

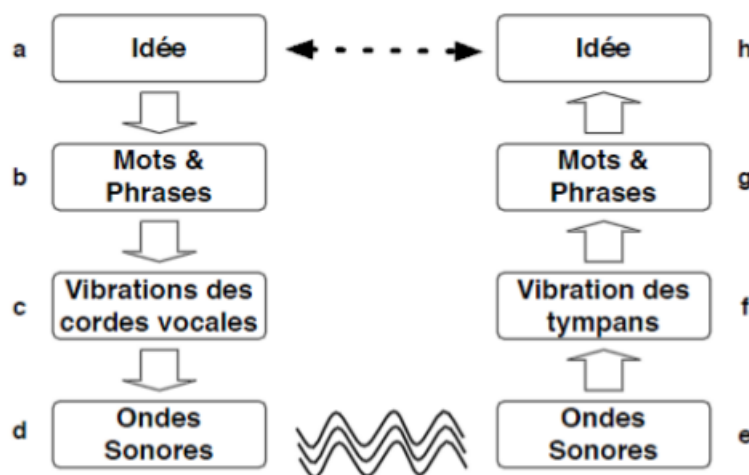
1 Introduction aux réseaux :

Un rappel :

- Un ordinateur manipule des informations diverses, représentées sous forme binaire c'est à dire : écrit au moyen d'un alphabet contenant seulement les chiffres 0 et 1, appelé **bit** = **binary digit**.
- Dans cet alphabet, les mots et les phrases représentant l'information s'écrivent sous forme de suites de bits. Ex : 0001011100010.
- On appellera ces informations binaires des données.
- Les fichiers sont des amas de bits cohérents représentant par exemple du texte, du son ou de l'image. Ex : mamusic.mp3, rapport.doc, readme.txt
- Les applications sont des programmes permettant aux internautes de transmettre des fichiers d'un ordinateur à l'autre. Exemple : les applications sont la partie visible d'Internet, que tout le monde connaît et utilise tous les jours. Le courriel, la navigation web, ou le chat sont des exemples d'applications.
- La transmission de fichiers : Les fichiers transmis peuvent être reçus quasiment instantanément à des dizaines de milliers de kilomètres de là.

La communication sur le réseau permet de transmettre des informations d'un ordinateur à un autre ordinateur en utilisant des techniques spécifiques avec un principe pas très différent de celui de la communication entre les êtres humains.

Communication entre êtres humains



Communication orale entre êtres humains

Les réseaux informatiques :

Quelques chiffres :

- Taille d'Internet - <http://www.isc.org/solutions/survey> + de 1200M d'hôtes en 2019 / le nombre a explosé avec les objets connectés
- Traffic sur Internet - <http://www.internetworldstats.com/stats.htm> - en 2019 : 2 200M d'utilisateurs (1000M en Asie, 500M en Europe, 270M aux US) - 5M de teraoctets (1012 octets) de données sur le Web (Eric Schmidt, the CEO of Google)

La classification des réseaux :






- LAN (Local Area Network) : à l'intérieur d'un immeuble, ou d'une superficie inférieure à 10 Kilomètres.
- MAN (Metropolitan Area Network) : circonscrit à une ville, comme par exemple, le réseau du métro.

- WAN (Wide Area Network) : au moins la dimension d'un pays, et englobent souvent la planète entière.
- CAN (Campus Area Network) : pour les campus universitaires (plusieurs immeubles, mais une surface de terrain limitée).
- TAN (Tiny Area Network) : réseaux domestiques, à la maison.
- RLE (Réseau Local d'Entreprise).

Le type d'organisation :

- Réseaux Terminaux / Grand Systèmes (Main Frame)
- Réseaux Postes à Postes (peer to peer ou d'égal à égal)
- Réseaux Clients/Serveurs

La topologie :

topologies	Schémas	Avantages	Inconvénients
Réseau maillé		Accès direct et non partagé à tous les noeuds	Couteux en nombre de liens à établir.
Bus		Simple et peu couteux. Tolère la panne des noeuds.	Beaucoup de collisions possibles
Etoile		Pas de collisions	Si le nœud central tombe en panne, il paralyse tout le réseau !
Anneau à jeton		Pas de collisions	Ordre arbitraire pour l'émission des messages
Arbre		Pas de collisions	Si le nœud racine tombe en panne, il paralyse la moitié du réseau !

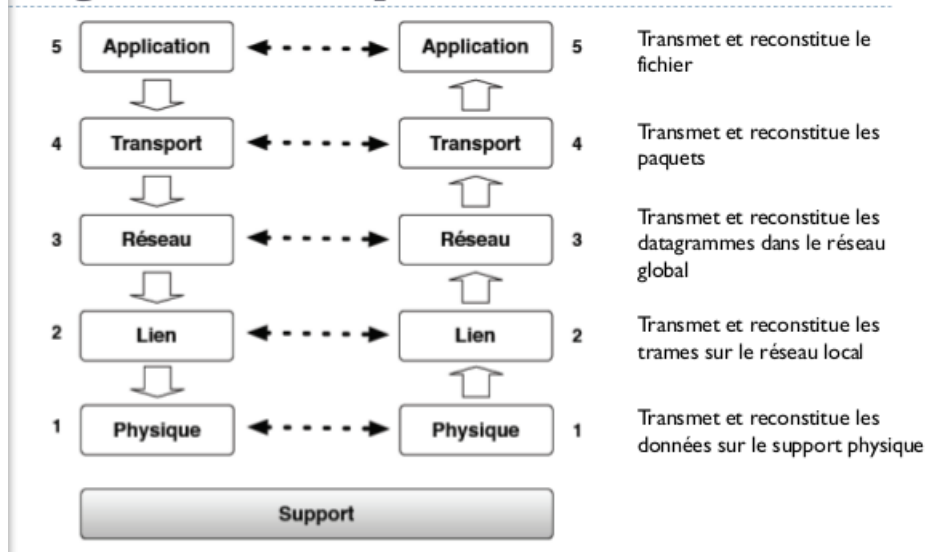
RETENIR : IL NE FAUT PAS CONFONDRE INTERNET \neq WEB :

Internet = interconnexion de réseaux de machines (réseau des réseaux) et

Web = données échangées sur internet via le protocole HTTP

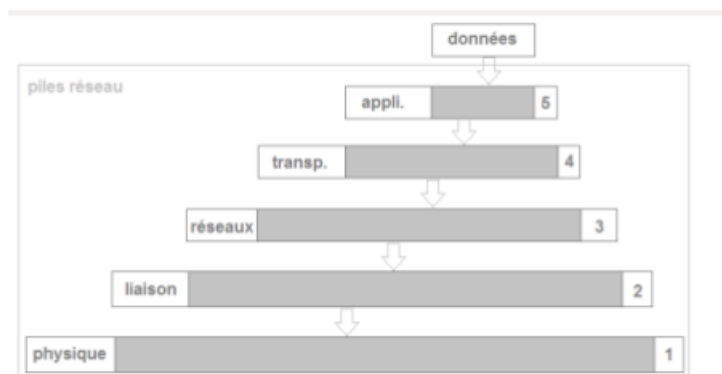
La communication entre ordinateurs utilise un empilement de couches, présentes sur chaque ordinateur du réseau. C'est une organisation en pile.

Organisation en pile

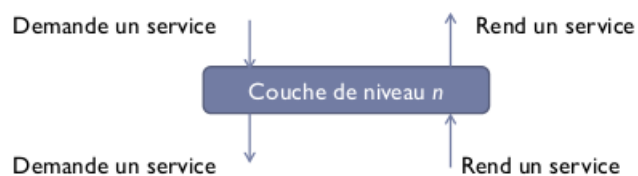


Encapsulation des trames :

A chaque niveau, on encapsule un en-tête et une fin de trame (message) qui comporte les informations nécessaires en suivant les règles définies par le protocole réseau employé.



Chaque couche semble communiquer avec la couche homologue du destinataire :



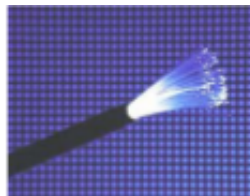
Le modèle de la couche OSI (7 couches) est une organisation « pédagogique », dans la pratique, les opérateurs de cœurs de réseaux ou autres utilisent leurs propres modèles. Voici par exemple une autre modélisation très utilisés :

Protocoles	Modèle TCP/IP	Modèle OSI
HTTP / FTP / POP / SMTP DNS / DHCP ...	Application	Application
		Présentation
		Session
TCP / UDP	Transport	Transport
IP / ARP / ICMP / IGMP	Internet	Réseau
Ethernet	Accès réseau	Liaison de donnée
		Physique

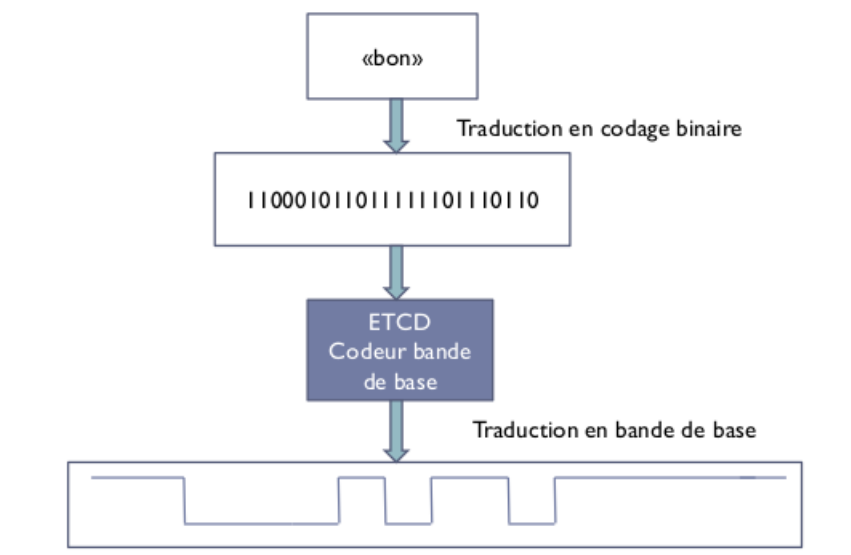
La couche physique :

La tâche accomplie par les protocoles de cette couche est le transfert individuel d'un 0 ou d'un 1 d'un bout à l'autre d'un support physique. Plusieurs types de supports physiques sont utilisés pour connecter les ordinateurs entre eux :

- des câbles métalliques véhiculant des électrons (supports filaires)
- des câbles optiques véhiculant des photons (fibres optiques)
- l'air véhiculant des ondes hertziennes (supports hertziens)



Exemple pour la couche physique :



Dans un monde idéal, les signaux sont fidèlement transmis de l'émetteur au récepteur. Dans la réalité, le signal peut être altéré. L'altération dépend du médium physique (cuivre, fibre, air).

SYNTHÈSE : LA COUCHE PHYSIQUE (NIV 1) S'OCCUPE DE TRANSMETTRE DES DONNÉES BINAIRES (0 OU 1) DIFFÉRENTS SUPPORTS PHYSIQUES EXISTENT (FILAIRE, AÉRIEN, OPTIQUE) IL FAUT UN ÉQUIPEMENT PHYSIQUE SPÉCIAL POUR ENVOYER LA DONNÉE ET LA DÉCODER À LA RÉCEPTION (EX : **modem = **mod**ULATEUR / **dem**ODULATEUR) UNE DONNÉE BINNAIRE PEUT ÊTRE PERDUE EN RAISON DES FAIBLESSES DE LA TRANSMISSION PHYSIQUE IL EXISTE DES TECHNIQUES SPÉCIFIQUES POUR PALLIER AUX DÉFAUTS DE TRANSMISSION.**

La couche lien - liaison de données :

La tâche accomplie par les protocoles de cette couche est de :

- transférer des paquets à travers le support physique
- identifier les ordinateurs directement connectés à ce support
- gérer le « temps de parole » de chacun sur le support.

Problème des collisions :

- 1 . Une solution pour gérer les collisions consiste à figer un ordre tournant que les ordinateurs doivent respecter pour que chacun puisse transmettre à son tour pendant un certain temps. Ex : chaque ordinateur peut parler pendant 2h par jour, à une heure fixe, chacun son tour. Cependant, cette solution centralisée a des inconvénients. Si l'on rajoute ou enlève des ordinateurs, il faut tout reprogrammer avec un nouvel ordre à respecter. Avec cet ordre systématique, on brime un ordinateur qui a soudainement beaucoup à transmettre si pendant ce temps-là les autres n'ont rien à dire.

- 2 . Une autre solution : **le protocole Ethernet** - Au milieu des années 70, aux Etats-Unis , protocole de liaison de données , norme internationale : ISO/IEC 8802-3

Il fonctionne en commutation de paquets : Segmente l'information en paquets de données, transmis indépendamment par les nœuds intermédiaires et ré-assemblés au niveau du destinataire.

Principe de fonctionnement (égalitaire) : Tous les nœuds partagent à égalité le même média. Toute information émise par un poste est reçue par tous les autres. Chaque ordinateur doit filtrer ce qui lui est destiné. Pendant que l'un des nœuds émet, toutes les machines du réseau doivent, de leur côté, observer le silence.

Lorsqu'un ordinateur veut envoyer des informations, il obéit à un algorithme commun (écoute du support, si occupé, renvoi suivant un temps aléatoire, après un nombre maxi d'essais, annoncer l'échec) à tous pour limiter les risques de collision.

Format de trame Ethernet (niv 2) :

Préambule (7 octets + 1 octet pour le délimiteur) // adresse destination (6 octets) // adresse source (6 octets) // longueur (taille totale la trame) // données (au moins 46 octets, au plus 1500 octets) // CRC (4 octets) : code de détection d'erreur



Les identifiants utilisés à la couche lien :

Chaque ordinateur possède un équipement réseau doté d'un identifiant. Le plus souvent, l'identifiant est une « **adresse MAC (Medium Access Control)** ». Une adresse MAC consiste en une suite de 48 bits, souvent notés de manière sous forme hexadécimale, dans un format regroupant des « mots » de 8 bits . Exemple 10 :93 :E9 :0A :42 :AC

L'en-tête des paquets envoyés par la couche lien comporte l'adresse MAC de l'ordinateur destinataire, ainsi que l'adresse MAC de l'ordinateur émetteur du paquet. **Une adresse MAC est unique et fournie par le constructeur.**

Connaître son adresse MAC :

- sur Windows : tapez ipconfig /all dans un terminal et chercher l'Adresse physique
- sur Linux : tapez ifconfig dans un terminal et chercher HWaddr

Il existe cependant une exception utile en pratique pour s'adresser à « tout le monde en même temps » . L'adresse de diffusion (broadcast) qui est toujours :

FF :FF :FF :FF :FF :FF

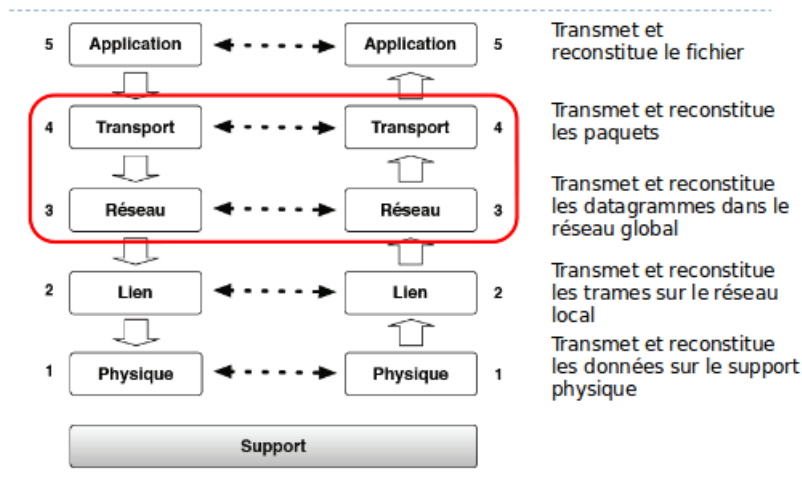
Équipements :

- **Concentrateur - hub** : permet de concentrer les flux Ethernet de plusieurs équipements sur un même support dans un réseau informatique local. Il tend à disparaître ! Chaque machine connectée transmet ses trames à tous les autres ports, ce qui induit un gros trafic. Il existe deux types de ports : les ports pour la connexion des machines et le port pour extension du réseau auquel se connecte un autre concentrateur.
- **Commutateur - switch** : Contrairement à un concentrateur, un commutateur ne reproduit pas sur tous les ports chaque trame qu'il reçoit. Il sait déterminer sur quel port il doit envoyer une trame, en fonction de l'adresse à laquelle cette trame est destinée. Les commutateurs sont souvent utilisés pour remplacer des concentrateurs car ils encombreront moins le réseau. Le nombre de ports Ethernet est variables entre 4 et plusieurs centaines.



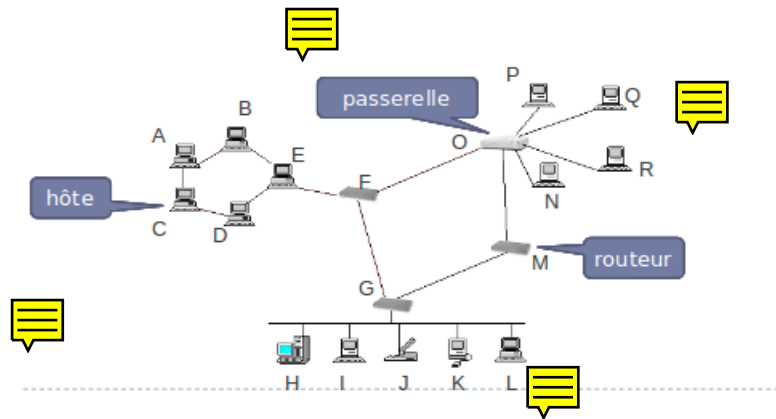
SYNTHÈSE : LA COUCHE LIAISON DE DONNÉES (NIV 2) TRANSFÈRE DES DONNÉES ENTRE DES NŒUDS SUR LE MÊME RÉSEAU LOCAL. LA COUCHE DE LIAISON DE DONNÉES PEUT DANS CERTAINS CAS DÉTECTER ET POTENTIELLEMENT CORRIGER LES ERREURS QUI PEUVENT SURVENIR AU NIVEAU DE LA COUCHE PHYSIQUE (NIV 1). CHAQUE NŒUD EST DOTÉ D'UN IDENTIFIANT UNIQUE MATÉRIEL. UN NŒUD PEUT ENVOYER UN MESSAGE À UN DESTINATAIRE EN PARTICULIER OU DIFFUSER À TOUS LES NŒUDS. IL EXISTE 2 TYPES DE MATÉRIELS LES CONCENTRATEURS (HUB) ET LES COMMUTATEURS (SWITCH).

2 Routage et transport :



Les objectifs de la couche réseau :

1. L'Adressage : comment identifier de façon unique une multitude d'équipements (plusieurs milliards) ? Il faut un encodage suffisamment grand mais pas trop non plus car il y aura une surcharge à chaque paquet. Avec n bits, on identifie 2^n machines. Soit si $n=32 \rightarrow 2^{32} = 4\,294\,967\,296 \approx 4,3$ milliards d'identifiants.
2. Le Routage : Pour acheminer un paquet d'une machine A vers une machine B, quelles informations doit connaître chaque nœud ? Comment faire si un nœud tombe en panne ?



L'hôte émet ou reçoit les messages. Le routeur sert d'intermédiaire dans la transmission d'un message. La passerelle (Gateway), routeur qui se trouve entre deux réseaux dépendant d'autorités différentes, comme entre le réseau local d'une entreprise et l'Internet. **Les routeurs Internet ne connaissent que les passerelles, pas les hôtes derrière la passerelle.**

Exemple : E veut envoyer un message $\langle m \rangle$ à L . 2 cas :

- $\langle m \rangle$ peut faire 3 bonds (E,F,G et L)
- 5 bonds (E,F,O,M,G et L)

Protocole de routage :

Le mécanisme par lequel des chemins sont sélectionnés dans un réseau pour acheminer les données d'un expéditeur jusqu'à un ou plusieurs destinataires. Il y a **plusieurs routes possibles** d'un hôte à un autre. Le routage doit tenir compte des **pannes éventuelles de routeur**. De nombreux algorithmes sont utilisés pour le routage suivant la localisation.

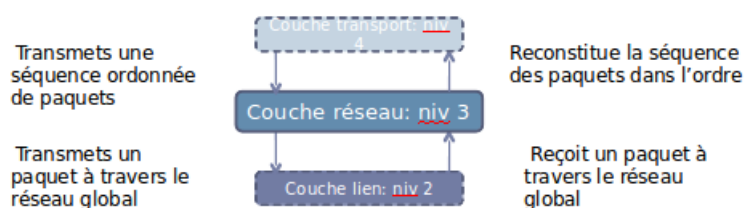
Le Protocole IP - Internet Protocol :

Couche 2 - lien : les adresses MAC, Ex : 10 :93 :e9 :0a :42 :ac , ne sont utilisées que dans le réseau local, pas sur internet, peuvent avoir des formats différents selon le support physique

@ mac \Rightarrow Adresse physique

Couche 3 - réseau : les adresses IP, format d'adresse indépendant des protocoles utilisés à la couche 2, valables à travers tout le réseau global, 32 bits = 4,3 Milliards d'identifiants. la notation décimale souvent usitée est sous forme de 4 mots de 8 bits X.X.X.X avec X compris entre 0 et 255, exemples : 216.239.59.104 et 127.0.0.1

@ ip \Rightarrow Adresse logique



Format d'un datagramme/paquet IPv4 :

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Version d'ID				Longueur de l'entête				Type de service								Longueur totale															
Identification								Flags								Paiement effectif															
Curtis de site								Protocole								Source de contrôle de l'entête															
Adresse source																Adresse destination															
Options et/ou remises en cause																															

La couche réseau a des limites :

- Certains paquets peuvent être perdus ou dupliqués.
- Elle ne fait pas la différence entre les applications qui s'exécutent sur une machine.

Principe du routage :

Pour trouver son chemin à travers le réseau de câbles et de liens radio connectant les ordinateurs entre eux, jusqu'à une destination identifiée par son adresse IP, il faut faire appel à un type de protocole supplémentaire, faisant également partie de la couche réseau : un protocole de routage.

Une table de routage est une sorte de "panneau indicateur" qui donne les routes (les réseaux) joignables à partir du "carrefour" que constitue un routeur. Les paquets arrivent sur une interface de la machine. Pour "router" le paquet, le routeur fondera sa décision en deux temps :

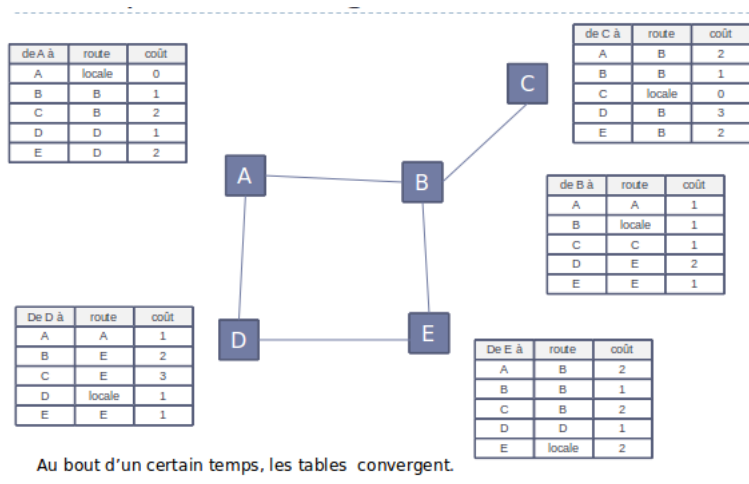
1. d'abord il regarde dans l'en-tête IP le réseau de destination et compare toutes les entrées dont il dispose dans sa table de routage.
2. Ensuite, si le réseau de destination est trouvé, il commute le paquet sur le bon port de sortie par contre si ce réseau n'est pas trouvé, le paquet est jeté!

Sur chaque routeur, une règle par nœud du réseau :

Règle : <pour aller à X, passer par Y, distance d>

Calcul des chemins optimaux : On observe les différents chemins possibles, on en déduit les chemins les plus courts, on les stocke dans une table de routage (= routage statique, simple, mais si on enlève ou ajoute des hôtes, il faut tout refaire!)

Un protocole de routage : IGP - Internet Global Protocol Il est basé sur l'**algorithme de Bellman-Ford** dont le principe est de Diffuser périodiquement à tous ses voisins un paquet spécial appelé HELLO contenant sa table de routage. La table de routage se remplit au fur et à mesure qu'il reçoit les tables de ses voisins (distance=1). Un routeur entend parler progressivement d'autres routeurs qui ne sont pas ses voisins, mais des voisins de ses voisins — les routeurs seront notés à distance de 2, puis 3, 4, etc ... dans les tables de routage des messages HELLO. Il peut ainsi répercuter ces nouvelles informations dans sa propre table de routage pour arriver à une convergence :



Avantages : Simple, Routeurs autonomes

Limitations : Convergent lentement. Dans certains cas le protocole dérègle durablement les tables de routage en ne détectant pas correctement qu'un ou plusieurs routeurs sont soudainement devenu hors-service, Sensible aux boucles, **La TTL ou durée de vie du**

paquet est décrémentée à chaque saut. **Le paquet est supprimé quand son TTL arrive à 0.**

De nombreux algorithmes de routage existent, en fin de cours, nous étudierons et implanterons 2 algorithmes qui sont au programme de terminale : RIP & OSPF.

À RETENIR : LES PROTOCOLES DE ROUTAGE ONT POUR FONCTION DE DÉCIDER SUR QUEL LIEN TRANSMETTRE UN PAQUET IP. CHAQUE NŒUD MAINTIENT UNE TABLE DE ROUTAGE CONTENANT DES LIGNES DE LA FORME : <POUR ALLER À X, PASSER PAR Y, DISTANCE D> .LA ROUTE QU'EMPRUNTE UN PAQUET PEUT ÊTRE DÉTERMINÉE **statiquement** : CHAQUE ROUTE EST ENTRÉE MANUELLEMENT PAR L'ADMINISTRATEUR RÉSEAU OU **dynamiquement** : LES NŒUDS DÉCOUVRENT INCRÉMENTALEMENT LEURS VOISINS PUIS LE RESTE DU RÉSEAU EN ÉCHANGÉANT LEUR TABLE DE ROUTAGE. CECI PERMET DE DÉTECTER LES PANNES DE ROUTEURS.

L'adressage IP : Une machine qui dispose de plusieurs interfaces raccordées à un réseau (un routeur par exemple) est dotée de plusieurs adresses IP, une par interface. 127.0.0.1 est l'adresse de rebouclage, sa propre carte ! Retenons donc qu'**IP fixe une adresse à une interface réseau et pas à une machine**. Depuis février 2011, la réserve d'adresse IPv4 est épuisée. Nous sommes passés aux adresses IPv6 sont sur 128 bits, soient 667 millions de milliards d'adresses par millimètre carré de surface terrestre ...

Une adresse IP est scindée en deux parties :

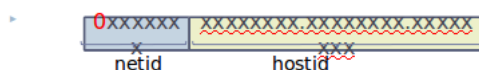
- Le préfix réseau - **netid** : il identifie un groupe de machine, généralement regroupées sur un même sous-réseau physique, l'adresse machine. Le préfix réseau associé à chaque adresse IP grâce à un masque de sous-réseau.
- Les machines- **hostid** : elle identifie la machine dans le sous-réseau considéré.

Le préfix réseau : Statique : au début, les adresses IP étaient classées en plusieurs catégories appelées «classes». Aujourd'hui, il est dynamique.

Les adresses IP sont regroupées en classe

► Classe A

- 126 réseaux, 16777214 hôtes max par réseau



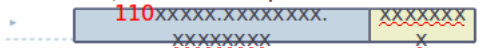
► Classe B

- 16384 réseaux, 65534 hôtes max par réseau



► Classe C

- 2097152, 254 hôtes max par réseau



Connaissant l'adresse Ip et le masque du réseau on peut en déduire l'adresse du réseau :

Exemple : @ en décimal pointé = 161.34.123.7 on fera :

1 . conversion en binaire = 10100001.00100010.01111011.00000111

2 . netmask 255.255.0.0 = 11111111.11111111.00000000.00000000

3 . soit @ réseau (avec &) = 10100001.00100010.00000000.00000000

4 . soit en décimal @ réseau = 161.34.0.0

On a alors l'adresse de diffusion sur le réseau auquel appartient cette machine : 161.34.255.255

Quelques adresses spéciales à connaître :

- Route par défaut : 0.0.0.0
- Le réseau de boucle de retour - loopback : 127.0.0.1

LES RÉSEAUX PRIVÉS 'NON-CONNECTÉS' RÉSEAUX QUI UTILISENT IP MAIS NE SONT PAS CONNECTÉS À L'INTERNET

- Un réseau de classe A : 10.0.0.0 ,
- 16 réseaux de classe B : de 172.16.0.0 à 172.31.0.0 ,
- 256 réseaux de classe C : de 192.168.0.0 à 192.168.255.0

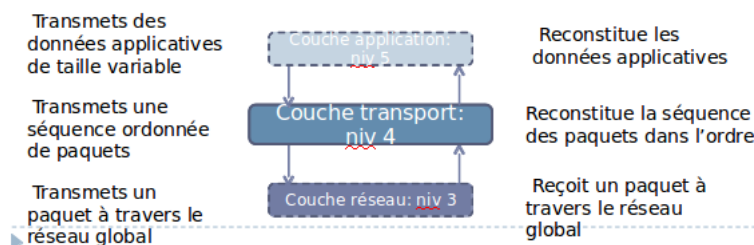
Par défaut, les routeurs des FAI (FreeBox, LiveBox, sfrBox, etc.) créent un réseau de type 192.168.0.0, avec 192.168.0.1 comme IP pour le routeur (passerelle). Il affecte ensuite aux machines du réseau les adresses 192.168.0.2 à 192.168.0.254.

À RETENIR : LES ADRESSES IP SONT DES ADRESSES LOGIQUES QUI IDENTIFIENT DES MACHINES INTERCONNECTÉES VIA INTERNET. LES ROUTEURS EXAMINENT L'ADRESSE DU DESTINATAIRE POUR DÉTERMINER SUR QUEL LIEN TRANSMETTRE LE MESSAGE. UN ROUTEUR NE CONSERVE QUE LES ADRESSES DES RÉSEAUX DANS SES TABLES ET NON TOUS LES HÔTES. IL UTILISE LE MASQUE DE RÉSEAU FOURNI DANS LE MESSAGE POUR DÉTERMINER L'ADRESSE RÉSEAU ASSOCIÉE AU DESTINATAIRE. LOCALEMENT, LA PASSERELLE PEUT ROUTER LES PAQUETS SUR DES SOUS-RÉSEAUX LOCAUX VIA UNE TABLE DE ROUTAGE LOCALE QUI STOCKE LES ADRESSES DES SOUS-RÉSEAUX. LES SOUS-RÉSEAUX SONT INVISIBLES DE L'EXTÉRIEUR DE LA PASSERELLE.

La couche Transport - Niveau 4 :

Les tâches accomplies par les protocoles de cette couche sont :

- Adressage des applications : identifier les applications en cours d'exécution qui utilisent le réseau.
- Fiabilité : assurer le transport des paquets de bout en bout en corrigeant les erreurs éventuelles de la couche 3.



Les identifiants de l'application = <@IP + port>

Le port est simplement un entier positif de 2 octets. Pour communiquer avec une application sur le réseau, il faut avoir connaissance de son numéro de port, en plus de l'adresse IP de la machine elle-même.

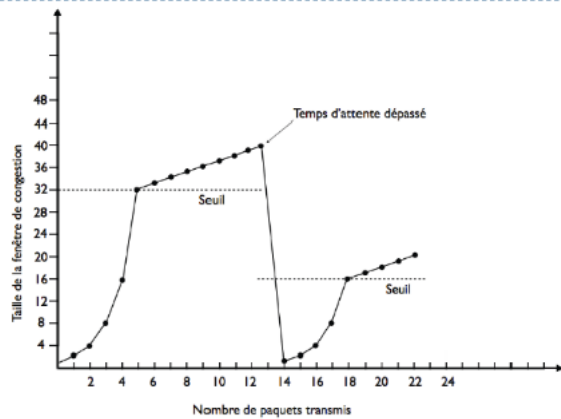
Les numéro de port ≤ 1024 sont des numéros réservés. Exemple : le port 80 = port HTTP.

Le système d'exploitation local a pour charge de définir le mécanisme qui permet à une application d'accéder à un port. **Socket** = mécanisme de communication entre les applications au-dessus d'Internet.

Il en existe 2 types :

- 1 . socket UDP : non fiable, sans garantie en mode datagramme pour des applications au dessus d'UDP tels que DNS, TFTP, NFS
- 2 . socket TCP : fiable, en mode connecté. Elle fonctionne en 3 phases : établissement de la connexion, transfert des données et libération. Les mécanismes de TCP permettent d'assurer l'acquiescement, le reséquencement, le contrôle du rythme d'envoi des paquets et le contrôle de congestion.

Contrôle de congestion



TCP. Ajustements progressifs de la cadence d'envois des paquets via les variations de la fenêtre de congestion.

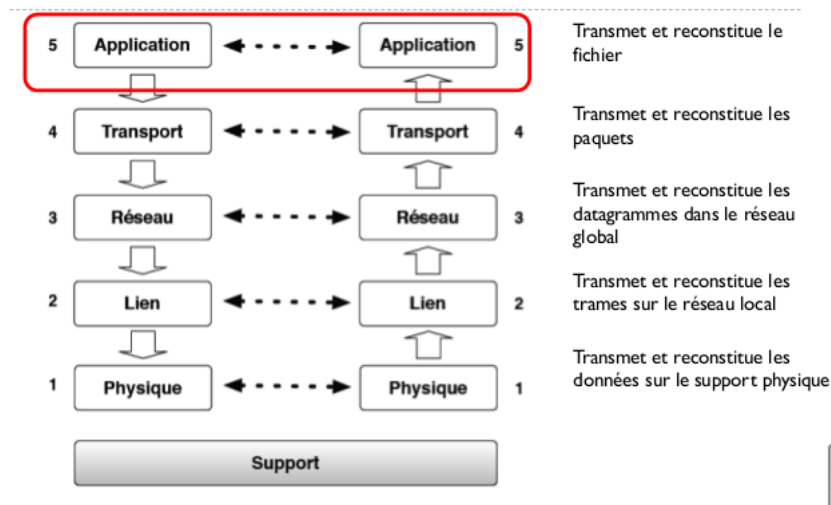
Format d'un segment TCP

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31																
Port Source 2 octets																Port destination 2 octets																															
Numéro de séquence																																															
Numéro d'acquittement																																															
Taille de l'en-tête				réserve		ECN		URG		ACK		PSH		RST		SYN		FIN		Fenêtre																											
Somme de contrôle																																Pointeur de données urgentes															
Options																								Remplissage																							
Données																																															

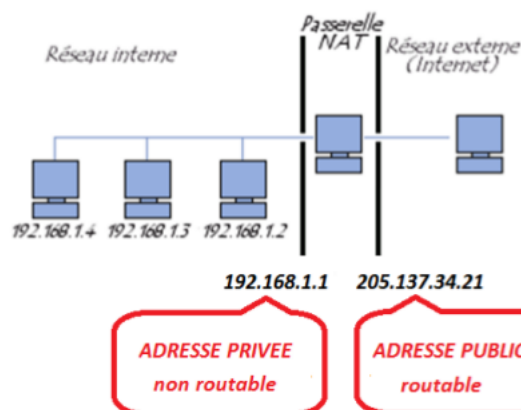
- En-tête TCP de 20 octets avec options sur 4 octets
- La taille du segment TCP dépend de la MTU de la couche sous-jacente

À RETENIR : LA COUCHE TRANSPORT A POUR FONCTION : L'ADRESSAGE DES APPLICATIONS VIA UN IDENTIFIANT DE LA FORME <@IP, PORT>. TCP ASSURE LA FIABILITÉ DE LA COMMUNICATION EN CAS DE PERTE DE PAQUETS OU DE DÉSÉQUENCEMENT VIA : LA NUMÉROTATION DES SEGMENTS, L'ACQUITTEMENT DES SEGMENTS. LES SEGMENTS NON ACQUITTES SONT RÉÉMIS ET PEUVENT ÊTRE À NOUVEAU PERDUS OU BIEN REDONDANTS. POUR LIMITER LES ERREURS, TCP TENTE DE LIMITER LA CONGESTION DU RÉSEAU EN AJUSTANT LA CADENCE D'ENVOI DES PAQUETS AUX CAPACITÉS DU RÉSEAU.

3 Les applications en réseau - Niveau 5-6-7 :



NAT - Translation d'adresses :



On distingue les :

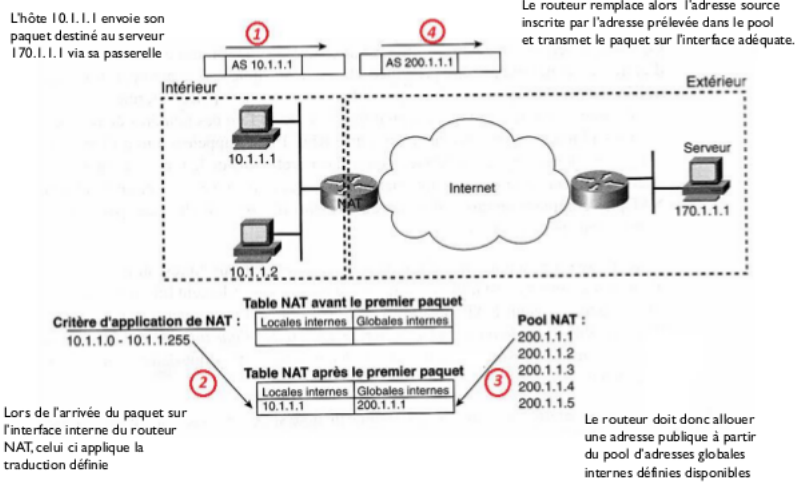
- Adresses routables = qui peut être utilisé dans les tables de routage des routeurs internet. Identifie un routeur ou une passerelle
- Adresses non routables = qui identifie un hôte avec une adresse ayant une signification locale, donc inutilisable par un routeur .

La **masquerade IP - IP masquerading** : Transformer une @ip non routable en une @ip routable. On établit une table de correspondance <@ip privé ↔ @ip publique> .

Lorsqu'une machine du réseau effectue une requête vers Internet :

- 1 . la passerelle effectue la requête à sa place en modifiant l'@ip privé de l'expéditeur avec l'@ip routable
- 2 . la passerelle reçoit la réponse et interroge sa table de correspondance
- 3 . elle transmet la réponse à la machine ayant fait la demande. De l'extérieur, toutes les requêtes semblent provenir de l'adresse publique.

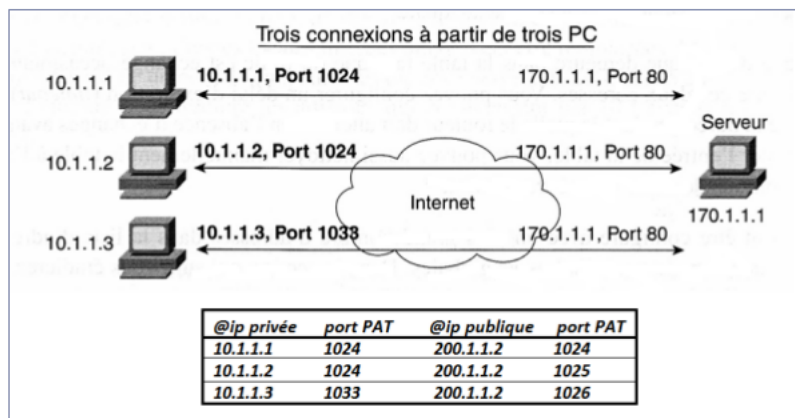
Exemple de NAT dynamique



NAT dynamique avec overloading

L'overloading, ou traduction PAT, permet à NAT de s'adapter à l'augmentation des clients Internet d'une entreprise. Plus de clients que d'@ip et des clients qui ne sont jamais tous connectés en même temps. **PAT - Port Address Translation** : affectation d'un port source différent à chaque requête ; (@ip privée, PAT) ↔ (@ip pub. src, @ip pub. dest, PAT) et maintient une correspondance entre les requêtes provenant du réseau interne et les réponses des machines sur Internet, toutes adressées à l'adresse IP du routeur .

Exemple de NAT dynamique avec overlapping



► Le serveur 170.1.1.1 ne fait pas la différence

SYNTHÈSE : NAT EST UN MÉCANISME DE CORRESPONDANCE ENTRE DES @IP PRIVÉES NON ROUTABLES ET DES @IP PUBLIQUES (ROUTABLES). NAT AUTORISE UNE MACHINE INTERNE À ENVOYER DES REQUÊTES VERS INTERNET LE NATAGE DÉPEND DU NOMBRE N D'@IP PUBLIQUES À DISPOSITION :

- NAT STATIQUE : $N \leftrightarrow N$ STATIQUEMENT
- NAT DYNAMIQUE : $N \leftrightarrow 1$ CHOISI À CHAQUE REQUÊTE - IP MASQUERADING -
- NAT DYNAMIQUE AVEC PAT : $M \leftrightarrow 1$, AVEC $M > N$

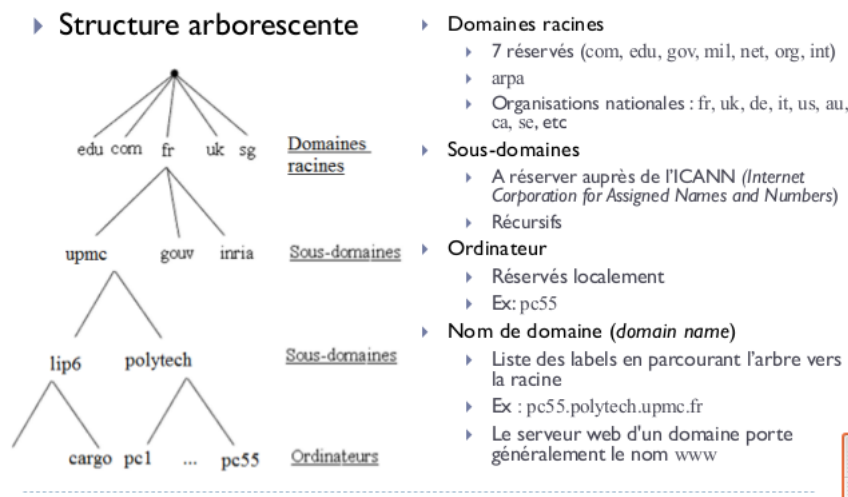
PORT FORWARDING : AUTORISER UNE MACHINE EXTERNE À ENVOYER DES REQUÊTES SUR UNE MACHINE INTERNE. LE PORT DE CONNEXION EST REDIRIGÉ VERS UNE MACHINE DONNÉE .

DHCP - Dynamic Host Configuration Protocol - cf mini-projet

SYNTHÈSE : LE PROTOCOLE DHCP PERMET D'ATTRIBUER **dynamiquement** DES @IP À DES MACHINES D'UN RÉSEAU LOCAL. LE SERVEUR DHCP **centralise** LES REQUÊTES DHCP ET IL EST CONFIGURÉ MANUELLEMENT. **Un bail** : LES @IP SONT ATTRIBUÉES TEMPORAIREMENT. UN CLIENT INTERROGE LE SERVEUR DHCP LORSQU'IL SE CONNECTE POUR LA PREMIÈRE FOIS SUR LE RÉSEAU OU BIEN LORSQUE SON BAIL ARRIVE À EXPIRATION.

DNS -Domain Name System - cf mini-projet

À RETENIR : ASSOCIER DES NOMS DE DOMAINE À UNE OU PLUSIEURS @IP. LE **FQDN - Fully Qualified Domain Name** = NOM DE DOMAINE COMPLET EST UN ESPACE DE NOMS DE DOMAINE HIÉRARCHISÉ PAR UNE ORGANISATION INTERNATIONAUX POUR LES DOMAINES RACINES ET LES ORGANISMES PROPRIÉTAIRES POUR LES SOUS-DOMAINES. LA RÉOLUTION DU NOM DE DOMAINE EST FAITE PAR **le protocole DNS** AU-DESSUS D'UDP/TCP. LES DIFFÉRENTS NIVEAUX DE SERVEURS DNS GÉRENT DES CACHES DE CORRESPONDANCE ENTRE FQDN ET @IP



Les protocoles texte :

À RETENIR : LA COMMUNICATION EN FORMAT ASCII EST UN ÉCHANGE DE MESSAGES TEXTE. CHAQUE MESSAGE TERMINE PAR LA BALISE <CRLF>. CES PROTOCOLES SONT COURANTS CAR LES PLUS SIMPLES À METTRE EN ŒUVRE ET LES PLUS PORTABLES. C'EST AUX PROGRAMMES COMMUNICANTS DE FAIRE LE TRAVAIL DE CODAGE ET D'INTERPRÉTATION DES CHÂÎNES REÇUES. CES PROTOCOLES SONT SUJETS À DES ERREURS D'INTERPRÉTATION. EXEMPLES DE PROTOCOLES TEXTE : HTTP , SMTP/POP , TELNET (= COMMANDES POUR CONTACTER UN SERVEUR MANUELLEMENT EN MODE TEXTE SUR LE PORT 23)

Autres applications réseaux, les applications sécurisées seront détaillées au prochain cours :

- FTP (File Transfert Protocol) : Transfert de fichiers sur le réseau
- TLS (Transport Layer Security) : Sécurisation des échanges internet
- SSH : Sécurisation des échanges internet. Repose sur un échange de clés de chiffrement en début de connexion.
- HTTPS = HTTP+TLS : sécurise le http
- SMTPS = SMTP+TLS : sécurise les mails

Conclusion :

INTERNET CONNAÎT UN SUCCÈS CROISSANT DEPUIS 50 ANS. ON PEUT LE MODÉLISER PAR UN DÉCOUPAGE EN COUCHES, UNE ORGANISATION EN PILE. LES SUPPORTS PHYSIQUES SONT PEU CHERS . SIMPLICITÉ, EFFICACITÉ ET ROBUSTESSE SONT LES QUALITÉS D'ETHERNET REPOSANT SUR UNE SIMPLICITÉ, UNE GÉNÉRICITÉ ET UNE ADAPTABILITÉ D'IP ET UNE ÉQUITÉ DE TCP ET PERMET UNE ADMINISTRATION DÉCENTRALISÉE. DE NOMBREUX CHALLENGES EN COURS ET À VENIR SUR LES RÉSEAU MOBILES , LES RÉSEAU AUTONOMES (MANET), LES RÉSEAU PEER-TO-PEER, LES RÉSEAU VIRTUELS, LE CLOUD (= APPLICATIONS DISTRIBUÉES). LE COMPROMIS SUR INTERNET SE JOUE ENTRE BEST-EFFORT VS QoS ET LIBRE ÉCHANGE VS COPYRIGHT.

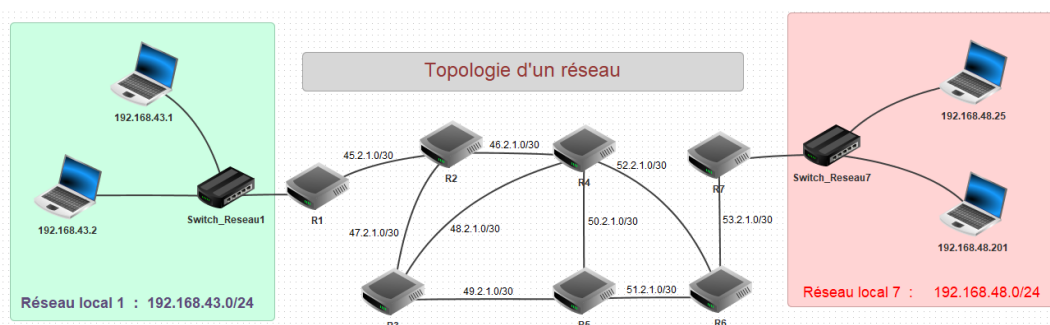
NB : Visualiser le film fait par l'Euro-IX, opérateur de coeur de réseau (durée : 5'24") : en recherchant sur le net **Internet Revealed : A film about IXPs**

4 Les protocoles de routage :

Comme nous l'avons vu précédemment les machines (hosts ou servers) sont identifiés avec une adresse IP et un masque de sous-réseau. Chaque paquet IP va prendre un chemin pour arriver à destination qui n'est pas obligatoirement le même dans le temps. De nombreux changements se produisent sur internet comme les pannes de routeurs, les coupures de liaisons, des ajouts de routeurs, des ajouts de réseaux, etc...

Les paquets IP sont acheminés à travers des routeurs d'accès, en bordure de réseau puis en général sur des routeurs internes, en coeur de réseau, beaucoup plus rapide. Ce paquet IP va être acheminé suivant différents protocoles et parcourir différentes topologies.

Nous allons voir en détail 2 types d'algorithmes de routage, actuellement les routeurs se découvrent et établissent leurs propres tables de routage de façon **décentralisés et dynamiques** afin d'assurer une cohérence entre eux et une fiabilité des échanges malgré tous changements de topologies, de pannes, etc...



Dans un premier temps, représenter avec les bons paramètres ce réseau sous le logiciel Filius en mode construction. Mettez les bons masques et les bon nombre d'interfaces pour chaque masque sous-réseau.

En général une interface ethernet (10 Mbit/s) se note eth0,eth1,...; une interface fast-ethernet (100 Mbit/s) fasteth0,fasteth1,...; une interface wifi (10 Mbit/s à 10 Gbit/s) (wlan0,wlan1,...); une interface FO (10 Gbit/s) (ffth0,ffth1,...).

4.1 Le protocole RIP - *Routing Information Protocol* :

Le principe du protocole RIP est :

chaque routeur transmet à ses voisins les adresses de ses propres voisins ou celles qu'il a reçues par d'autres routeurs. En plus des adresses, le routeur indique la distance, le nombre de sauts, qu'il le sépare d'un autre réseau. Nous obtenons donc par RIP un couple (**adresse,distance**) appelés **vecteurs de distance**.

Une fois, le réseau stabilisé, chaque routeur aura une indication de distance donnant le moins de routeurs pourcourus d'une machine à une autre.

La distance maximale pour le protocole RIP est fixée à 15 routeurs, au delà, les routes sont ignorées. Cette limite fait que le protocole RIP est utilisé sur des réseaux de petites tailles afin de réduire le délai de convergence pour connaître la topologie.

le **protocole RIP permet aussi de détecter les pannes**. Pour cela, un routeur considère qu'un voisin est en panne s'il ne reçoit pas de tables après une demande RIP après un certain laps de temps, **par défaut fixé à 3 minutes**. **Le routeur ayant détecté une panne enverra à ses voisins que la distance est infinie par ce routeur soit une distance de 16**.

Voyons comment R1 va établir sa table de routage :

Table de routage de R1 - au départ			
Destination	Passerelle	Interface	distance
192.168.43.0/24		192.168.43.254	1
45.2.1.0/30		45.2.1.1	1

Pendant ce temps, les routeurs vont établir de la même façon leur table de départ, phase d'initialisation.

Puis le routeur va échanger des **demandes RIP** avec ses voisins. Lorsque le voisin reçoit une telle demande, il va accuser reception en lui envoyant sa table en réponse, ou une partie de sa table.

Lorsque le routeur reçoit la réponse de son voisin, il y a 4 cas :

- 1 . Il découvre un nouveau sous-réseau alors il modifie sa table.
- 2 . Il découvre une nouvelle route plus courte vers un sous-réseau connu passant par un autre routeur, il modifie sa table.
- 3 . Il reçoit une route plus longue alors il l'ignore.
- 4 . Il reçoit une nouvelle route plus longue passant par le même voisin. Un problème est apparu sur les routes de son voisin mais il met à jour sa table avec cette nouvelle route.

Table de routage de R1 finale - après 3 minutes maximum (immédiat sur filius)			
Destination	Passerelle	Interface	distance
192.168.43.0/24		192.168.43.254	1
45.2.1.0/30		45.2.1.1	1
192.168.48.0/24	45.2.1.2	45.2.1.1	5

Les

autres routeurs ont alors tous leurs tables de routages.

Exercice :

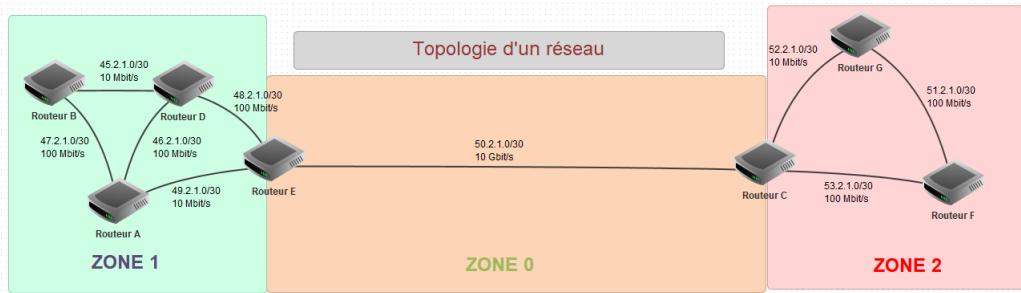
Établir les tables de R2,R3,R4,R5,R6 et R7 puis les écrire sur chacun des routeurs sous filius et testez avec un ping du réseau local1 au réseau local 7.

Visualisez le trajet pris :

Utilisez sur le client 192.138.43.1 traceroute pour vérifier le trajet jusqu'au client 192.168.48.201 :

Comment fonctionne la commande traceroute (Sur Filius, passez en mode simulation, clic droit et visualisez "afficher les échanges de données") ?

4.2 Le protocole OSPF, année 90 par IETF - *Open Shortest Path First* :



Contrairement au protocole RIP, l'objectif n'est plus de minimiser le nombre de routeurs traversés par un paquet. La notion de distance utilisée dans le protocole OSPF est uniquement liée aux coûts des liaisons.

L'objectif est alors de minimiser la somme des coûts des liaisons traversées.

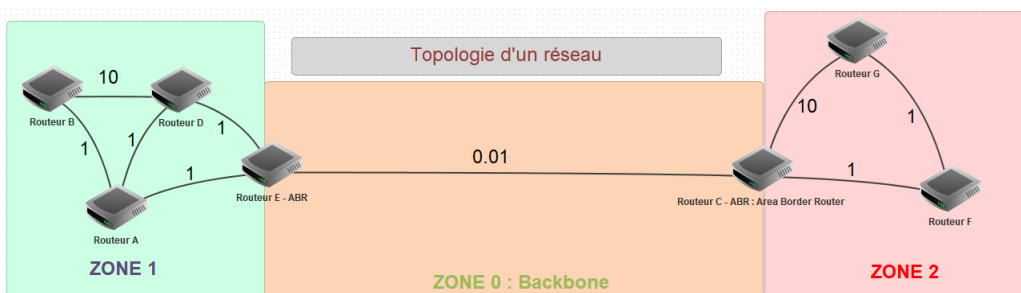
Le coût d'une liaison est donnée par la formule suivante :

$$\text{coût} = 10^8 / d$$

où d est la bande passante en bit/s entre les 2 routeurs et 10^8 relatif au fastEthernet 100Mbits/s. Afin que le protocole OSPF puisse être utilisé dans de grands réseaux, on

répartit les routeurs dans des zones. Alors la recherche de voisins, l'échange des états de liens, la topologie sont alors restreintes aux routeurs d'une même zone. Un routeur nommé **ABR** sont les seuls rattachés à 2 zones et les seuls à connaître la topologie de leur zone : ils servent aux échanges inter-zones. Le backbone étant le cœur de réseau permet de laisser les échanges s'établir entre les différentes zones sans en connaître la topologie. Les ABRs communiqueront au backbone et aux autres réseaux le chemin le plus court calculer sur leur zone.

Une politique d'échanges gratuites ou payantes est établi afin de garantir un trafic optimal des paquets.



La première grande étape du protocole OSPF est de créer pour chaque zone une table pour chaque routeur de ce type :

Topologie du réseau pour le routeur E			
Lien	sous-réseau	coût	zone
RE - RD	48.2.1.0/30	1	1
RE - RA	49.2.1.0/30	1	1
RD - RA	46.2.1.0/30	1	1
RA - RB	47.2.1.0/30	1	1
RB - RD	45.2.1.0/30	10	1

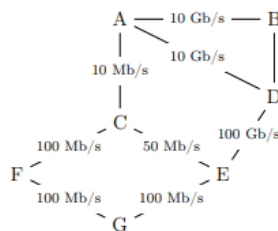
Les routeurs de la zone 1 ont d'abord un identificateur unique (par exemple la plus grande @IP du sous-réseau), Le routeur E a découvert ses voisins (routeurs D et A) par un message HELLO (identificateur, le numéro de la zone et les identificateurs des voisins de voisins) en vérifiant si son identificateur apparaît sinon il envoie un message LSA (Link State Advertissement). Le processus est une diffusion (flooding) ou multidiffusion (multicast) toutes les 10 secondes. (sur @ 224.0.0.5 par défaut par le protocole OSPF).

Le routeur routeur E va informer qu'il va jouer le rôle d'ABR (routeur E pour la zone 1) puis il va ensuite déterminer le plus court chemin vers tous les routeurs de sa zone grâce à l'algorithme de Edsger Dijkstra (1959).

Enfin, le backbone va transmettre les tables et les plus courts chemins définis par les ABRs sur tous l'ensemble du réseau.

Comme exercice, répondre :

1 . aux questions du sujet 0 du bac NSI



Question 3

1. Vérifier que le coût de la liaison entre les routeurs A et B est 0,01.
2. La liaison entre le routeur B et D a un coût de 5. Quel est le débit de cette liaison ?

Question 4 Le routeur A doit transmettre un message au routeur G, en empruntant le chemin dont la somme des coûts sera la plus petite possible. Déterminer le chemin parcouru. On indiquera le raisonnement utilisé.

2 . Faire la preuve de l'algorithme de Dijkstra

3 . Écrire l'algorithme en pseudo-code puis le programme python de l'algorithme de Dijkstra

RÉFÉRENCES :

- « Les Réseaux ». Andrew Tanenbaum. Edition Pearson Education.
- « Les Réseaux ». Guy Pujolle. Edition Eyrolles.
- « Informatique et Sciences du Numérique - Spécialité ISN en Terminale S », Gilles Dowek and co. Edition Eyrolles.
- Cours Cécile Le Pape - Lip6
- NSI_Tle T.Balabonski-S.Conchon-JC.Filliâtre-K.Nguyen Edition Ellipses.