SYSTÈMES ET RÉSEAUX

Aix*Marseille université

Licence MIAGE

Configuration et gestion d'un serveur

Chapitre 4 : TCP/IP : une pile de protocoles !

Objectifs :

Maîtriser la composition et le rôle des différents protocoles du modèle TCP-IP et la notion d'encapsulation des données.

Plan :

1. Que signifie TCP/IP ?

TCP/IP n'est pas un protocole mais une suite de protocoles.
Le sigle TCP/IP signifie "Transmission Control Protocol/Internet Protocol".
Il provient des noms des deux protocoles majeurs de la suite de protocoles, c'est-à-dire les protocoles TCP et IP.

TCP/IP représente d'une certaine façon l'ensemble des règles de communication sur Internet et se base sur la notion adressage IP, c'est-à-dire le fait de fournir une adresse IP à chaque machine du réseau afin de pouvoir acheminer des paquets de données. Etant donné que la suite de protocoles TCP/IP a été créée à l'origine dans un but militaire, elle est conçue pour répondre à un certain nombre de critères parmi lesquels :

- Le fractionnement des messages en paquets ;
- L'utilisation d'un système d'adresses ;
- L'acheminement des données sur le réseau (routage) ;
- Le contrôle des erreurs de transmission de données.

La connaissance de l'ensemble des protocoles TCP/IP n'est pas essentielle pour un simple utilisateur, au même titre qu'un téléspectateur n'a pas besoin de connaître le fonctionnement de son téléviseur, ni des réseaux audiovisuels.
Toutefois, sa connaissance est nécessaire pour les personnes désirant administrer ou maintenir un réseau TCP/IP, ou un webmaster qui pourrait un jour être amené à travailler … sur Internet :-p .

2. TCP/IP est un modèle en couches.

2.1. Présentation.

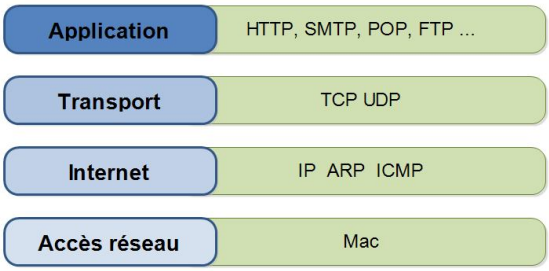
Le modèle TCP/IP, initialement appelé modèle DOD, car développé par le "Department Of Defense" américain, toujours sous la houlette de l'ARPA.

Afin de pouvoir appliquer le modèle TCP/IP à n'importe quelle machine, c'est-à-dire indépendamment du système d'exploitation, le système de protocoles TCP/IP a été décomposé en plusieurs modules effectuant chacun une tâche précise. De plus, ces modules effectuent ces tâches les unes après les autres dans un ordre précis, on a donc un système stratifié, c'est la raison pour laquelle on parle de modèle en couches.

Le terme de couche est utilisé pour évoquer le fait que les données qui transitent sur le réseau traversent plusieurs niveaux de protocoles. Ainsi, les données (paquets d'informations) qui circulent sur le réseau sont traitées successivement par chaque couche, qui vient rajouter un élément d'information (appelé entête) puis sont transmises à la couche suivante.

Le modèle TCP/IP est très proche du modèle OSI (modèle comportant 7 couches) qui a été mis au point par l'organisation internationale des standards (ISO, organisation internationale de normalisation) afin de normaliser les communications entre ordinateurs.

2.2. Le modèle TCP/IP



Modèle DOD ou TCP/IP

Les rôles des différentes couches sont les suivants :

Couche Accès réseau : elle spécifie la topologie réseau c'est-à-dire la forme sous laquelle les données doivent être acheminées quel que soit le type de réseau utilisé. Les protocoles présents sur cette couche sont Ethernet, FDDI, Token Ring, …
Cette couche met en évidence le système d'adressage Mac des interfaces réseau.
Pour rappel, une adresse Mac, pour Media Access Control, est l'adresse physique, supposée unique, de l'interface réseau, composée de 3 octets identifiant le fabricant et de 3 octets codant le numéro de série de l'interface.
C'est l'organisation OUI (Organizationally Unique Identifier), gérée par l'IEEE, qui gère et distribue ces adresses. Par exemple, 00:19:5B, 00:1E:58 et plein d'autres représentent le constructeur D-Link.

Couche Internet : elle est chargée de fournir le paquet de données (datagramme). Le protocole principal de cette couche est le protocole IP, qui permet de spécifier l'adresse IP d'une interface réseau.
D'autres protocoles composent également cette couche :
ARP : protocole qui permet d'interroger le réseau à la recherche de l'adresse Mac qui correspond à une adresse IP spécifiée.
ICMP : protocole qui permet de tester les communications sur un réseau, entre autre grâce à la commande PING.

Couche Transport : elle assure l'acheminement des données, ainsi que les mécanismes permettant de connaître l'état de la transmission.
TCP est le premier protocole de la couche Transport. UDP est le second.
Le premier est un protocole dit connecté et plus sécurisé : les communications ne s'effectueront entre les interfaces réseau qu'après une phase de connexion non authentifiée, garantissant que les deux interfaces sont prêtes à communiquer. De plus, des trames d'accusés de réception sont émises toutes les deux trames échangées, et des mécanismes de vérification de l'intégrité des trames et de réémission en cas d'erreurs.
A l'inverse, UDP est plus rapide car les données sont émises même si le destinataire n'est pas à l'écoute, sans contrôle de réception ou d'intégrité. Ce protocole est privilégié pour les réseau à priorité de vitesse ou sans besoin de garantie, comme la ToIP, le Peer to peer ou encore DHCP. Généralement, ce sont les applications qui gère la qualité de l'information.

Pour les deux, les trames sont fragmentées afin de leur garantir une taille optimale, fixée sur Internet à 1500 octets. Cela s'appelle le MTU.
Ces protocoles savent alors numéroter les paquets d'un même message pour permettre de le recomposer à l'arrivée.

Ce sont également ces protocoles transport qui adressent les paquets en leur affectant un numéro de port.

Couche Application : elle englobe les protocoles applications standard du réseau (HTTP, SMTP, FTP, ...). TCP/IP est un protocole de communication réseau, aucune application n'est présente ici.

3. La gestion des ports de la couche Transport.

Les ports sont des canaux de communications qui garantissent la présentation des données au bon protocole de la couche application.

3.1. Les ports d'écoute des serveurs.

Un serveur exécute un ou plusieurs services réseau, en permanence à l'écoute, qui attend des requêtes des clients. Chaque service est alors associé à un port, sur lequel il va recevoir les requêtes.
Plusieurs services sur un même serveur ont chacun un ou parfois plusieurs ports unique sur le serveur.
Par exemple, sur un serveur web classique, on peut trouver les services HTTP, HTTPS, mariaDB, SSH et FTP (voir d'autres).

3.2. Les ports de réponse.

Chaque client, lorsqu'il émet une requête à l'intention d'un service, précise le port prédéfini pour le service ou sur un port autre connu à l'avance.
Il fixe également, au hasard parmi ceux libres, un port sur lequel il attend la réponse à sa requête, également appelé port établi. Chaque client gère ses propres ports. Rien n'interdit que plusieurs clients utilisent le même port établi.

3.3. Les ports bien connus.

Une liste prédéfinie de ports est établie pour que chaque service standard d'Internet soit accessible par tous. Les clients savent donc à l'avance sur quel port envoyer une requête. Il s'agit des 1024 premiers ports, appelé les Well Known Ports. Vous pourrez les trouver à cette adresse : www.frameip.com/
En voici quelques un à connaître :

Port	Protocole	Usage
20	ftp-data	Transfert des données
21	ftp	Connexion au serveur et exploration de son arborescence
22	ssh	Connexion distante sécurisée
25	smtp	Envoi de courriels
53	dns	Résolution d'adresses URL
80	http	Serveur Web
110	pop3	Récupération de courriels
443	https	Serveur web sécurisé
465	smtps	Envoi sécurisé de courriels
996	pop3s	Récupération sécurisée de courriels

3.4. Le choix des ports.

Par exemple, un navigateur web qui demande la page https://www.gap.univ-mrs.fr/miw/index.php émettra toutes ses requêtes à destination du port 443.
Un premier port de réponse est choisi. Ces deux ports (serveur/destination et client/origine) sont indiqué dans la trame, dans l'entête Transport.

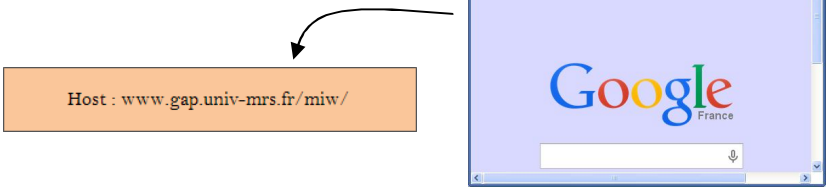
En recevant la page index.php, le navigateur constate qu'il doit récupérer d'autres fichiers (style.css, script.js, fond.jpg, …). Toutes ces requêtes seront émises simultanément, avec des ports établis différents.

Ainsi, toutes les réponses seront acheminées au bon endroit.

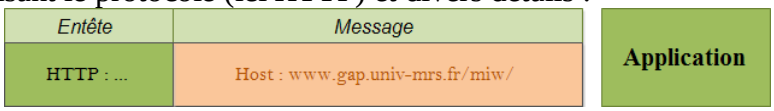
4. Encapsulation des données.

Les trames sont composées en partant des données fournies par l'application, traitées par le protocole **Application**, puis par le protocole **Transport**, puis par le protocole **Internet** et enfin par le protocole **Ethernet**.

Prenons l'exemple d'une requête web saisie dans le navigateur par l'utilisateur qui souhaite obtenir la page : http://www.gap.univ-mrs.fr/miw/

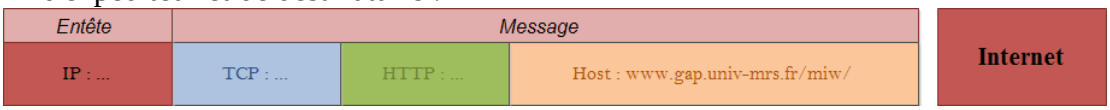


L'application transmet son message à la couche **Application**, en précisant qu'il s'agit d'une requête HTTP. L'entête de la couche est alors généré, en précisant le protocole (ici HTTP) et divers détails :

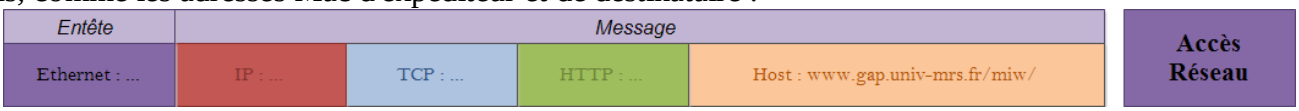


La couche **Application** envoie ce qu'elle a généré à la couche **Transport**.
L'entête de la couche **Transport** est alors généré, en précisant le protocole (ici TCP), les ports source et destination et divers détails :

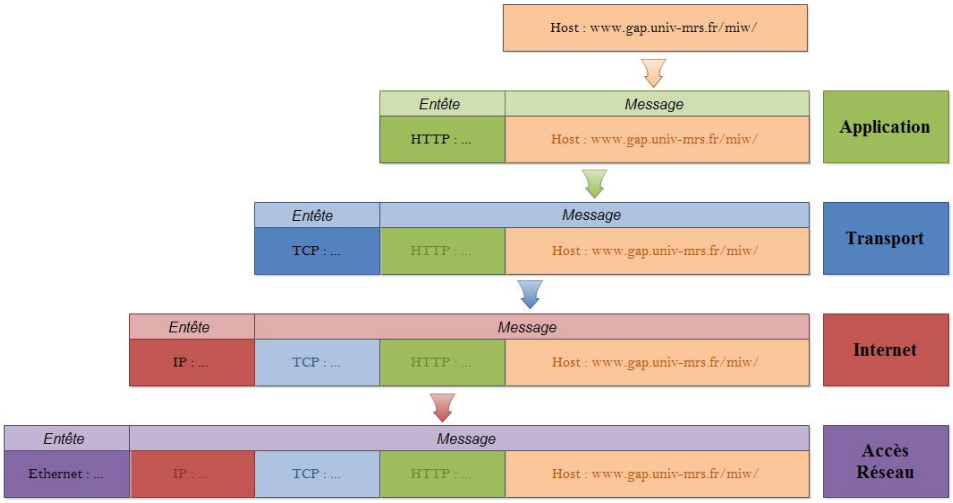
La couche **Transport** envoie ce qu'elle a généré à la couche **Internet**.
L'entête de la couche **Internet** est alors généré, en précisant le protocole (IPv4 ou IPv6) et divers détails, comme les adresses IP d'expéditeur et de destinataire :



La couche **Internet** envoie ce qu'elle a généré à la couche **Accès Réseau**.
L'entête de la couche **Accès Réseau** est alors généré, en précisant le protocole (ici Ethernet) et divers détails, comme les adresses Mac d'expéditeur et de destinataire :



Globalement cela donne :



Chez le destinataire, hormis quelques modifications apportées dans les entêtes Ethernet et IP durant le voyage, la trame est la même.

Elle remonte les couches pour être interprétée au mieux, et arriver à l'application destinataire.