Modélisations des réseaux de télécommunications

Philippe Latu
philippe.latu(at)inetdoc.net

https://www.inetdoc.net

Résumé

La modélisation du fonctionnement des réseaux de télécommunications a longtemps été l'objet de luttes d'influence entre les organismes de normalisation, les compagnies de télécommunication et les constructeurs d'équipements. Avec l'avènement de l'Internet, un modèle contemporain faisant la synthèse entre les modèles de référence historiques OSI et TCP/IP s'est imposé. L'objectif de cet article est d'introduire les concepts de modélisation, de présenter les deux modélisations dominantes et le «dénominateur commun» qui en est issu.

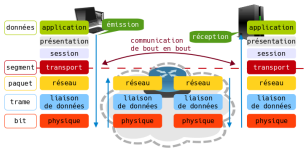


Table des matières

1. Copyright et Licence 2
    1.1. Meta-information 2
2. Modélisation des réseaux de télécommunications 2
    2.1. Classification 3
    2.2. Modélisations en couches 3
    2.3. Concepts communs aux modélisations 3
    2.4. Commutation de circuit ou commutation de paquet 4
    2.5. Types de communications 6
    2.6. Services avec et sans connexion 6
    2.7. Encapsulation 7
    2.8. Modèles de référence 7
3. Modélisation OSI 7
    3.1. Point fort : la transmission de l'information 7
    3.2. Point faible : le traitement de l'information 8
    3.3. Définitions 8
    3.4. Couche physique (bit) 8
    3.5. Couche liaison de données (trame) 9
    3.6. Couche réseau (paquet) 9
    3.7. Couche transport (segment ou datagramme) 9
    3.8. Couche session 10
    3.9. Couche présentation 10
    3.10. Couche application 10
4. Modélisation TCP/IP 11
    4.1. Point fort : les protocoles 11
    4.2. Point faible : le modèle 12
    4.3. Couche Internet : le protocole IP 12
    4.4. Couche Host-to-Host : les protocoles TCP & UDP 14
    4.5. Protocole TCP 14
    4.6. Protocole UDP 16
    4.7. Unités de données 17
5. Modèle Contemporain 18
6. En guise de conclusion 18
    6.1. Documents de référence 19
    6.2. Glossaire des acronymes 19

1. Copyright et Licence

Copyright (c) 2000,2018 Philippe Latu.
Permission is granted to copy, distribute and/or modify this document under the
terms of the GNU Free Documentation License, Version 1.3 or any later version
published by the Free Software Foundation; with no Invariant Sections, no
Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included
in the section entitled "GNU Free Documentation License".

Copyright (c) 2000,2018 Philippe Latu.
Permission est accordée de copier, distribuer et/ou modifier ce document selon
les termes de la Licence de Documentation Libre GNU (GNU Free Documentation
License), version 1.3 ou toute version ultérieure publiée par la Free Software
Foundation ; sans Sections Invariables ; sans Texte de Première de Couverture,
et sans Texte de Quatrième de Couverture. Une copie de la présente Licence est
incluse dans la section intitulée « Licence de Documentation Libre GNU ».

1.1. Meta-information

Cet article est écrit avec DocBook XML sur un système Debian GNU/Linux. Il est disponible en version imprimable au format PDF : `modelisations.pdf`.

Le ton de cet article est volontairement «polémique». L'objectif pédagogique est de susciter la réaction et, pourquoi pas, la réflexion sur un sujet souvent jugé trop académique. Une bonne compréhension de la genèse des différents modèles d'interconnexion des réseaux de télécommunications permet de construire une analyse critique des évolutions actuelles.

2. Modélisation des réseaux de télécommunications

Si l'utilisation des connexions aux réseaux de télécommunications a explosé avec le développement de l'Internet, la conception des techniques de connexion a débuté dans les années 1960.

À cette époque, comme le nombre de fournisseurs d'équipements informatiques était réduit, chacun a développé «sa» solution de connexion. Les difficultés sont très vite apparues lorsque les utilisateurs ont eu besoin d'interconnecter des systèmes hétérogènes distants.

Aujourd'hui, la très grande majorité des interconnexions utilise des équipements et des réseaux acquis auprès de fournisseurs différents. Pour parvenir à ce résultat, il a fallu harmoniser les modes d'interconnexion. Les modélisations sont les outils essentiels de cette harmonisation.

Pendant la guerre froide, l'ARPANET, l'ancêtre militaire de l'Internet, a été développé à partir de 1969 pour maintenir les communications entre les centres névralgiques du continent nord américain face aux menaces d'attaques nucléaires. Même si ces conditions d'utilisation sont très éloignées du contexte actuel, l'interconnexion de systèmes hétérogènes était une nécessité impérieuse pour le département d'état des États-Unis.

Les protocoles TCP et IP qui dominent les réseaux de télécommunications contemporains ont été conçus pour répondre à ces objectifs d'harmonisation des échanges d'informations entre systèmes différents. Sans une modélisation cohérente des communications, il serait impossible de faire transiter des flux très différents tels que les données, la voix ou la vidéo sur des réseaux hétérogènes utilisant aussi bien les radiocommunications que des câbles en cuivre ou en fibre optiques.

2.1. Classification

Historiquement, c'est la distance entre les équipements à connecter qui a constitué le premier critère de classement des réseaux de télécommunication.

Ce critère est fondé sur le mode de transport de l'information. Même si c'est de moins en moins vrai, on part du principe que l'on n'emploie pas les mêmes techniques pour véhiculer des données d'une pièce à l'autre ou d'un continent à l'autre.

Tableau 1. classification des réseaux

Distance	Acronyme	Type de réseau
jusqu'à 25 mètres	PAN	Réseau local «domestique» : Personal Area Network
jusqu'à 10 Km	LAN	Réseau local : Local Area Network
jusqu'à 50 Km	MAN	Réseau métropolitain : Metropolitan Area Network
jusqu'à 1000 Km	WAN	Réseau longue distance : Wide Area Network
jusqu'à 40000 Km	Internet	Réseau mondial

2.2. Modélisations en couches

La technique usuelle en informatique pour résoudre un problème complexe consiste à le découper en problèmes simples à traiter. L'interconnexion réseau étant un problème complexe, on a donc abouti à des traitements séparés par niveaux ou couches. La fonction de chaque couche est de fournir des services à son homologue de niveau supérieur en occultant ses traitements propres.

Entre deux équipements, chaque couche dialogue à son niveau à l'aide d'un protocole. Pour l'ensemble des couches utilisées lors d'une communication réseau, on parle de pile de protocoles.

2.3. Concepts communs aux modélisations

Il existe un certain nombre de concepts communs liés aux modélisations en couches. Ces concepts sont implémentés dans les protocoles. Les protocoles peuvent être vus comme une sélection des traitements possibles au niveau de chaque couche. Voici une présentation succincte de ces concepts :

adressage

Pour que chaque couche puisse reconnaître ses pairs sur les autres systèmes connectés au réseau, il est nécessaire de recourir à un adressage. Le rôle d'une adresse est d'identifier sans ambiguïté un hôte du réseau. Les mécanismes d'adressages jouent un rôle essentiel dans l'acheminement de l'information.

Il existe de très nombreux exemples d'utilisation de mécanismes d'adressage uniques ou multiples dans les réseaux :

- L'analogie la plus usuelle est fournie par le courrier papier qui est routé par le service postal en fonction de l'adresse du domicile suivant un protocole qui utilise le code postal, le type de voie, etc.
- Le courrier électronique est acheminé à partir d'une adresse composée du nom d'utilisateur (partie gauche) et d'un nom de domaine (partie droite).
- Un téléphone mobile met en œuvre plusieurs mécanismes d'adresses simultanément. Il est repéré dans une cellule par son International Mobile Equipment Identity ou code IMEI et les communications utilisent le numéro de l'abonné. C'est aussi sur le format du numéro de téléphone que des décisions d'acheminement sont prises (opérateur, zone géographique, etc.).
- Pour un hôte connecté à l'Internet, au moins une adresse IPv4 ou IPv6 doit lui être attribuée. Elle identifie cet hôte de façon unique. Les adresses IP ne sont généralement pas les seules utilisées dans un même

système. On retrouve souvent une adresse MAC utilisée pour repérer le même hôte dans un réseau local ou dans la zone de couverture radio du réseau sans fil.

routage

Les protocoles de chaque couche prennent leurs décisions d'acheminement de l'information à partir des adresses et des itinéraires disponibles. La technique d'acheminement d'une information à travers de multiples circuits de communications est appelée routage.

contrôle d'erreur

Les circuits de communications n'étant pas parfaits, il est nécessaire de mettre en œuvre des mécanismes de contrôle d'erreur. Suivant le niveau de traitement de chaque couche, ces contrôles d'erreur sont pris en charge par les protocoles de chaque niveau. Au niveau le plus bas, on contrôle que le nombre de bits reçus correspond bien au nombre de bits émis sur un média (paire cuivre, fibre optique, canal hertzien). À un niveau plus élevé, on contrôle le séquencement de l'acheminement de blocs d'informations. Si une suite de blocs est émise dans un ordre donné, ces mêmes peuvent parvenir dans le désordre à l'autre extrémité d'un réseau étendu.

contrôle de flux

Tous les systèmes n'ayant pas les mêmes capacités de traitement, il faut éviter que les hôtes les mieux dotés mobilisent à leur seul usage les circuits de communications. De la même façon, il faut éviter qu'un émetteur ne sature l'interface d'un récepteur plus lent. Les solutions à ces problèmes peuvent être complexes. Généralement, les protocoles implémentent des mécanismes de notification qui permettent contrôler qu'un récepteur a bien traité l'information qui lui est destinée. On parle alors de contrôle de flux.

(dé)multiplexage

Les routes empruntées par les circuits de communications dépendent de la topographie. L'interconnexion des réseaux entre les continents passe par un nombre limité de circuits appelés dorsales (backbones). La transmission de l'information sur les dorsales utilise les fonctions de multiplexage (temporel ou fréquentiel) à l'émission et de démultiplexage à la réception. Ces fonctions permettent de véhiculer plusieurs flux distincts sur un même circuit.

2.4. Commutation de circuit ou commutation de paquet

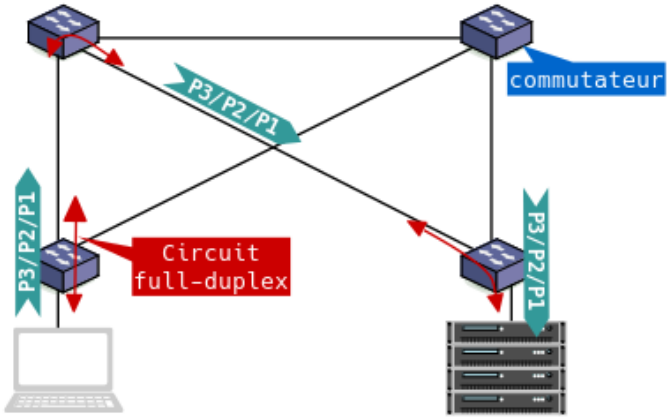
Dans les réseaux de télécommunications contemporains on retrouve deux techniques de commutation distinctes. Ces techniques peuvent se croiser dans la description des couches des modélisations et dans les technologies d'implémentation des protocoles. Ainsi, dans un réseau local, on peut très bien utiliser une commutation de circuit avec la technologie Ethernet au niveau liaison et utiliser un réseau à commutation de paquets avec le protocole IP.

Commutation de circuit

Cette technique consiste à commuter des circuits physiques ou virtuels pour que deux hôtes du réseau puissent communiquer comme s'ils étaient connecté directement l'un à l'autre. Voici deux exemples classiques de ce type de commutation.

- Sur un réseau téléphonique filaire lors de l'émission d'un nouvel appel en composant un numéro d'abonné, les commutateurs téléphoniques établissent un circuit unique entre les deux combinés. Une fois la communication établie, les échantillons de voix transitent séquentiellement sur ce circuit.

- Sur un réseau local utilisant des commutateurs Ethernet, une fois les tables de correspondance entre les adresses physiques des hôtes constituées, les hôtes peuvent communiquer entre eux via un circuit unique établi par l'électronique des commutateurs.



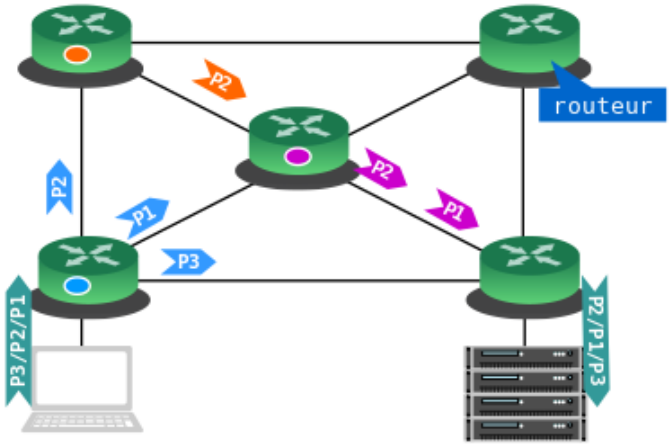
Dans la figure ci-dessus, les commutateurs ont constitué un circuit full-duplex unique entre les deux hôtes en communication. Les paquets P1, P2 et P3 sont nécessairement reçus dans l'ordre dans lequel ils ont été émis.

Si un circuit de communication est rompu, toutes les données présentes sur ce circuit sont perdues et toute communication est impossible tant qu'un nouveau circuit n'a pas été établi.

Commutation de paquet

Avec cette technique, les informations découpées en paquets de taille limitée peuvent emprunter des itinéraires différents en fonction de l'état de l'interconnexion réseau entre deux points.

Le protocole IP, utilisé au niveau réseau de la modélisation TCP/IP, est l'exemple le plus connu d'exploitation de la commutation de paquets.



La figure ci-dessus illustre le fait que chaque paquet peut suivre un chemin propre. Suite à l'émission d'une série de trois paquets, le premier routeur prend une décision d'acheminement fantaisiste et décide d'envoyer un paquet par lien. Cette première décision entraîne ensuite une arrivée des trois paquets dans le désordre.

Les caractéristiques de ces deux types de commutation sont adaptées à différents besoins. Avec la commutation de circuit, la constitution d'un circuit unique de bout en bout permet de conserver la séquence des informations émises et la réservation de bande passante évite la congestion. Avec la commutation de paquets, la tolérance aux pannes et l'optimisation de l'utilisation des canaux de communication sont bien meilleures. Cependant, l'absence de réservation de bande passante peut entraîner des problèmes de congestion.

On peut aussi prendre le temps de transmission comme point de comparaison. Sur un réseau à commutation de circuits, le temps de transit de l'information est connu. Il dépend uniquement des caractéristiques du circuit. Sur un réseau à commutation de paquets, chaque paquet peut emprunter un itinéraire propre et tous ces itinéraires ne possèdent pas les mêmes caractéristiques. De plus, chaque élément d'interconnexion doit stocker les paquets avant de prendre une décision d'acheminement ; ce qui peut introduire un temps de latence supplémentaire.

Les débits réseau et la capacité de traitement des équipements d'interconnexion se sont considérablement développés durant les dernières années. De ce fait, les temps de transmission de l'information deviennent négligeables devant d'autres paramètres comme le temps d'accès aux médias de stockage. C'est un des facteurs qui facilite le déploiement de presque tous les nouveaux services sur Internet.

2.5. Types de communications

Les différents types de communications entre les hôtes d'un réseau peuvent se regrouper en quatre catégories.

unicast

Ce type d'échange implique un échange unique et exclusif entre deux hôtes d'un réseau.

broadcast

Avec ce type d'échange, un émetteur unique impose à tous les autres hôtes d'un réseau de traiter son message.

multicast

Avec ce type d'échange, seuls les hôtes «abonnés» reçoivent un flux réseau émis par un émetteur unique. Si l'émission est continue, on parle alors de streaming.

anycast

Avec ce type d'échange, le trafic émis par une source unique est traité par la destination la plus proche parmi un groupe d'hôtes susceptibles de traiter ce trafic.

2.6. Services avec et sans connexion

Les services fournis par les couches paires entre deux hôtes d'un réseau peuvent fonctionner selon deux modes principaux : avec et sans connexion.

Service orienté connexion

Les communications téléphoniques sont un exemple caractéristique de service orienté connexion. Ce n'est qu'après avoir composé le numéro du correspondant et que celui-ci ait décroché que la conversation peut commencer. De la même façon, il faut que les deux correspondants aient raccroché pour qu'une nouvelle communication puisse être initiée.

Pour généraliser, on parle de trois phases : établissement, maintien et libération de la connexion.

Pendant la phase de maintien, les services des couches paires utilisent un circuit de communication unique physique ou virtuel de bout en bout.

Certains services utilisent la phase d'établissement pour négocier des options d'utilisation du circuit utilisé en phase de maintien. C'est notamment le cas de la couche transport du modèle TCP/IP avec le protocole TCP.

Les opérateurs téléphoniques utilisent beaucoup les services en mode connecté pour préserver la tarification basée sur les temps de communication. En effet, dès que l'information ne circule plus sur un circuit unique, il est beaucoup moins facile de comptabiliser le temps d'une connexion.

Service non orienté connexion

Les réseaux locaux privés sont généralement les exemples caractéristiques de services sans connexion. Sur ces réseaux, seuls les volumes d'informations comptent. Si on ne s'intéresse qu'à la quantité d'informations transitant en un point donné, peu importe le chemin emprunté par ces informations.

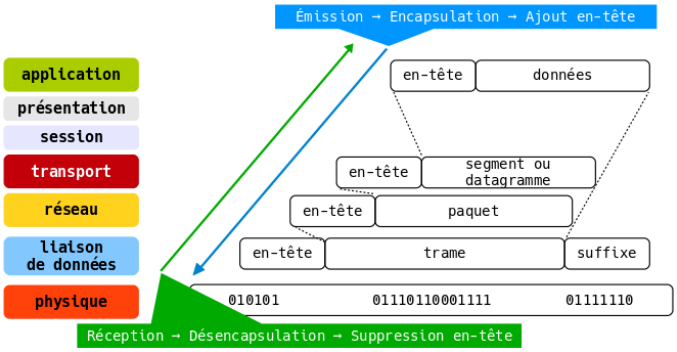
Par opposition à l'analogie avec les communications téléphoniques, on peut utiliser l'exemple du courrier postal. Deux lettres à destination d'une même adresse sont routées indépendamment et peuvent très bien ne pas parvenir dans l'ordre dans lequel elles ont été émises.

Le service de couche réseau de l'Internet avec son protocole IP fonctionne en mode non connecté. Tous les paquets IP sont routés indépendamment et peuvent suivre des chemins différents s'il existe plusieurs itinéraires disponibles.

2.7. Encapsulation

On peut prendre l'exemple des étapes de l'acheminement du courrier postal pour illustrer le concept d'encapsulation. Une lettre est d'abord insérée dans une enveloppe pour être postée. Cette enveloppe est ensuite placée dans un sac postal. Le sac postal est lui-même transporté dans un conteneur. Ces étapes illustrent l'encapsulation de l'information lors de son émission. Pour la réception, on reprend les mêmes étapes dans l'ordre inverse. Le sac postal est extrait du conteneur. L'enveloppe est extraite du sac postal et déposée dans la boîte aux lettres du destinataire. On peut parler de désencapsulation pour décrire les étapes de réception.

Si on aborde le concept de façon plus formelle, on reprend les mêmes étapes entre les couches de la modélisation. Au passage d'une couche N vers la couche inférieure (N-1), le flot de données est enrichi de champs supplémentaires placés en début et/ou en fin. Dans le premier cas, il s'agit d'un en-tête ou préfixe (header) ; dans le second, d'un suffixe (trailer). Ces informations apportées renseignent l'unité de donnée au niveau de la couche qui les a émises (ici N). Ces champs servent donc, lors de la réception par la couche de même niveau (N) de la station destinataire, au traitement que celle-ci doit effectuer. On peut y trouver les adresses source et destination (de niveau N), un contrôle de parité, la longueur concernant le paquet, des bits de priorité, l'identification du protocole de niveau supérieur (N+1) pour le décodage, des numéros d'acquittement, etc.



2.8. Modèles de référence

L'histoire des modélisations réseau a plus de quarante ans. Pour une technologie aussi évolutive que l'interconnexion des réseaux de télécommunications, quarante ans représentent une durée très longue au cours de laquelle plusieurs révolutions se sont produites.

À l'époque de la suprématie d'IBM, les plus hautes autorités politiques ont craint que cette société n'exerce une main mise irréversible sur les réseaux en imposant son modèle en 7 couches SNA. C'est en partie pour «répondre» à cette crainte que l'ISO a lancé les travaux sur la modélisation OSI : un autre modèle à 7 couches.

Parallèlement, le département de la Défense des États-Unis a lancé le projet ARPANET : l'ancêtre de l'Internet. Ce réseau qui a relié plus d'une centaine d'universités, a généré sa propre modélisation baptisée du nom de ses deux protocoles phares : TCP et IP. Les profits générés par ce réseau de recherche ont été suffisants pour que les constructeurs investissent dans la conception d'équipements utilisant ses protocoles. Comme ARPANET est devenu Internet et que les profits réalisés sur cette base ont explosé, TCP/IP se retrouve en tête des modèles de références.

Il faut aussi compter avec l'ITU. Cet organisme regroupe les agences réglementaires qui coordonnent la gestion des télécommunications. Parmi ces organismes, on trouve la Federal Communications Commission (FCC) aux USA, l'ARCEP en France. Depuis 1975, le développement des réseaux téléphoniques à commutation de paquets à partir des normalisations X.25 a contribué à figer la structure des couches basses de l'ensemble des modélisations.

3. Modélisation OSI

Il s'agit d'un modèle en 7 couches dont le principe fondamental est de définir ce que chaque couche doit faire mais pas comment elle doit le faire.

Les protocoles et les normalisations IEEE sont là pour définir comment les services sont fournis entre les couches.

3.1. Point fort : la transmission de l'information

Il a fallu quelques années entre la proposition initiale de l'ISO (1978) et la publication du standard IS7498:84 (1984). C'est ce standard, largement adopté par les constructeurs les plus importants et d'autres organismes

de normalisation comme l'ITU, qui a contribué à la popularité de ce «modèle d'interconnexion des systèmes ouverts». Un temps d'élaboration aussi long donne la mesure de la tâche accomplie pour fédérer les standards existants et obtenir un consensus entre des partenaires aux conceptions très éloignées sur l'organisation des réseaux.

Les spécifications des services des couches dédiées à la transmission de l'information, aussi appelées couches basses, sont si «chargées» qu'il a fallu les subdiviser en sous-couches respectant les modes de fonctionnement avec et sans connexion. Le consensus obtenu si difficilement est encore en vigueur aujourd'hui ; tous les constructeurs d'équipements le respectent.

3.2. Point faible : le traitement de l'information

Alors que pour les couches liées à la transmission de l'information les standards existants on pesé très lourd dans l'élaboration du modèle, la voie était quasiment libre pour les couches dédiées au traitement de l'information dans les années 80.

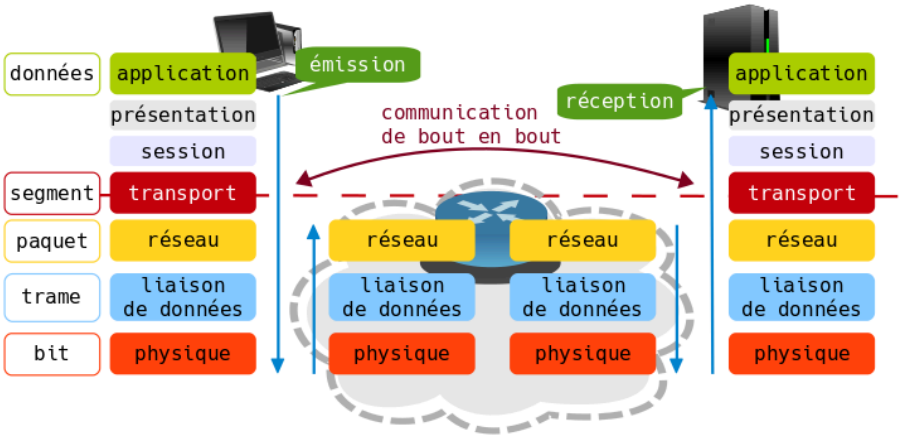
La tâche était à priori plus facile sachant qu'il n'y avait pas «d'ordre établi» sur les applications de traitement. Ce sont pourtant ces couches hautes qui ont provoqué le déclin de la modélisation OSI.

Les spécifications qui ont été produites pour les couches transport, session et application étaient si complexes que seules de rares applications mastodontes ont pu être développées. Ces services réseau, tels que les annuaires de services X500 normalisés par l'ISO et l'ITU n'ont pu être popularisés qu'après avoir été simplifiés et allégés. Aujourd'hui, on ne parle plus que des annuaires LDAP (Lightweight Directory Access Protocol).

Cette expérience a montré que l'on ne peut pas produire des spécifications trop «distantes» de l'état de la technologie et des infrastructures existantes. L'ISO a renoncé à promouvoir le modèle OSI en Décembre 1994 après avoir publié le standard ISO/IEC 7498-1:1994. A cette époque, l'Internet universitaire était déjà une réalité et les investissements industriels sur TCP/IP étaient bien engagés.

Le plus curieux, c'est que tous les organismes ne semblent pas avoir retenu la leçon. Le Forum ATM (Asynchronous Transfer Mode : technologie réseau répandue dans les grandes dorsales des opérateurs d'interconnexion) à produit deux spécifications contradictoires à un an d'intervalle vers le milieu des années 1990. La technologie ATM est aujourd'hui obsolète et remplacée par des dorsales Ethernet.

3.3. Définitions



Usuellement, on distingue les Couches Hautes (de Transport jusqu'à Application) qui ont une fonction de traitement des données indépendante de la technique de connexion entre 2 systèmes des couches basses (de Physique jusqu'à Réseau) qui ont une fonction de transmission de l'information liée à la technologie de communication.

3.4. Couche physique (bit)

Elle s'occupe de la transmission «brute» des flots de bits sur un circuit de communication sans connaître ni la structure, ni la signification de ces bits. À ce niveau, on s'intéresse à l'amplitude du signal, à la durée d'un bit, à la possibilité de transmettre simultanément dans les deux sens, à l'établissement et la libération du canal de connexion.

3.5. Couche liaison de données (trame)

Elle transforme les flots de bits en lignes de données sans erreur. Pour cela, elle fractionne les données d'entrée de l'émetteur en trames de données. C'est donc à elle de reconnaître les frontières des trames. Cette fonction entraîne la résolution des problèmes de trames endommagées, perdues ou dupliquées. On retrouve ici la fonction de contrôle d'erreur.

C'est aussi à ce niveau que l'on peut trouver des mécanismes de régulation pour éviter la saturation du canal de communication par un émetteur unique. C'est la fonction de contrôle de flux. Une technique très simple, employée dans les réseaux Ethernet, interdit les émissions continues à tous les hôtes du réseau. Une émission ne peut avoir lieu que si tous les hôtes ont eu le temps matériel de détecter que le média partagé est libre.

Si le service le requiert, le récepteur confirme la réception de chaque trame en émettant une trame d'acquittement.

Les réseaux à diffusion utilisent un service ou une sous-couche spécifique pour contrôler que l'accès au média est libre. Dans le cas des réseaux sans-fil de types IEEE 802.11 ou Wifi, des trames de gestion indépendantes des informations utilisateur sont échangées entre les équipements pour contrôler l'accès aux canaux hertziens.

3.6. Couche réseau (paquet)

Elle gère le sous-réseau (les couches basses), c'est-à-dire la façon dont les paquets sont acheminés de l'émetteur au récepteur. Elle contrôle la route empruntée par les paquets.

Les stratégies utilisées pour le routage sont très variables. On peut trouver des tables statiques dans les réseaux qui évoluent rarement. Cependant, on utilise généralement des protocoles de routage plus ou moins sophistiqués, dédiés à l'échange d'informations entre les équipements d'interconnexion fournissant un service de niveau réseau.

En plus des itinéraires disponibles, les choix de route se font en fonction du nombre d'équipements d'interconnexion à traverser, du débit disponible, de la charge d'un lien ou encore du temps de transit entre deux extrémités.

Cette couche doit aussi résoudre les problèmes d'interconnexion entre réseaux hétérogènes. Si un paquet doit transiter entre deux réseaux utilisant des technologies différentes, la couche réseau doit gérer :

- le changement de formats d'adresses,
- le redimensionnement des paquets,
- la mise en conformité entre protocoles différents,
- la comptabilisation du coût d'acheminement de l'information.

C'est encore à la couche réseau de contrôler la congestion d'un réseau en notifiant les hôtes voisins à l'aide d'informations spécifiques.

3.7. Couche transport (segment ou datagramme)

Sa fonction de base est de traiter les données de la couche session et de les découper au besoin en petites unités. Ces petites unités sont ensuite transmises à la couche réseau tout en s'assurant qu'elles sont parvenues à destination si on utilise un protocole orienté connexion.

Une connexion de transport est un canal point à point délivrant des messages sans erreur dans l'ordre d'émission toujours dans le cas d'un protocole orienté connexion. Avec la couche transport on aborde les couches de «bout en bout» (couches hautes), c'est-à-dire que le même protocole s'exécute sur l'émetteur et le destinataire en utilisant les messages d'en-tête et de contrôle. Cette couche doit gérer l'initialisation et la fin des connexions sur le réseau ; ce qui nécessite un mécanisme d'adressage permettant d'identifier le ou les destinataires. Les numéros de ports constituent le mécanisme d'adressage de la couche transport.

La couche transport est parfois considérée comme faisant partie des couches basses parce qu'elle doit préserver la couche session des changements de technologies entre réseaux.

- La prise réseau ou socket est le canal de communication entre une application et la couche transport. Une même application peut utiliser plusieurs prises réseau. Le navigateur Chrome est un excellent exemple. Ce programme utilise un grand nombre de sockets lors de l'ouverture d'une seule page web.
- En réception, la couche transport reçoit une séquence de segments ou datagrammes de la couche réseau. Les segments ou datagrammes peuvent être destinés à différentes prises réseau alors que les adresses IP source et destination des paquets de la couche réseau sont identiques.
- L'opération qui permet de délivrer les segments ou datagrammes aux bonnes prises réseau est appelée démultiplexage.
- L'opération qui permet d'assembler les segments ou datagrammes pour les passer à la couche réseau est appelée multiplexage.
- Les opérations de multiplexage et de démultiplexage sont nécessaires lorsque le canal de communication de bout en bout est partagé entre deux hôtes.

Les deux protocoles disponibles au niveau de la couche transport sont TCP (orienté connexion) et UDP (non orienté connexion). Ils sont présentés dans la Section 4.4, « Couche Host-to-Host : les protocoles TCP & UDP ».

3.8. Couche session

Elle permet à des utilisateurs, opérant sur différentes machines, d'établir des sessions entre eux. Une session a pour but le transport des données. Par rapport à la couche transport, elle offre des services supplémentaires tels que :

- La gestion du dialogue ou du jeton : certains protocoles utilisent des jetons (autorisation d'émission) que les machines d'un réseau peuvent s'échanger.
- La synchronisation : cette technique consiste à insérer des éléments tests dans le flot de données de manière à ne pas devoir reprendre la totalité d'une opération en cas d'échec.

C'est à travers la couche session qu'un utilisateur peut accéder à un système à temps partagé distant ou transférer des fichiers.

3.9. Couche présentation

Elle traite la syntaxe de l'information transmise. Elle assure l'encodage et/ou la compression des données dans une norme agréée.

Elle assure des conversions telles que celles des protocoles d'utilisation de terminaux incompatibles entre eux, celles entre les différents systèmes de fichiers ou encore celles des formats du courrier électronique.

3.10. Couche application

Cette couche assure l'interface entre l'utilisateur et les services du réseau. On y trouve toutes les applications cliente ou serveur connues : transfert de fichiers, courrier électronique, Web, multimédia, etc.

On distingue deux grands types de services au niveau application.

Pair à pair

> Avec ce mode de communication, les données sont directement échangées entre tous des hôtes (souvent appelés nœuds) qui exécutent un même programme.
>
> On peut imaginer un réseau de capteurs qui échangent leurs mesures directement entre eux en permanence. Ainsi, le superviseur ne doit interroger qu'un seul capteur pour connaître l'ensemble des mesures connues.

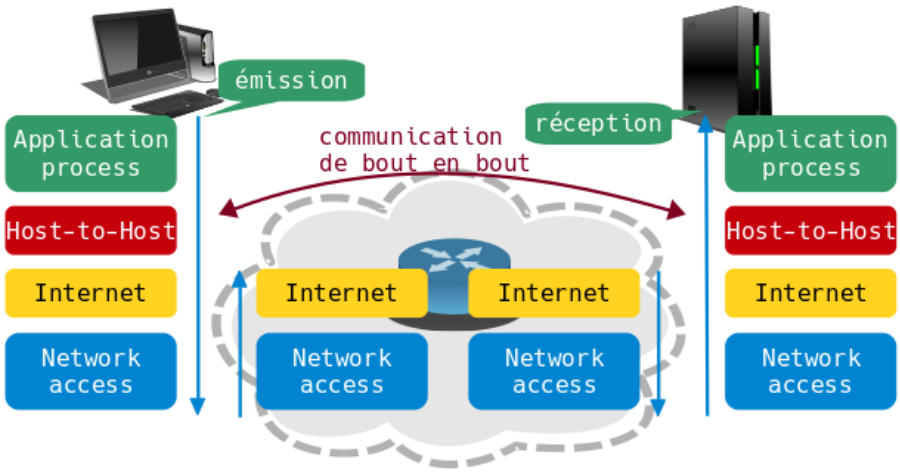
Client-serveur

> Dans ce contexte, les données sont détenues par un seul hôte : le serveur. Les clients doivent interroger le serveur pour obtenir ces données. Les programmes exécutés sont différents entre le serveur et ses clients. Le World Wide Web est l'exemple le plus emblématique de service client-serveur.

4. Modélisation TCP/IP

Le nom de ce modèle de référence provient de ses deux principaux protocoles. Ce modèle est apparu en 1974 avec la construction de l'ancêtre militaire de l'Internet, l'ARPANET. Les objectifs principaux de cette modélisation sont :

- relier des réseaux hétérogènes de façon transparente (lignes téléphoniques, réseaux locaux, etc),
- garantir les connexions quel que soit l'état des lignes de transmission (commutation de paquets),
- assurer le fonctionnement d'applications très différentes (transfert de fichier, multimédia, etc).



Network Access

La couche d'accès réseau a pour rôle de transmettre les données sur le média physique utilisé. En fonction du type de réseau, des protocoles différents peuvent être utilisés à ce niveau.

Internet

La couche inter-réseaux a pour rôle de transmettre les données à travers une série de réseaux physiques différents qui relient un hôte source avec un hôte destination. Les protocoles de routage sont étroitement associés à ce niveau. IP est le protocole routé de base sur l'Internet.

Host-to-Host

La couche hôte-à-hôte prend en charge la gestion de connexion, le contrôle de flux, la retransmission des données perdues et d'autres modes de gestion des flux. Les protocoles TCP et UDP sont dédiés à ces fonctions de transport.

Process/Application

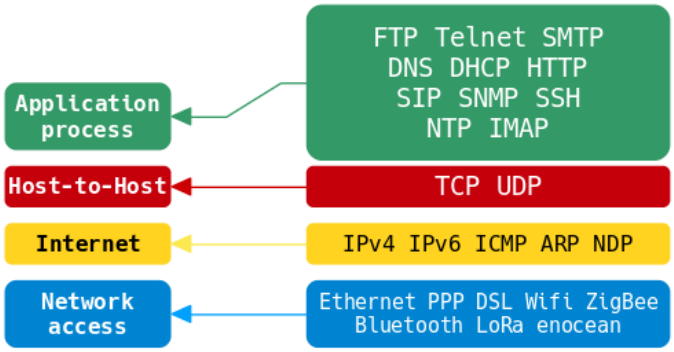
La couche application sert à l'exécution des protocoles de niveau utilisateur tels que les échanges de courrier électronique (SMTP), le transfert de fichiers (FTP) ou les connexions distantes (`telnet`).

4.1. Point fort : les protocoles

Le fait que ce modèle porte le nom de ces protocoles est lourd de signification. Si la démarche de recherche de consensus dans le développement du modèle s'apparente à la démarche suivie pour le modèle OSI, les spécifications ont été directement accessibles pour un public beaucoup plus large.

C'est ce principe de publication de RFC (Request for comments) qui a favorisé le développement des protocoles au profit du modèle. Tous les protocoles de l'Internet ont été «standardisés» à l'aide de ces documents. Lorsque quelqu'un met au point un protocole, il le soumet à la communauté à l'aide d'un document RFC. Ce travail est ensuite repris et amélioré par d'autres qui publient un nouveau RFC et ainsi de suite. C'est la démarche d'origine de développement des logiciels libres.

Ce travail à base de propositions ouvertes s'est montré très efficace puisqu'il a supplanté le modèle issu de l'ISO, l'organisme officiel de normalisation. Dès les premiers documents RFC, les piles de protocoles ont été illustrées.



4.2. Point faible : le modèle

La notion de modélisation n'est pas apparue comme une priorité relativement au développement des protocoles. Pour répondre aux objectifs du modèle Internet, ses développeurs ne se sont que très peu intéressés aux modes de transmission de l'information. Ils devaient utiliser l'existant de façon transparente. Le modèle Internet est donc très incomplet sur les aspects transmission.

En reprenant le principe à l'origine du réseau de communication militaire ARPANET, on doit pouvoir communiquer d'un point à un autre de l'Internet «quel que soit l'état du réseau». Une grande partie de l'infrastructure peut être détruite par une frappe nucléaire et les communications doivent toujours être possibles. C'est ce mode de fonctionnement singulier qui a conduit à l'adoption d'un réseau à commutation de paquets fonctionnant en mode non connecté sans aucune hiérarchie. Si un autre principe avec supervision, hiérarchie et mode connecté avait été retenu il suffirait qu'un point névralgique soit touché pour interrompre l'ensemble des communications.

C'est donc sur les couches basses qui traitent de la transmission de l'information que le modèle OSI conserve l'avantage. Le protocole IP est une implémentation particulière des fonctions de la couche réseau décrites dans le modèle OSI. De la même façon, les protocoles TCP et UDP sont des implémentations particulières des fonctions de la couche transport.

4.3. Couche Internet : le protocole IP

Pour répondre aux objectifs énoncés ci-dessus, le principe d'un réseau à commutation de paquets en mode non connecté a été retenu. Ce type de réseau correspond à un mode particulier d'utilisation de la couche réseau (3) du modèle OSI. Le fonctionnement de la couche réseau du modèle TCP/IP a été décrit pour la première fois dans le document standard RFC791 Internet Protocol.

Le rôle de la couche Internet est de transmettre des paquets sur n'importe quel type de liaison indépendamment les uns des autres. Les paquets émis dans un certain ordre peuvent ainsi être reçus dans un autre ordre en différents fragments.

Par principe, ce protocole ne dispose que de mécanismes de détection d'erreur. La correction d'erreur et donc la fiabilisation des communications ne se joue pas au niveau réseau mais au niveau transport avec le protocole TCP.

Le recours à la commutation de paquets a une autre conséquence. Chaque paquet doit contenir les adresses de l'émetteur et du destinataire. Ces adresses servent non seulement à identifier les extrémités en communication, mais elles sont aussi utilisées par les routeurs pour prendre leurs décisions d'acheminement du trafic entre ces extrémités.

Aujourd'hui, il existe deux versions de protocole IP.

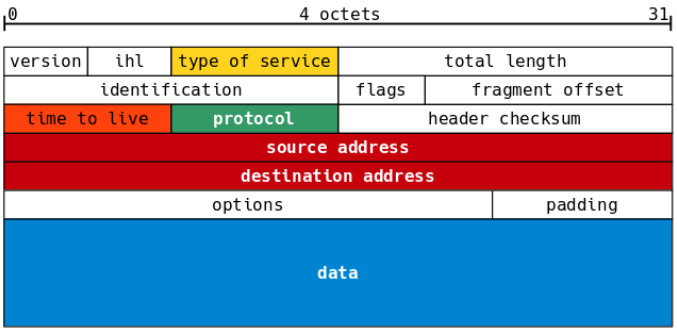
- Le protocole IPv4, dont les adresses sont représentées sur 32 bits, est le plus largement utilisé mais son espace d'adressage arrive à épuisement puisque toutes les adresses disponibles ont déjà été attribuées par l'IANA.

  Le document Adressage IPv4 présente le format des adresses du protocole IPv4 ainsi que les différentes évolutions des mécanismes de découpage du plan d'adressage en groupes logiques adaptés aux différents usages.

- Le protocole IPv6, dont les adresses sont représentées sur 128 bits, est adopté progressivement mais à un rythme très lent. Au delà du gain en espace d'adressage, l'en-tête IPv6 est plus simple que l'en-tête IPv4 et les

traitements d'analyse doivent être plus légers et raccourcir les temps de commutation dans les équipements d'interconnexion.

En-tête paquet IPv4



En-tête paquet IPv4

Version : 4 bits

Version du protocole IP codée sur 4 bits : `0100` pour IPv4 et `0110` pour IPv6.

Internet Header Length : 4 bits, IHL

Longueur de l'en-tête en mots de 32 bits. Cette valeur est utilisée pour distinguer la partie en-tête de la partie données du paquet. La représentation usuelle de l'en-tête se fait sur 32 bits de largeur. Comme les champs `Options` et `Padding` ne sont pas obligatoires, la valeur minimum du champ `IHL` est 5 (`0101`).

Type Of Service : 8 bits, TOS

Champ découpé en 2 parties. Les 3 premiers bits sont appelés precedence et les 5 derniers représentent le type de service. La définition d'origine prévoyait 3 choix : low-delay, high-reliability et high-throughput. Ce «marquage» des paquets est utilisable pour définir des flux prioritaires sur une interconnexion réseau «sous contrôle». Sur l'Internet, les opérateurs définissent leurs propres priorités ; donc leurs propres valeurs pour ce champ. Voir le document HOWTO du routage avancé et du contrôle de trafic sous Linux.

Total Length : 16 bits

Longueur du datagramme : en-tête & données. La taille minimum est de 21 octets (en-tête + 1 octet de donnée). Comme se champ est représenté sur 16 bits, la taille maximum est de 2^16 - 1, soit 64 Ko.

Identification : 16 bits

Chaque paquet IPv4 reçoit un numéro d'identification à sa création. Il est possible qu'un paquet soit découpé en fragments avant d'atteindre sa destination finale. Chaque fragment appartient au même paquet IPv4. Chaque fragment possède le même numéro d'identification.

Flags : 3 bits

Ce champ contient 3 indicateurs d'état :

- Reserved flag : doit toujours être à 0.
- Don't Fragment (DF) : à 0 si le paquet peut être fragmenté ; à 1 s'il ne doit pas être fragmenté.
- More Fragments (MF) : à 1 si d'autres fragments sont attendus ; à 0 s'il n'y a pas/plus de fragments.

Fragment Offset : 13 bits

Position du fragment dans le datagramme courant. Cette position est comptée en octets.

Time To Live : 8 bits, TTL

Ce compteur est décrémenté à chaque traversée de routeur. Si la valeur 0 est atteinte, le paquet est jeté. Cela signifie qu'il ne peut être délivré à sa destination finale. La valeur initiale du champ TTL dépend du système d'exploitation utilisé.

Protocol : 8 bits

Ce champ spécifie le protocole utilisé dans les données du paquet IP. Par exemple, la valeur 1 indique que le protocole utilisé est ICMP. On sait ainsi que ce paquet n'est pas destiné à une application. Les différentes valeurs de ce champs sont listées dans le fichier `/etc/protocols` sur les systèmes GNU/Linux ou *BSD.

Header Checksum : 16 bits

A chaque création ou modification d'un paquet, une somme de contrôle (cyclic redundancy check) est calculée sur son en-tête. Lorsque le paquet arrive à destination, cette somme est recalculée. Si le résultat diffère, c'est que le paquet a été endommagé lors de son trajet.

Source Address : 32 bits

Adresse IPv4 de l'hôte qui a émis le paquet.

Destination Address : 32 bits

Adresse IPv4 de l'hôte qui doit recevoir le paquet.

Options and Padding

Cette partie de l'en-tête est optionnelle. Ce champ est utilisé pour fournir des instructions spécifiques de distribution du paquet qui ne sont pas couvertes par les autres champs de l'en-tête. La taille maximum de ces instructions est limitée à 40 octets regroupés en double mots de 32 bits. Les bits de padding servent à compléter le dernier double mot de 32 bits.

Data

C'est le dernier champ du paquet IPv4. Il contient les données vues de la couche réseau. Celles ci peuvent débuter par un en-tête de couche transport (4) ou un message ICMP.

4.4. Couche Host-to-Host : les protocoles TCP & UDP

Avec la couche transport, on aborde le domaine des communications de bout en bout indépendantes de l'état du sous-réseau. Les paquets de la couche réseau peuvent être acheminés à destination par des chemins différents et dans le désordre. Par nature, le protocole IP n'offre pas de garantie. Les routeurs peuvent se débarrasser des paquets suivant plusieurs critères tels que des erreurs sur les sommes de contrôle, des congestions de trafic sur les interfaces réseau ou des adresses ne correspondant à aucune route connue. Tous les programmes et services de la couche application ne peuvent se contenter d'un mode de fonctionnement aussi «fragile». C'est une des raisons pour laquelle deux protocoles distincts ont été développés pour la couche transport.

4.5. Protocole TCP

Historiquement, TCP est le premier protocole de transport développé pour l'Internet. Les premières spécifications ARPANET prévoyaient un transport de l'information très fiable indépendant du type et de l'état du réseau. Le fonctionnement du protocole TCP a été décrit dans le document RFC793 Transmission Control Protocol.

- Protocole de bout en bout.
  Les processus pairs des couches transport de deux équipements connectés dialoguent l'un avec l'autre sans rien connaître du réseau sous-jacent. Les numéros de port source et destination présents dans l'en-tête de segment servent à adresser les processus de couche application en communication.

- Protocole orienté connexion.
  La fiabilité du transport TCP dépend de l'établissement d'une connexion entre les processus pairs qui veulent dialoguer. L'établissement d'une connexion est réalisé par l'échange d'informations telles que les numéros de ports, les numéros de séquence et la taille de fenêtre.

- Multiplexage à l'aide des numéros de ports.
  Les numéros de ports constituent le mécanisme d'adressage de la couche transport. Ils servent à désigner le processus de la couche application utilisé pour l'émission ainsi que celui utilisé pour la réception.

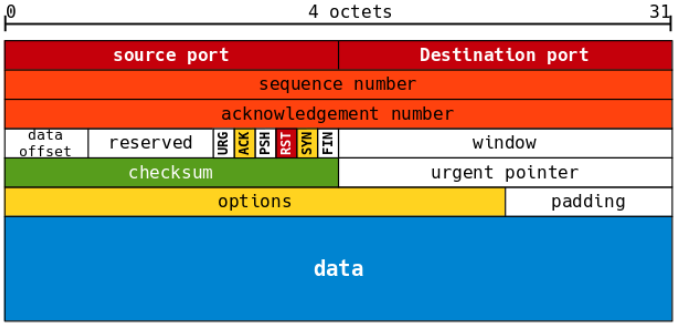
- Transfert de données segmenté et ordonné.
  Le flux des données issues de la couche application est segmenté et comptabilisé lors de l'encapsulation puis délivré dans le même ordre au processus qui le reçoit.

- Récupération sur erreur.
  L'utilisation des numéros de séquence et d'acquittement permet de comptabiliser les données transmises et de reprendre l'émission des données non reçues.

- Contrôle de flux avec fenêtrage.
  La combinaison de l'utilisation des numéros de séquence et d'acquittement avec la notion de fenêtre permet de contrôler la quantité de données à transmettre avant de procéder à un acquittement. Au début des échanges, la taille de fenêtre est réduite. Si aucune erreur ne survient, cette taille de fenêtre augmente suivant une règle définie. Au contraire, si des erreurs surviennent, la taille de fenêtre diminue de façon à augmenter le nombre des contrôles.

En-tête TCP

Les fonctions d'établissement, de maintien, de libération et de contrôle des échanges ont conduit au développement d'un en-tête comprenant un grand nombre de champs.



Source Port : 16 bits

Numéro du port source. Ce numéro correspond au point de communication (socket inet) utilisé par le service de la couche application de l'émetteur.

Destination Port : 16 bits

Numéro du port destination. Ce numéro correspond au point de communication (socket inet) utilisé par le service de la couche application du destinataire.

Sequence Number : 32 bits

Le protocole TCP a besoin de garder une trace de toutes les données qu'il reçoit de la couche application de façon à être sûr qu'elles ont bien été reçues par le destinataire. De plus, le protocole doit être sûr que ces données ont été reçues dans l'ordre dans lequel elles ont été envoyées. Il doit retransmettre toute donnée perdue.

On affecte un numéro de séquence à chaque octet de donnée pour en garder une trace lors du processus de transmission, réception et acquittement. Dans la pratique, ce sont des blocs d'octets qui sont gérés en utilisant les numéros de séquence de début et de fin de bloc.

Les numéros de séquence sont nécessaires à la mise en œuvre du système de fenêtre glissante du protocole TCP. C'est ce système qui garantit fiabilité et contrôle de flots de données.

Acknowledgment Number : 32 bits

Le rôle des numéros d'acquittement est le même que celui des numéros de séquence. Simplement, chaque extrémité en communication initie son propre jeu de numéros. Ainsi chaque extrémité assure la fiabilisation et le contrôle de flux de façon autonome.

Data Offset : 4 bits

Nombre de mots de 32 bits contenus dans l'en-tête TCP. Indication du début des données. Tout en-tête TCP, avec ou sans options, est un multiple de mots de 32 bits.

Reserved : 6 bits

Champ réservé pour une utilisation ultérieure. Les 6 bits doivent être à 0.

Control bits : 6 bits

Ces bits sont les indicateurs d'état qui servent à l'établissement, au maintien et à la libération des connexions TCP. Leur rôle est essentiel dans le fonctionnement du protocole.

- URG : indique que le champ Urgent Pointer est significatif. Une partie des données du segment sont urgentes.
- ACK : indique que le champ Acknowledgment field est significatif. Le segment acquitte la transmission d'un bloc de d'octets.
- PSH : indique à l'hôte en réception de «pousser» toutes les informations en mémoire tampon vers l'application en couche supérieure. L'émetteur notifie le récepteur qu'il a transmis toutes ses données «pour l'instant».
- RST : indique un arrêt ou un refus de connexion.
- SYN : indique une demande de synchronisation de numéro de séquence. Demande d'ouverture de connexion TCP.
- FIN : indique que l'émetteur n'a plus de données à transmettre. Demande de libération de connexion.

Window : 16 bits

Nombre d'octets de données à transmettre à partir de celui indiqué par le champ Acknowledgment.

Checksum : 16 bits

Somme de contrôle sur 16 bits de l'en-tête et des données.

Urgent Pointer : 16 bits

Ce champ est interprété uniquement si le bit de contrôle URG est à 1. Le pointeur donne le numéro de séquence de l'octet qui suit les données urgentes.

Options : variable entre 0 et 44 octets

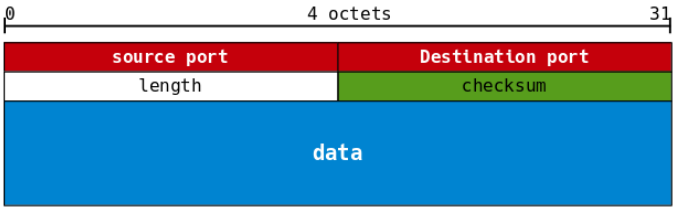
Il existe 2 formats d'options : un seul octet de catégorie d'option ou un octet de catégorie d'option suivi d'un octet de longueur d'option et de l'octet des données de l'option.

4.6. Protocole UDP

Le protocole UDP est apparu avec le développement des réseaux locaux dont la fiabilité est connue à priori. Il permet de s'affranchir des fonctions de contrôle. C'est un protocole minimum sans garantie de délivrance des messages et sans séquencement. En conséquence, l'en-tête est très nettement simplifié et le nombre de champs est très réduit.

Ce protocole présente un grand intérêt dans les applications orientées temps réel dans la mesure où il n'introduit aucune latence relativement aux fonctions de contrôle de flux de TCP.

En-tête UDP

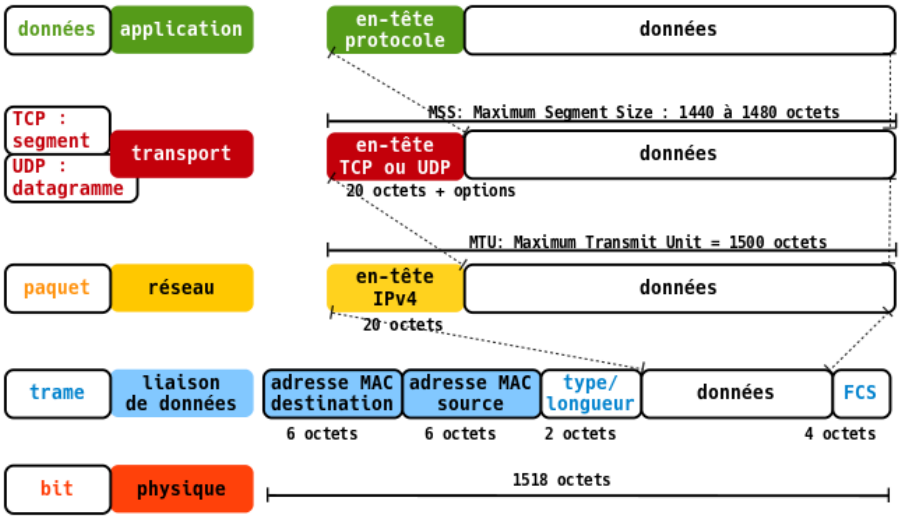


Les numéros de ports constituent le mécanisme d'adressage pour les communications de bout en bout comme dans le cas du protocole TCP.

4.7. Unités de données

Les protocoles listés ci-avant échangent des données entre eux lors du passage d'une couche à l'autre. On parle d'unité de donnée de protocole ou Protocol Data Unit (PDU) propre à chaque couche. De nos jours, on ne retrouve l'acronyme PDU que dans le contexte de l'étude du protocole Spanning Tree au niveau liaison de données.

Avec l'utilisation systématique des protocoles de l'Internet, l'acronyme PDU a laissé la place à des termes spécifiques à chaque couche. Voici un schéma sur lequel figure ces termes ainsi que les dimensions en octets de chaque élément.



Cette représentation fait apparaître le format de trame Ethernet. Même si la technologie Ethernet n'est pas directement liée aux protocoles de l'Internet, son format de trame tend à devenir universel. On le retrouve avec les technologies Wifi, les connexions ADSL ou FTTH avec PPPoE et même de plus en plus sur les réseaux étendus.

Avant 1997, date à laquelle l'IEEE a incorporé le format «historique» de trame Ethernet dans le standard officiel, on devait systématiquement distinguer deux formats de trames suivant le champ Type/Longueur.

- La définition de trame Ethernet II, celle qui utilise le champ type, a été intégrée avec les protocoles de l'Internet à partir des documents RFC894 Standard for the transmission of IP datagrams over Ethernet networks et RFC1042 Standard for the transmission of IP datagrams over IEEE 802 networks. Le champ type de la trame indique le type du protocole de couche supérieure ; IP ou ARP dans la plupart des cas. Pour plus d'informations, voir la référence sur les ETHER TYPES.

- La définition de trame IEEE 802.3 initiale, celle qui utilise le champ longueur, n'est jamais utilisée pour le trafic IP ; donc pour le trafic utilisateur. Seules les communications spécifiques entre équipements réseau utilisent ce format de trame associé à des protocoles spécifiques.

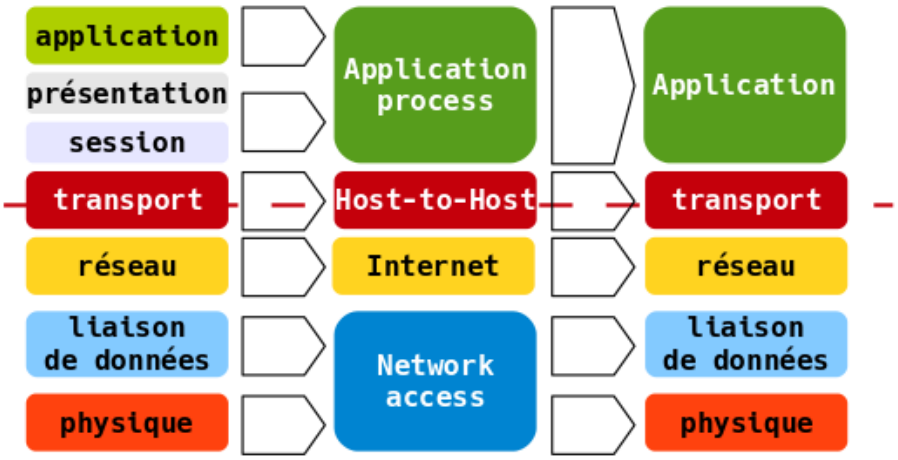
5. Modèle Contemporain

Cette dénomination n'a vraiment rien d'officiel. Elle signifie simplement qu'actuellement la conception et l'exploitation des réseaux se fait à partir de la synthèse entre le modèle OSI et le modèle Internet.

Chaque modèle a compensé les faiblesses de l'autre.

- Le modèle OSI a structuré les relations entre les couches basses.
  Sans ce travail de normalisation, l'évolution des réseaux de télécommunications était compromise. L'interconnexion entre systèmes propriétaires hétérogènes aurait toujours posé problème.

- Le modèle Internet a structuré les protocoles d'applications par services.
  C'est le développement libre des services (noms de domaine, courrier, Web) au dessus des couches basses du réseau en tenant compte des infrastructures existantes qui a permis l'explosion de l'Internet là où les spécifications trop lourdes ont complètement échoué.



On peut aussi illustrer la comparaison entre les deux modèles en partant du positionnement des protocoles TCP (RFC793 Transmission Control Protocol : Transmission Control Protocol) et IP (RFC791 Internet Protocol : Internet Protocol) qui datent de 1981.

```
Couches| Couches     | RFC 791                                    |Système
OSI    | TCP/IP      |                                            |d'exploitation
-------+-------------+--------------------------------------------+--------------
 7     |             |+------+ +-----+ +-----+     +-----+        |Processus
 6     | Application||Telnet| | FTP | | TFTP| ... | ... |        | utilisateur
 5     |             |+------+ +-----+ +-----+     +-----+        |'userspace'
       |.............|      |   |         |           |           |..............
       |             |     +-----+     +-----+     +-----+       |Sous système
 4     | Transport   |     | TCP |     | UDP | ... | ... |       | du noyau
       |             |     +-----+     +-----+     +-----+       |'kernelspace'
       |.............|        |           |           |          | . . . . . . .
       |             |     +---------------------------+----+    |Adressage
 3     | Réseau      |     |    Internet Protocol & ICMP    |    |Logique
       |             |     +---------------------------+----+    |
       |.............|                   |                       | . . . . . . .
 2     |             |       +---------------------------+       |Adressage
 1     | Accès       |       |   Local Network Protocol  |       |Physique
       |             |       +---------------------------+       |
```

6. En guise de conclusion

Une fois les concepts des modélisations réseau introduits, une bonne compréhension du fonctionnement de chaque couche suppose que l'on se penche sur les technologies et les protocoles correspondants. En remontant les niveaux du modèle contemporain proposé ci-avant, voici la liste des articles et des supports de cours à consulter suivie d'un glossaire sur les acronymes couramment utilisés.

6.1. Documents de référence

Technologie Ethernet

La technologie Ethernet et les normalisations IEEE 802.3 dominent très largement aux niveaux physique (couche 1) et liaison (couche 2) dans le monde des réseaux locaux. Voir Technologie Ethernet.

Adressage IPv4

L'adressage IPv4 synthétise les caractéristiques de fonctionnement du protocole de niveau réseau (couche 3) du modèle TCP/IP. Voir Adressage IPv4.

Analyse réseau

Toutes les descriptions académiques «livresques» ne valent pas grand chose sans illustration à partir du trafic réseau réel. L'analyse réseau est l'outil pédagogique fondamental pour s'assurer d'une bonne compréhension des mécanismes de fonctionnement des protocoles réseau. Voir Introduction à l'analyse réseau avec Wireshark.

6.2. Glossaire des acronymes

ARCEP

ARCEP : Autorité de Régulation des Communications Électroniques et des Postes

ARPANET

ARPANET : Advanced Reseach Projects Agency NETwork

Ancêtre militaire de l'Internet développé aux États-Unis à partir des années 60.

IANA

IANA : Internet Assigned Numbers Authority (IANA)

Organisme responsable de l'attribution des préfixes d'adresses IPv4 et IPv6 ainsi que des numéros de systèmes autonomes.

IEEE

IEEE : Institute of Electrical and Electronics Engineers

Organisme responsable de la publication des normes sur les technologies réseaux notamment Ethernet.

ISO

International Standard Organisation : International Organization for Standardization

Organisme international responsable de la publication de nombreuses normes dont la modélisation OSI.

ITU

ITU : International Telecommunication Union

Organisme international responsable de la publication des normes sur les télécommunications.

OSI

OSI : Open Systems Interconnection

Le Modèle de référence de base pour l'interconnexion de systèmes ouverts est une norme (ISO 7498) composée de 4 parties :

- Le modèle de base
- Architecture de sécurité
- Dénomination et adressage

- Cadre général de gestion

Seule la première partie est abordée dans le présent article.

SNA

SNA : Systems Network Architecture

Modélisation propriétaire promue par IBM dans les années 70 et aujourd'hui abandonnée.