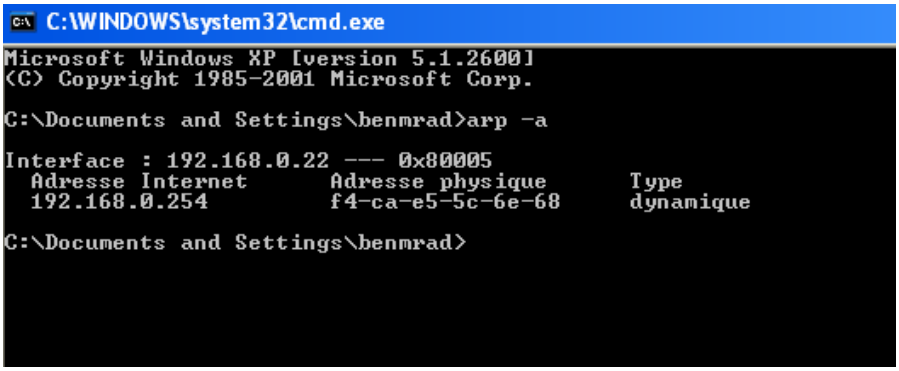
Etapes de l'activité :

1. Connectez-vous à l'ordinateur

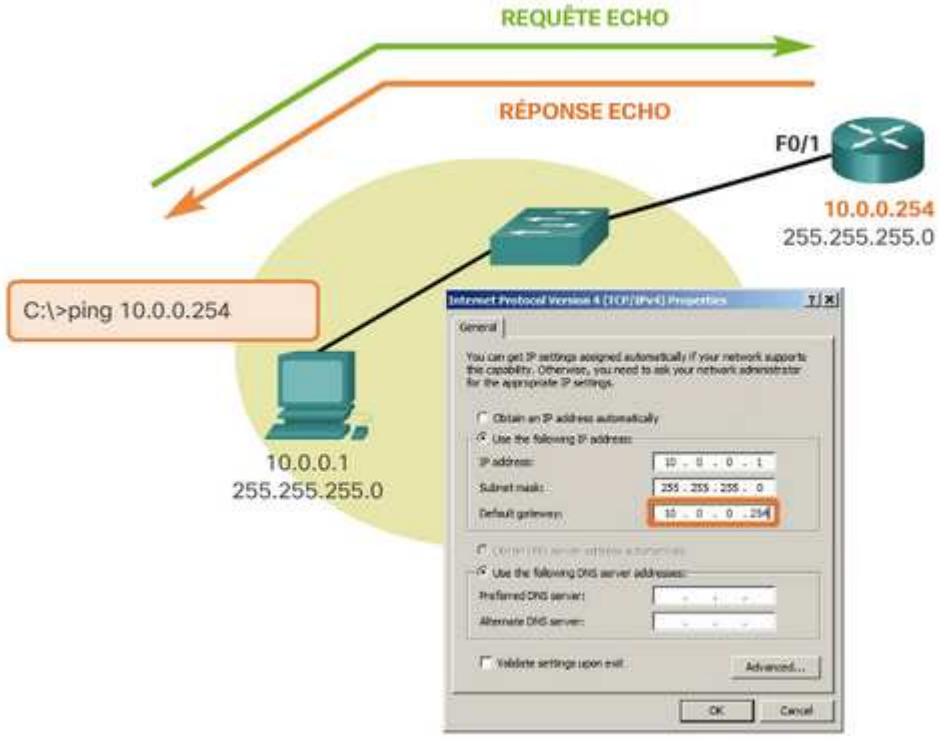
2. Appuyez sur les touches + R pour lancer la console d'exécution puis tapez la commande **cmd**
3. La console devrait s'afficher. Saisissez alors la commande **arp -a** pour afficher les associations d'adresses MAC avec les adresses IP correspondantes.



Dans cette capture, ainsi, on peut visualiser l'adresse MAC de la passerelle de l'ordinateur, **00-50-56-e7-68-12.** Cela signifie que l'ordinateur a réussi par le biais d'un protocole spécialisé (ARP) à obtenir cette information pour communiquer avec le périphérique.



Ping - Tester la connectivité au réseau local



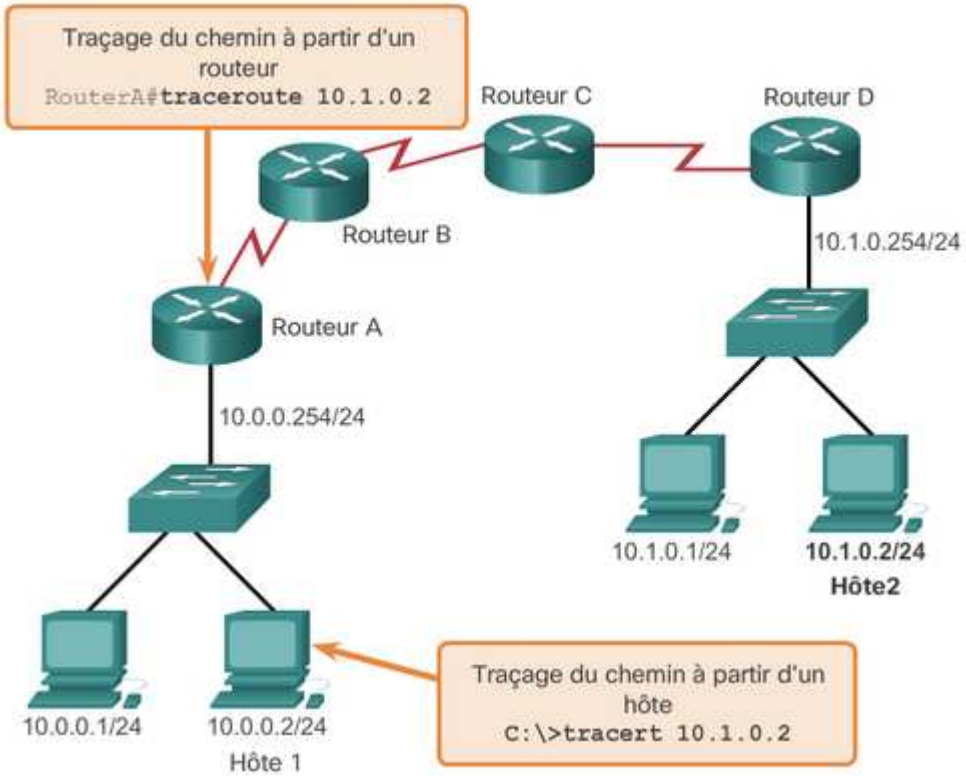
Vous pouvez également utiliser la commande ping pour tester la capacité d'un hôte à communiquer sur le réseau local. Cela consiste généralement à envoyer une requête ping à l'adresse IP de la passerelle de l'hôte. Une **requête ping à la passerelle indique que l'hôte et l'interface du routeur qui sert de passerelle sont fonctionnels (ou non) sur le réseau local.**

Pour ce test, l'adresse de la passerelle est souvent utilisée car le routeur est, en principe, toujours fonctionnel. Si l'adresse de la passerelle ne répond pas, une requête ping peut être envoyée à l'adresse IP d'un autre hôte sur le réseau local connu pour fonctionner.

Si une réponse est obtenue, soit de la passerelle, soit d'un autre hôte, cela signifie que les hôtes locaux peuvent communiquer sans problème sur le réseau local. Si la passerelle ne répond pas mais qu'un autre hôte répond, cela peut être révélateur d'un problème sur l'interface du routeur qui sert de passerelle.

Il se peut qu'une adresse de passerelle incorrecte ait été configurée sur l'hôte. Peut-être que l'interface du routeur est fonctionnelle, mais qu'une règle de sécurité en vigueur l'empêche de traiter des requêtes ping ou d'y répondre.

Traceroute - Tester le chemin



La commande **ping** permet de tester la connectivité entre deux hôtes, mais ne fournit pas d'informations sur les détails des périphériques entre les hôtes. Traceroute (**tracert**) est un utilitaire qui génère une liste de sauts qui ont été traversés sur le chemin. Cette liste peut fournir d'importantes informations pour la vérification et le dépannage. Si les données parviennent à destination, la commande affiche tous les routeurs situés entre les hôtes. Si les données restent bloquées au niveau d'un saut, l'adresse du dernier routeur ayant répondu à la commande peut fournir une indication sur l'endroit où se situe le problème ou sur d'éventuelles restrictions de sécurité.

Durée de transmission ou RTT (Round Trip Time)

L'exécution de la commande **traceroute** fournit la durée de transmission sur chacun des sauts rencontrés sur le chemin et indique si un saut n'a pas répondu. La durée de transmission correspond à la durée nécessaire à un paquet pour atteindre l'hôte distant, plus le temps mis par l'hôte pour répondre. Un astérisque (*) indique un paquet perdu ou sans réponse.

Cette information permet de localiser un routeur problématique sur le chemin. Si des temps de réponse longs ou des pertes de données caractérisent un saut particulier, cela indique que les ressources du routeur ou que ses connexions sont saturées.

Champs de durée de vie TTL IPv4 et limite de nombre de sauts IPv6

La commande traceroute utilise une fonction du champ de durée de vie TTL du protocole IPv4 et le champ de limite de nombre de sauts du protocole IPv6 dans les en-têtes de couche 3, ainsi que le message ICMP de dépassement de délai.

La première séquence des messages envoyés par traceroute contient un champ TTL de durée de vie égal à 1. Cela entraîne l'expiration du champ TTL de durée de vie du paquet IPv4 au niveau du premier routeur. Ce routeur répond ensuite en envoyant un message ICMPv4. L'utilitaire traceroute dispose à présent de l'adresse du premier saut.

Puis, il incrémente progressivement le champ TTL (2, 3, 4, etc.) pour chaque séquence de messages. Cela permet d'obtenir l'adresse de chaque saut, à mesure que les paquets expirent sur le chemin restant. Le champ TTL est incrémenté jusqu'à ce que la destination soit atteinte ou jusqu'à une valeur maximale prédéfinie.

Une fois que la destination finale est atteinte, l'hôte répond par un message ICMP Port Unreachable (port inaccessible) ou ICMP Echo Reply (réponse d'écho), à la place du message ICMP Time Exceeded (dépassement de délai).

Activité : Test de la latence réseau avec les commandes ping et traceroute

Pré-requis de l'activité : Un PC équipé de Windows 7, Vista ou XP, connecté à Internet

Etapes de l'activité :

1. Téléchargez le fichier PDF à l'aide du lien suivant
2. Suivez les étapes contenues dans le fichier
3. Répondez aux questions à la fin de chaque partie d'activité

Si vous le souhaitez, vous pouvez imprimer ce fichier pour plus de facilité.

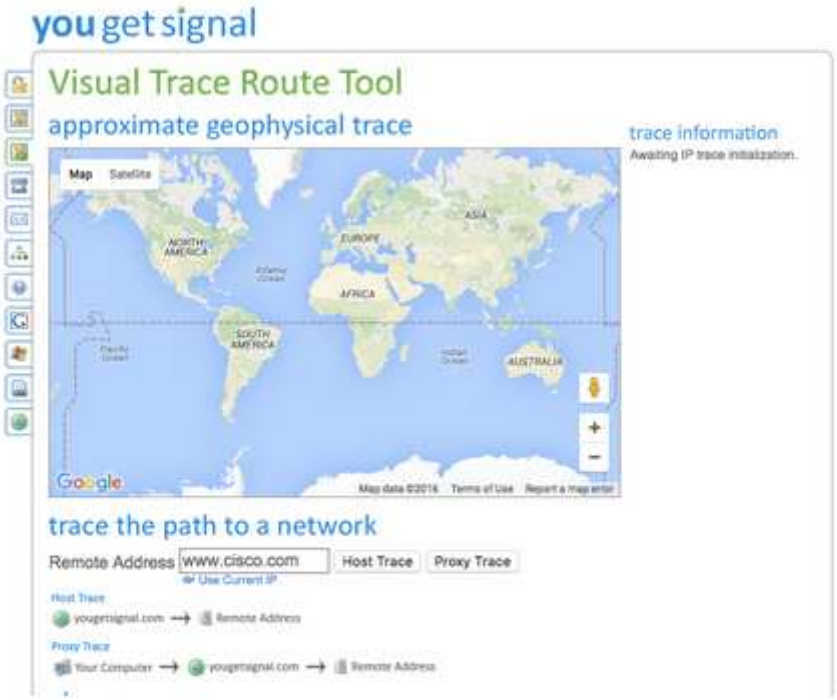
Activité : Visualiser par quel chemin l'information transite entre un serveur et une destination

Prérequis :

- Un ordinateur équipé d'un navigateur Internet

Etapes de l'activité :

1. Connectez vous sur le site suivant : http://www.yougetsignal.com/tools/visual-tracert/ (Liens vers un site externe.)Liens vers un site externe.



2. Saisissez le site de votre choix, par exemple, cisco.com

2. Saisissez le site de votre choix, par exemple, cisco.com (Liens vers un site externe.)Liens vers un site externe.

3. Puis, cliquez sur le bouton "Host Trace" pour commencer la trace.

4. Il s'affiche alors le chemin approximatif entre le serveur et la destination

Une fois cette activité realisée, répondez aux questions suivantes :

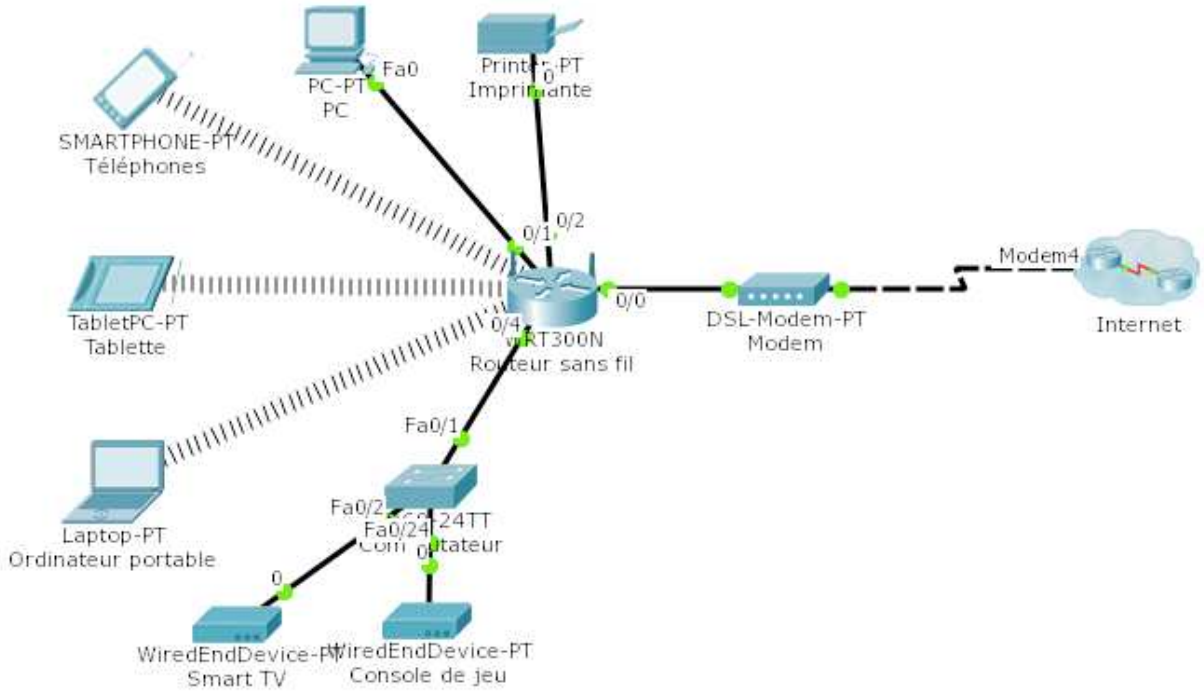
- **Question : Combien d'étapes se trouvent entre le serveur et la destination ?**
- **Question : En combien de temps la trace a pu être complétée ?**
- **Question bonus : Pourquoi la trace part des États-Unis et pas de France ?**
- Les supports de cours seront disponibles sur notre plateforme en ligne NetAcad.
- Vous pourrez ainsi délivrer le cours aux élèves en utilisant notre cours mais aussi notre plateforme NetSpace.
- La plateforme NetSpace vous permettra, entre autres, de communiquer avec les élèves, de planifier des examens, de réaliser vos propres évaluations et de moduler le parcours de formation en fonction des besoins des élèves.
- Pour votre information, la formation à l'utilisation de NetSpace sera fournie lors de la 3ème partie de formation de formateur en ligne.

Packet tracer

- Packet Tracer est notre outil de simulation réseau phare, déjà utilisé dans la plupart de nos cursus Cisco Networking Academy. Il est à la fois disponible pour les élèves et instructeurs du programme.
- Il permet aux instructeurs du monde entier de simuler des équipements divers et variés (routeurs, commutateurs, tablettes, smartphones, ...) dans le cadre de l'apprentissage des réseaux.
- Vous pourrez utiliser l’outil Packet Tracer en classe avec vos élèves.
- Afin de le télécharger et découvrir cet outil, merci de suivre le lien suivant.

- Pour information, un module de formation est prévu lors du 3ème module de formation de formateur.

Activités du Packet Tracer



Le but de cette partie est de vous familiariser avec l'outil Packet Tracer et comment appréhender les activités que vous allez offrir à vos étudiants en classe.

L'image que vous voyez ci-dessus représente la topologie typique d’un réseau domestique sur laquelle se basera cette première série d'exercices.

Activité 1 : Identifier les périphériques présents dans un réseau local

Pré-requis de l'activité : Packet Tracer 6.3 installé

Etapes de l'activité :

1. Ouvrez le fichier suivant : asterix_master_topology_FR.pkt
2. Visualiser la topologie réseau et les différents types de liens entre les équipements
3. Explorer les différents équipements en cliquant dessus
4. Une fois la fenêtre de configuration ouverte, vous pouvez explorer les différents onglets pour identifier la nature ainsi que la latitude de configuration de chaque équipement

Une fois cette activité terminée, répondez à ces questions :

Question : quelle est l'adresse IP de l'imprimante ?

Question : quelle est l'adresse IP de la passerelle par défaut de l'ordinateur portable ?

Question : quel est le masque de sous-réseau du réseau local ?

Question : quel est le mot de passe Wi-Fi du réseau sans-fil (SSID) nommé asterix ?

Activité 2 : Paramétrer les périphériques finaux

Pré-requis de l'activité : Packet Tracer 6.3 installé

Etapes de l'activité :

1. Ouvrez le fichier suivant : asterix_master_topology_FR_ACT2_Cisco.pkt
   Note : pour les besoins de cette activité, le routeur sans-fil a été remplacé par un routeur traditionnel

2. Cliquez sur le poste de travail fixe, nommé PC

3. Une fois la fenêtre de configuration ouverte, cliquez sur l'onglet **Desktop** puis sélectionnez l'option **IP Configuration.**

4. Définissez les paramètres suivants en mode **statique :**

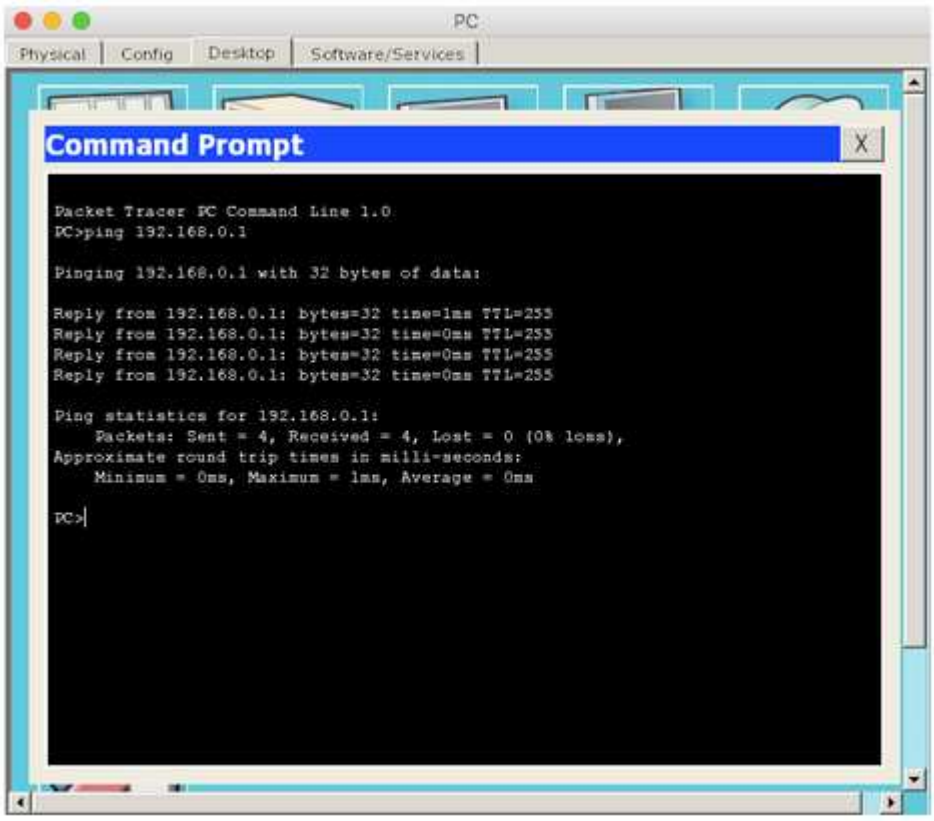
   - Adresse IP : 192.168.0.210
   - Masque de sous-réseau : 255.255.255.0
   - Passerelle par défaut : 192.168.0.1
   - Serveur de résolutions de noms (DNS) : 197.54.122.2

Fermez ensuite la fenêtre de configuration IP pour valider vos choix.

Pour vérifier l'application de vos paramètres, testons la connectivité à la passerelle par défaut à l'aide des manipulations suivantes :

1. Sélectionnez Command Prompt, dans la même fenêtre de configuration

2. Tapez la commande **ping 192.168.0.1.** Vous devriez obtenir le résultat suivant :



Une fois cette activité terminée, répondez à ces questions :

Question : pouvez-vous confirmer que le client a bien accès au serveur DNS. Comment ? Quel est le résultat ?

Question : modifiez la passerelle par défaut du client à la valeur 1.1.1.1 et essayez de pinger à nouveau le serveur DNS. Quel est le résultat ? Pouvez-vous l'expliquer ?

Question : arrivez-vous à pinger un autre membre du réseau local, comme par exemple l'ordinateur portable en laissant la passerelle par défaut à la valeur 1.1.1.1 ? Quel est le résultat ? Pouvez-vous l'expliquer ?

Question : essayez de modifier l'adresse IP à la valeur suivante : 192.256.1.1. Quel est le résultat ? Pouvez-vous l'expliquer ?

Activité 3 : Tester la connectivité au réseau

Pré-requis de l'activité : Packet Tracer 6.3 installé

Etapes de l'activité :

1. Ouvrez le fichier suivant : asterix_master_topology_FR.pkt

2. Dans la barre latérale droite, cliquez sur cet icône pour générer un test de connectivité (ping) entre deux équipements

3. Cliquez sur le PC en premier puis cliquez sur Internet, puis DNS

Vous avez ainsi disposé l'équivalent d'un ping entre ces deux équipements. Pour tester la connectivité, vous pouvez alors lancer ce dernier en cliquant sur le bouton présent en bas à droite.

Faites de même pour disposer un test de connectivité entre le PC et la tablette.

Vous devriez obtenir le résultat suivant :

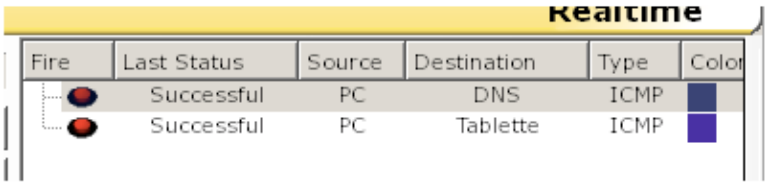
2. Dans la barre latérale droite, cliquez sur cet icône pour générer un test de connectivité (ping) entre deux équipements

3. Cliquez sur le PC en premier puis cliquez sur Internet, puis DNS

Vous avez ainsi disposé l'équivalent d'un ping entre ces deux équipements. Pour tester la connectivité, vous pouvez alors lancer ce dernier en cliquant sur le bouton présent en bas à droite.

Faites de même pour disposer un test de connectivité entre le PC et la tablette.

Vous devriez obtenir le résultat suivant :



Une fois cette activité terminée, répondez à ces questions :

Question : vous avez peut-être constaté que le test de connectivité n'a pas fonctionné aux premiers essais. Selon vous, pourquoi ?

Question : est-ce que cette manipulation assure une connectivité uni-directionnelle ou bidirectionnelle entre les équipements ? Justifiez.