Chapitre 1: Couche transport et couche application du protocole TCP/IP

1.1 Couche transport TCP/IP

1.1.1 Introduction à la couche transport
1.1.2 Contrôle de flux
1.1.3 Établissement, maintenance et fermeture de session
1.1.4 Échange en trois étapes
1.1.5 Fenêtrage
1.1.6 Accusé de réception
1.1.7 Protocole TCP (Transmission Control Protocol)
1.1.8 Protocole UDP (User Datagram Protocol)
1.1.9 Numéros de port TCP et UDP

1.2 La couche application

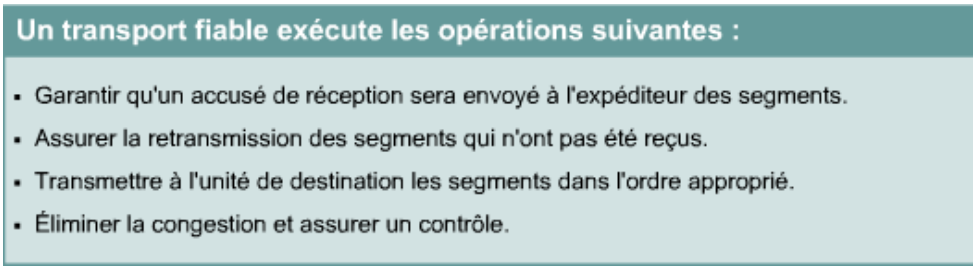
1.2.1 Introduction à la couche application du modèle TCP/IP
1.2.2 DNS
1.2.3 FTP and TFTP
1.2.4 HTTP
1.2.5 SMTP
1.2.6 SNMP
1.2.7 Service Telnet

La couche transport du modèle TCP/IP achemine les données entre les applications des machines source et de destination. Pour comprendre les réseaux de données actuels, il est capital de bien connaître le mécanisme de la couche transport. Ce module a pour objectif de décrire les fonctions et les services de cette couche.
Bon nombre des applications réseau intervenant au niveau de la couche application TCP/IP sont déjà connues des utilisateurs des réseaux. Les acronymes HTTP, FTP et SMTP sont familiers aux utilisateurs de navigateurs Web et de clients de messagerie. Ce chapitre présente également le rôle de ces applications, entre autres, du modèle de réseau TCP/IP.

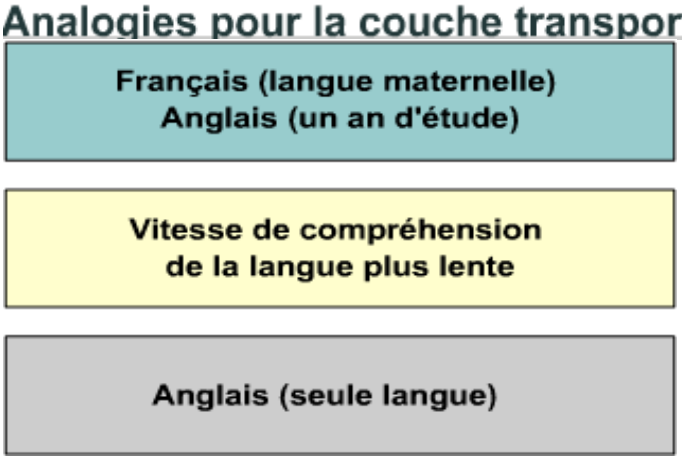
1.1 Couche transport TCP/IP

1.1.1 Introduction à la couche transport

Le rôle principal de la couche transport est d'acheminer et de contrôler le flux d'informations de la source à la destination, de manière fiable et précise. Le contrôle de bout en bout ainsi que la fiabilité sont assurés grâce aux fenêtres glissantes, aux numéros de séquence et aux accusés de réception.



Pour mieux comprendre les concepts de fiabilité et de contrôle de flux, imaginez une personne qui apprend une langue étrangère pendant un an avant de se rendre dans le pays en question. Au cours d'une conversion, certains mots seront répétés pour assurer la fiabilité de la compréhension. Les interlocuteurs doivent par ailleurs parler lentement afin de se faire comprendre, ce qui peut être associé au contrôle de flux.

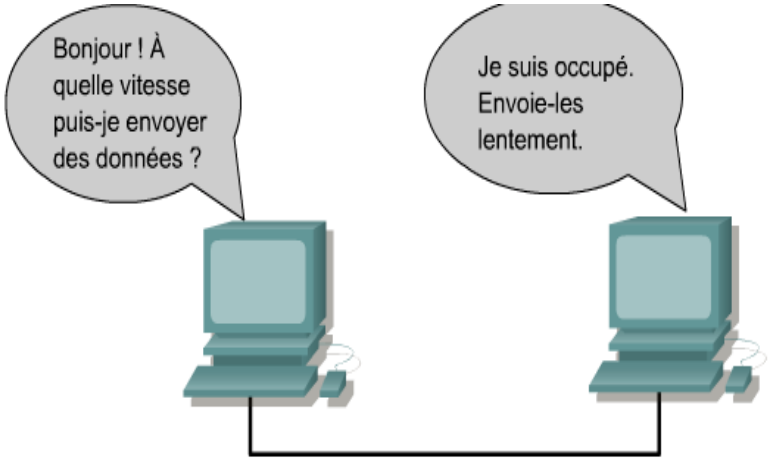


La couche transport établit une connexion logique entre deux points d'extrémité d'un réseau. Les protocoles de cette couche segmentent et rassemblent les données envoyées par les applications de couche supérieure en un flux de données identique, qui offre des services de transport de bout en bout.
Les deux principaux rôles de la couche transport sont donc le contrôle de flux et la fiabilité. Elle définit une connectivité de bout en bout entre les applications hôtes. Voici quelques services de transport de base:

- Segmentation des données d'application de couche supérieure.
- Établissement d'une connexion de bout en bout.
- Transport des segments d'un hôte d'extrémité à un autre.
- Contrôle du flux assuré par les fenêtres glissantes.
- Fiabilité assurée par les numéros de séquence et les accusés de réception.

TCP/IP est une combinaison de deux protocoles distincts : IP et TCP. IP opère au niveau de la couche 3 du modèle OSI et est un protocole non orienté connexion offrant un acheminement au mieux (best-effort delivery) sur le réseau. TCP opère au niveau de la couche transport. C'est un service orienté connexion qui assure le contrôle du flux et la fiabilité. Combinés, ces deux protocoles offrent une gamme de services plus vaste. Ils constituent la base de la pile de protocoles TCP/IP, et c'est sur cette pile de protocoles que repose Internet.

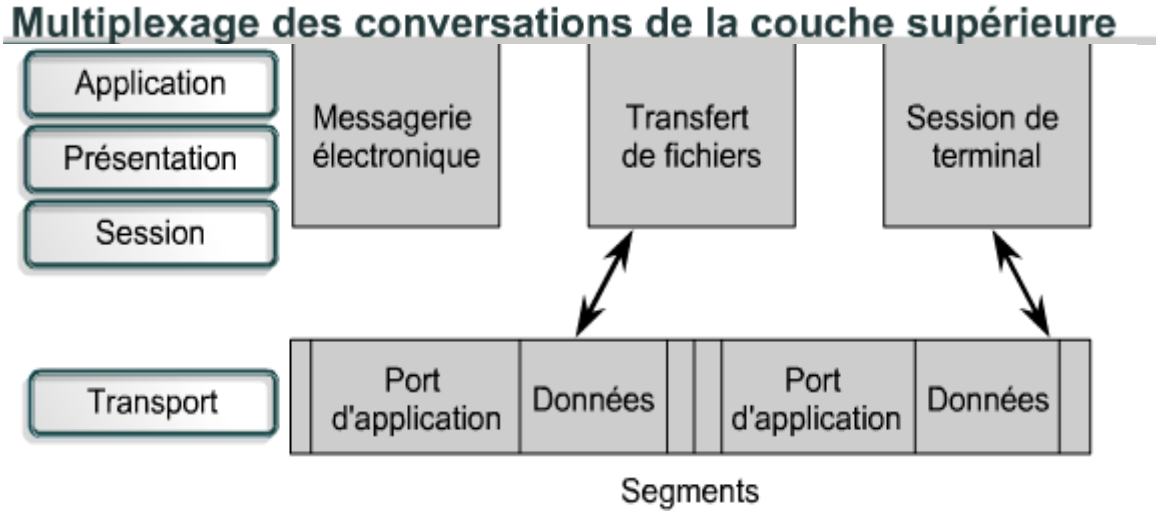
1.1.2 Contrôle de flux



Lorsque la couche transport envoie des segments de données, elle cherche à s'assurer que les données ne se perdent pas. Des données peuvent en effet être perdues si un hôte n'est pas capable de les traiter suffisamment vite au fur et à mesure qu'il les reçoit. Il est alors obligé de les rejeter. Le contrôle de flux permet d'éviter le dépassement de capacité des mémoires tampons d'un hôte de destination. Pour ce faire, TCP met en relation les hôtes source et de destination qui conviennent alors d'un taux de transfert des données acceptable

1.1.3 Établissement, maintenance et fermeture de session

Les applications envoient des segments de données suivant la méthode du premier arrivé, premier servi. Les segments les premiers arrivés sont pris en charge les premiers. Ils peuvent être acheminés vers une même destination ou vers des destinations différentes. Dans le modèle de référence OSI, plusieurs applications peuvent partager la même connexion de transport. On parle alors de multiplexage des conversations de couche supérieure. Plusieurs conversations simultanées de couche supérieure peuvent être multiplexées sur une seule connexion.

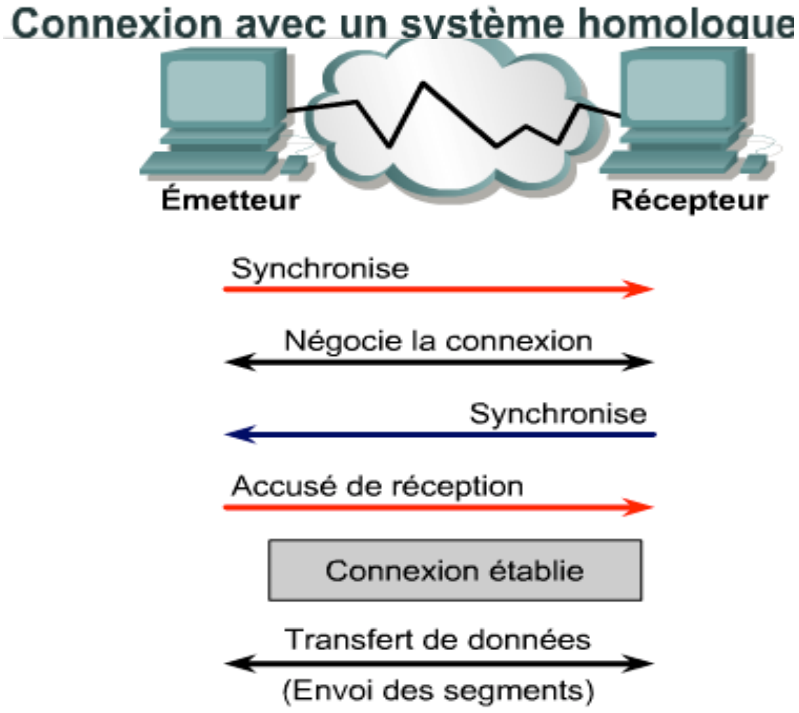


Un des rôles de la couche transport est d'établir une session orientée connexion entre des unités identiques de la couche application. Pour que le transfert de données puisse débuter, les applications source et de destination doivent informer leur système d'exploitation qu'une connexion va être initiée. Un des nœuds initie la connexion qui doit obligatoirement être acceptée par l'autre. Les modules logiciels de protocole des deux systèmes d'exploitation communiquent en envoyant des messages sur le réseau pour vérifier si le transfert est autorisé et si les deux ordinateurs sont prêts.

La connexion est établie et le transfert des données peut commencer après synchronisation. Pendant le transfert, les deux ordinateurs continuent de communiquer au moyen de leur logiciel de protocole pour vérifier si les données sont bien reçues.

La figure montre une connexion type établie entre deux systèmes. La première étape du protocole d'échange bidirectionnel demande la synchronisation. Le deuxième échange accuse réception de la demande de synchronisation initiale et synchronise les paramètres de connexion dans la direction opposée. Le troisième

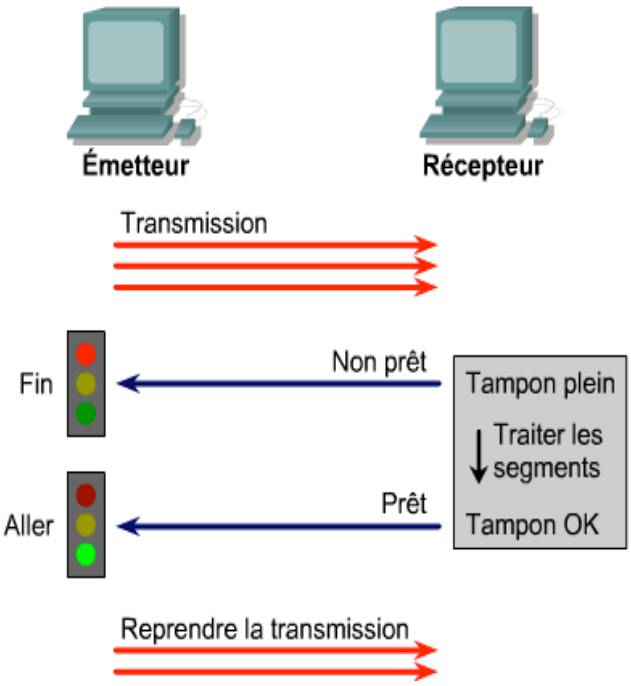
segment d'échange est un accusé de réception indiquant à la destination que la connexion peut être établie des deux côtés. Une fois la connexion établie, le transfert des données commence.



Une congestion peut se produire lors de deux situations:

- Lorsqu'un ordinateur génère un trafic dont le débit est plus rapide que la vitesse de transfert du réseau.
- Lorsque plusieurs ordinateurs doivent envoyer simultanément des datagrammes à une même destination (celle-ci peut alors devenir encombrée, même si le problème ne provient pas d'une seule source).

Lorsque des datagrammes arrivent trop rapidement et que l'ordinateur ou la passerelle ne peut les traiter, ils sont stockés temporairement en mémoire. Si le trafic continue, la mémoire de l'hôte ou de la passerelle finit par être saturée et les datagrammes qui arrivent doivent être abandonnés.



Contrôle de flux

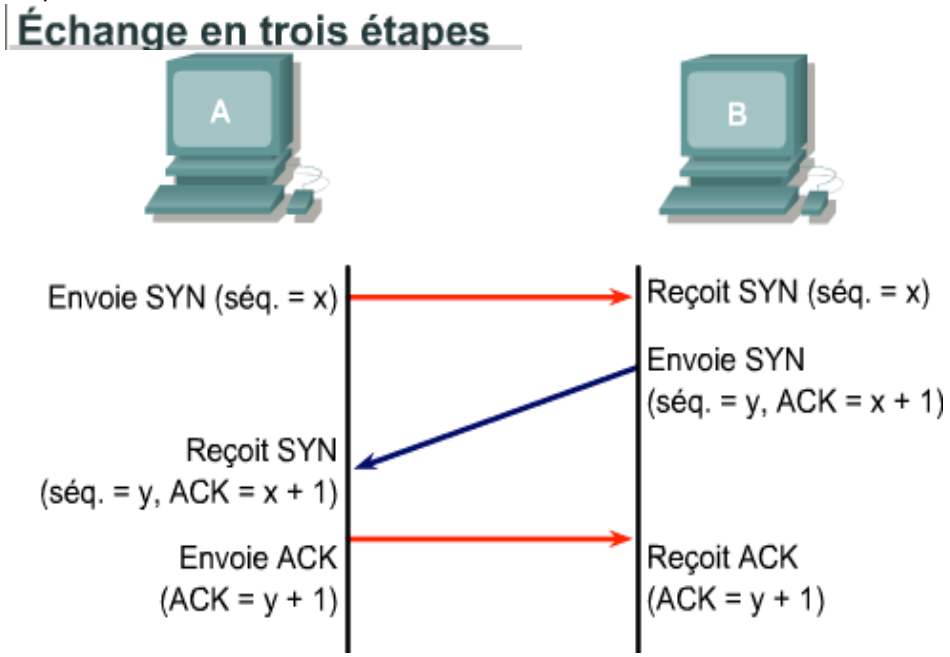
Pour éviter la perte des données, le processus TCP de l'hôte récepteur envoie un indicateur «non prêt» à l'émetteur, afin que ce dernier arrête de transmettre. Lorsque le récepteur peut accepter de nouvelles données, il envoie l'indicateur de transport «prêt» à l'émetteur qui reprend alors la transmission des segments.

Une fois le transfert des données terminé, l'hôte source envoie un signal indiquant la fin de la transmission. L'hôte de destination accuse réception et la connexion se termine.

1.1.4 Échange en trois étapes

Le protocole TCP est orienté connexion. Une connexion doit par conséquent être établie avant le début du transfert des données. Pour établir cette connexion, les deux hôtes doivent synchroniser leurs numéros de séquence initiaux (ISN – Initial Sequence Number). La synchronisation s'effectue par le biais d'un échange de segments transportant un bit de contrôle SYN (synchroniser) et les numéros de séquence initiaux. Cette méthode nécessite une opération pour sélectionner les numéros de séquence initiaux et un protocole d'échange bidirectionnel pour les échanger.

Au cours de la synchronisation, chaque hôte envoie son propre numéro de séquence initial et reçoit une confirmation de cet échange via un accusé de réception (ACK) envoyé par l'autre hôte. Chaque hôte doit donc recevoir le numéro de séquence initial envoyé par l'autre hôte et répondre en envoyant un message ACK. La séquence est la suivante:



1. L'hôte émetteur (A) initie une connexion en envoyant un paquet SYN à l'hôte récepteur (B) indiquant que son numéro de séquence initial ISN = X:
   A —> B SYN, séq. de A = X
2. B reçoit le paquet, enregistre que la séq. de A = X, répond par un accusé de réception de X + 1 et indique que son numéro de séquence ISN = Y. L'accusé X + 1 signifie que l'hôte B a reçu tous les octets jusqu'à X inclus et qu'il attend l'arrivée de X + 1:
   B —> A ACK, séq. de A = X, SYN séq. de B = Y, ACK = X + 1
3. L'hôte A reçoit le paquet de B, apprend que la séquence de B est Y et répond par un accusé de Y + 1, qui met fin au processus de connexion:
   A —> B ACK, séq. de B = Y, ACK = Y + 1

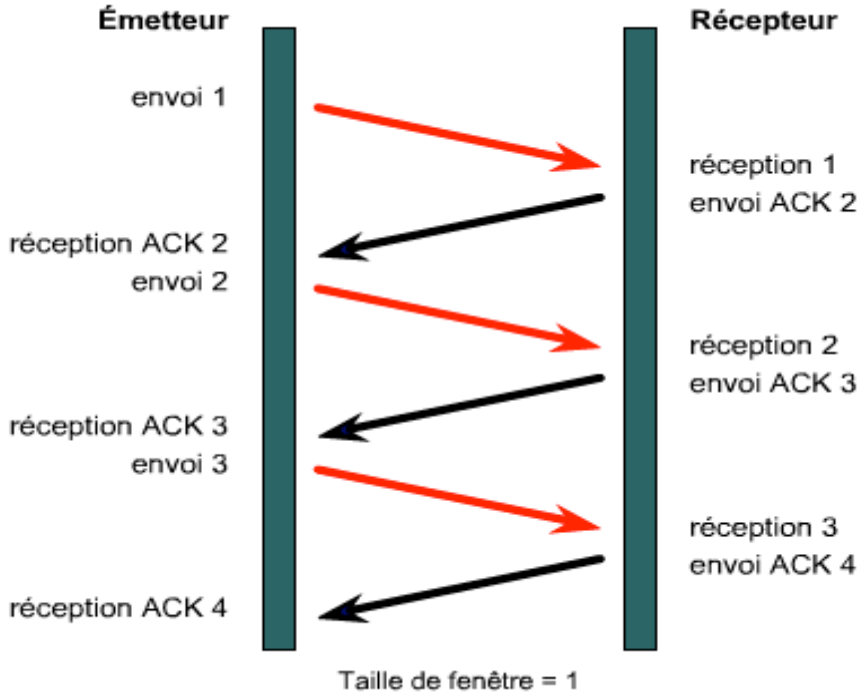
Cet échange est un échange en trois étapes.

Il est essentiel car les numéros de séquence ne reposent pas sur une horloge universelle sur le réseau et les méthodes utilisées par les protocoles TCP pour choisir les numéros de séquence initiaux peuvent différer. Le récepteur du premier SYN ne peut savoir si le segment a été différé à moins de conserver une trace du dernier numéro de séquence utilisé dans la connexion. Sans cette information, il doit demander à l'émetteur de vérifier le SYN.

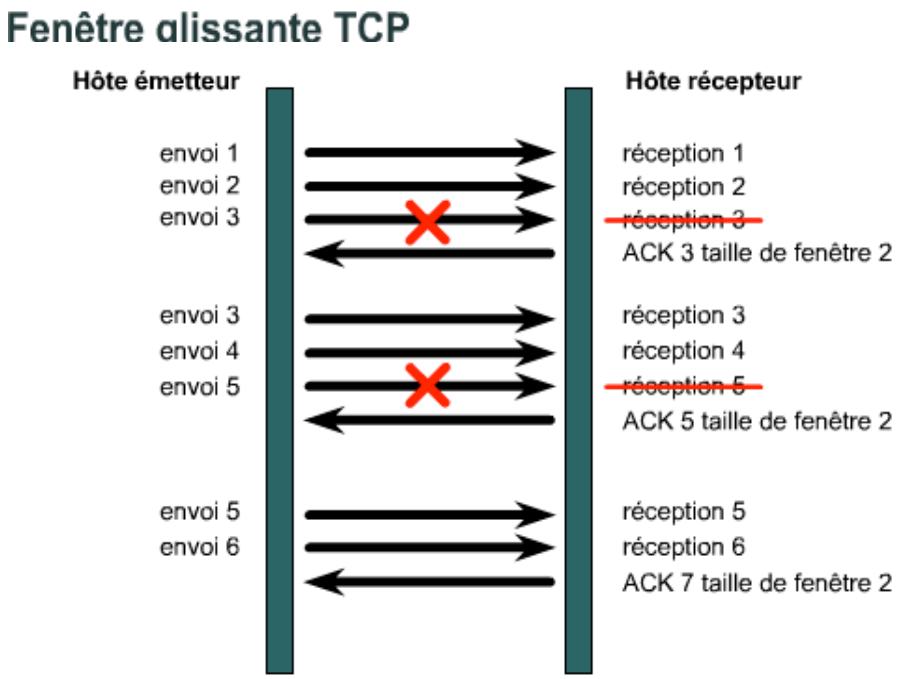
1.1.5 Fenêtrage

Pour qu'un transfert de données soit orienté connexion et fiable, les paquets de données doivent être délivrés au destinataire dans le même ordre que celui dans lequel ils ont été transmis. Le protocole échoue si des paquets de données sont perdus, endommagés, dupliqués ou reçus dans un ordre différent. Une solution simple consiste, pour le destinataire, à accuser réception de chacun des paquets avant que le paquet suivant ne lui soit envoyé.

Fenêtre de base TCP



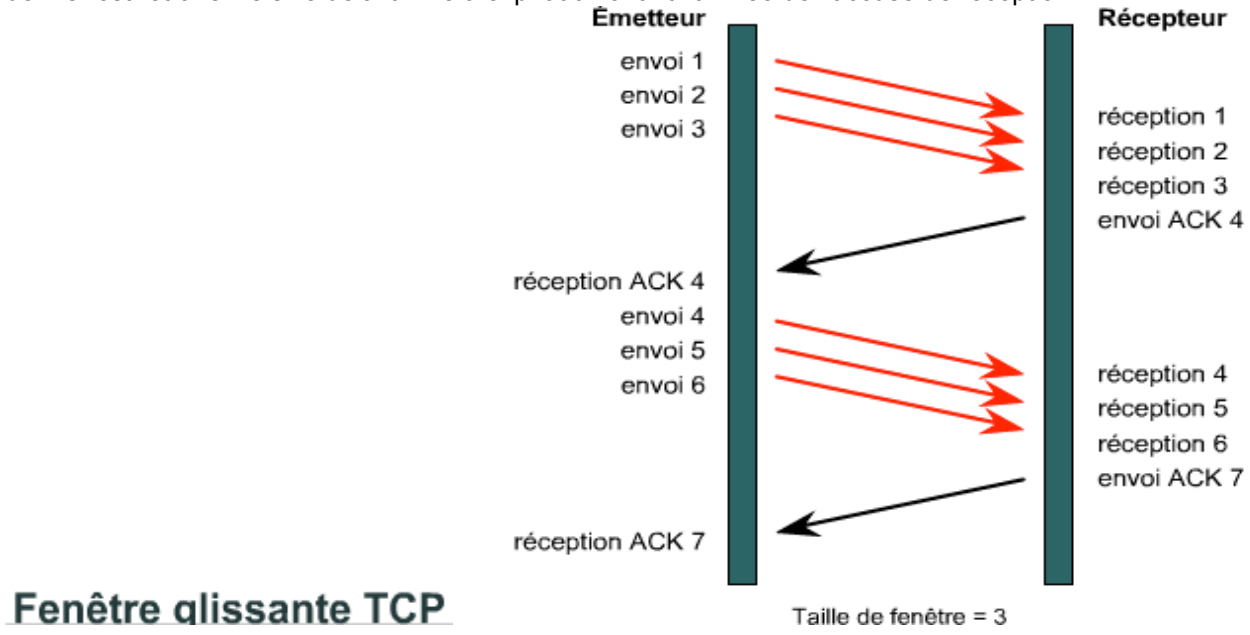
Toutefois, si l'émetteur devait attendre un accusé de réception après l'envoi de chaque paquet, le débit serait particulièrement lent. C'est pourquoi la plupart des protocoles orientés connexion fiables permettent l'envoi de plusieurs paquets avant qu'un accusé ACK ne soit effectivement reçu. L'émetteur utilise l'intervalle de temps qui s'écoule entre le moment où il envoie un paquet et celui où il traite l'accusé de réception pour transmettre d'autres données. Le nombre de paquets de données pouvant ainsi être transmis avant réception d'un accusé de réception est connu sous le nom de taille de fenêtre ou fenêtre.
TCP utilise des accusés de réception prévisionnels. Cela signifie que le numéro de l'accusé indique le paquet suivant attendu.
Le fenêtrage fait référence au fait que la taille de la fenêtre est négociée de manière dynamique pendant la session TCP. Il constitue un mécanisme de contrôle de flux. Après qu'une certaine quantité de données a été transmise, la machine source doit recevoir un accusé de l'hôte de destination. Ce dernier signale une taille de fenêtre à l'hôte source. Cette fenêtre indique le nombre de paquets que l'hôte de destination est prêt à recevoir, le premier d'entre eux étant l'accusé de réception.
Si la taille de fenêtre est de trois, l'hôte source peut envoyer trois octets à l'unité de destination avant d'attendre l'accusé de réception. Lorsque l'hôte de destination reçoit les trois octets, il envoie un accusé de réception à la source qui peut alors envoyer trois autres octets. Si l'unité de destination ne reçoit pas ces trois octets, parce que ses mémoires tampons sont saturées, elle n'envoie pas d'accusé de réception. L'hôte source sait alors qu'il doit retransmettre les octets à un débit de transmission inférieur.



Dans la figure , l'émetteur envoie trois paquets avant d'attendre l'accusé de réception. Si le récepteur ne peut en traiter que deux, la fenêtre abandonne le troisième paquet, indique que le paquet 3 sera le paquet suivant, puis spécifie une nouvelle fenêtre de deux. L'émetteur envoie les deux autres paquets, mais continue d'indiquer une taille de fenêtre de trois. Il attend donc toujours que le récepteur lui envoie un accusé de réception tous les trois paquets. Le récepteur répond en demandant le paquet cinq et indique de nouveau une taille de fenêtre de deux.

1.1.6 Accusé de réception

Une transmission fiable garantit qu'un flux de données envoyé depuis un ordinateur sera acheminé via une liaison de données vers un autre ordinateur, sans duplication ni perte des données. Un accusé de réception positif avec retransmission est une technique qui garantit cette fiabilité. Ce type d'accusé nécessite que le destinataire communique avec la source en lui envoyant un message pour accuser réception des données. L'émetteur conserve un enregistrement de chaque paquet de données, ou segment TCP, qu'il envoie, puis attend un accusé de réception. De plus, un décompte est entamé lorsque l'émetteur envoie un segment et ce dernier est retransmis si le délai arrive à expiration avant l'arrivée de l'accusé de réception.



La figure montre un émetteur transmettant les paquets 1, 2 et 3. Le destinataire accuse réception des paquets en demandant le paquet 4. À réception de l'accusé, l'émetteur envoie les paquets 4, 5 et 6. Si le paquet 5

n'arrive pas à destination, le récepteur demande sa retransmission. L'émetteur envoie alors le paquet 5, puis reçoit un accusé de réception lui demandant le paquet 7.

Séquence et accusé de réception TCP

Le protocole TCP assure le séquençage des segments grâce à des accusés de réception vers l'avant. Chaque segment est numéroté avant la transmission. Arrivés à destination, ces segments sont rassemblés en un message complet par le protocole TCP. Si un numéro de séquence est absent de la série, le segment correspondant est retransmis. Les segments qui ne font pas l'objet d'un accusé de réception dans un délai donné sont retransmis.

1.1.7 Protocole TCP (Transmission Control Protocol)

TCP est un protocole orienté connexion de la couche transport, qui assure une transmission fiable des données en full duplex. TCP fait partie de la pile de protocoles TCP/IP. Dans un environnement orienté connexion, une connexion est établie entre les deux extrémités avant que le transfert des informations ne commence. TCP découpe les messages en segments, les rassemble à l'arrivée et renvoie toute donnée non reçue. Il assure un circuit virtuel entre les applications utilisateur.

Les protocoles utilisant TCP sont les suivants:

- FTP
- HTTP
- SMTP
- Telnet

Structure de segment TCP

Bit 0		Bit 15 Bit 16	Bit 31
Port source (16)		Port de destination (16)	
Numéro de séquence (32)			
Numéro d'accusé de réception (32)			
Longueur d'en-tête (4)	Réservé (6)	Bits de Code (6)	Fenêtre (16)
Somme de contrôle (16)		Urgent (16)	
Options (0 ou 32 le cas échéant)			
Données (variable)			

Voici la description des champs contenus dans le segment TCP:

- **Port source:** numéro du port qui envoie les données.
- **Port de destination:** numéro du port qui reçoit les données.
- **Numéro de séquence:** numéro utilisé pour garantir une livraison des données dans l'ordre approprié.
- **Numéro d'accusé de réception:** octet TCP suivant attendu.
- **HLEN:** nombre de mots de 32 bits contenus dans l'en-tête.
- **Réservé:** champ réglé sur zéro.
- **Bits de code:** fonctions de contrôle, telles que l'ouverture et la fermeture d'une session.
- **Fenêtre:** nombre d'octets que l'émetteur acceptera.
- **Somme de contrôle:** somme de contrôle des champs de données et d'en-tête.
- **Pointeur d'urgence:** indique la fin des données urgentes.
- **Option:** une des options actuellement disponibles est la taille maximale d'un segment TCP (MSS – Maximum Segment Size).

Données: données de protocole de couche supérieure.

1.1.8 Protocole UDP (User Datagram Protocol)

C'est un protocole simple qui échange des datagrammes sans garantir leur bonne livraison. Il repose entièrement sur les protocoles de couche supérieure pour le contrôle des erreurs et la retransmission des données.

UDP n'utilise ni fenêtres ni accusés de réception. La fiabilité est assurée par les protocoles de la couche application. Le protocole UDP est conçu pour les applications qui ne doivent pas assembler de séquences de segments.

Les protocoles utilisant UDP sont les suivants:

- TFTP
- SNMP
- DHCP
- DNS

Structure de segment UDP

Bit 0	Bit 15 Bit 16	Bit 31
Port source (16)	Port de destination (16)	8 octets
Longueur (16)	Somme de contrôle (16)	
Données (le cas échéant)		

Voici la description des champs contenus dans le segment UDP:

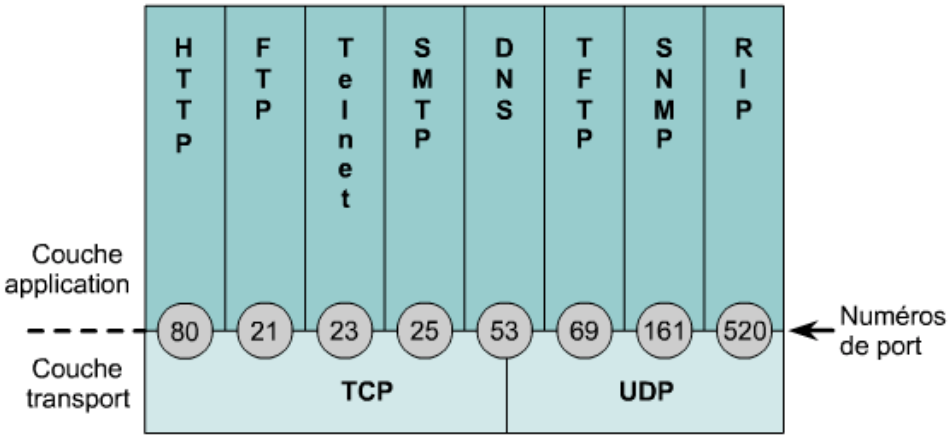
- **Port source:** numéro du port qui envoie les données.
- **Port de destination:** numéro du port qui reçoit les données.
- **Longueur:** nombre d'octets de l'en-tête et des données.
- **Somme de contrôle:** somme de contrôle des champs de données et d'en-tête.

Données: données de protocole de couche supérieure.

1.1.9 Numéros de port TCP et UDP

Les protocoles TCP et UDP utilisent des numéros de port pour transmettre les informations aux couches supérieures. Ces numéros servent à distinguer les différentes conversations qui circulent simultanément sur le réseau.

Numéros de port



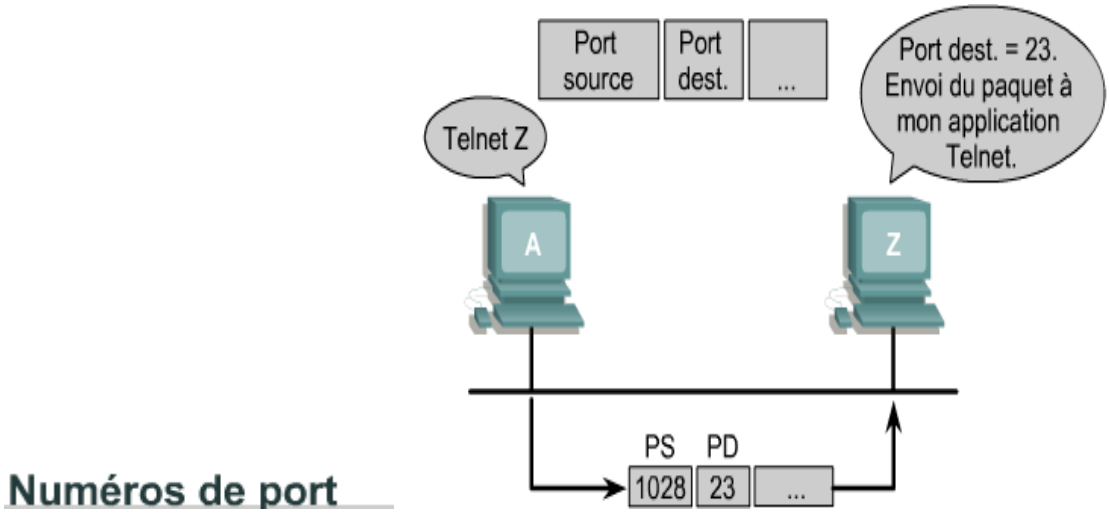
Les développeurs d'applications ont convenu d'utiliser les numéros de port reconnus émis par l'IANA (*Internet Assigned Numbers Authority*). Toute conversation destinée à l'application FTP fait appel aux numéros de port standard 20 et 21. Le port 20 est utilisé pour la partie données et le port 21 pour le contrôle. Les conversations qui n'impliquent pas d'application utilisant un numéro de port reconnu se voient attribuer des numéros de manière aléatoire sélectionnés dans une plage spécifique supérieure à 1023. Certains ports sont réservés aux protocoles TCP et UDP, bien que les applications ne soient pas forcément conçues pour les prendre en charge. Les plages attribuées aux numéros de port sont les suivantes:

- Les numéros inférieurs à 1024 sont considérés comme des numéros de port reconnus.
- Les numéros supérieurs à 1024 sont des numéros attribués de manière dynamique.
- Les numéros de port enregistrés sont destinés à des applications spécifiques d'un fournisseur. La plupart se situent au-delà de 1024.

Les systèmes d'extrémité utilisent les numéros de port pour sélectionner l'application appropriée. L'hôte source attribue dynamiquement les numéros de port source. Ils sont toujours supérieurs à 1023.

Numéros de port UDP et TCP réservés

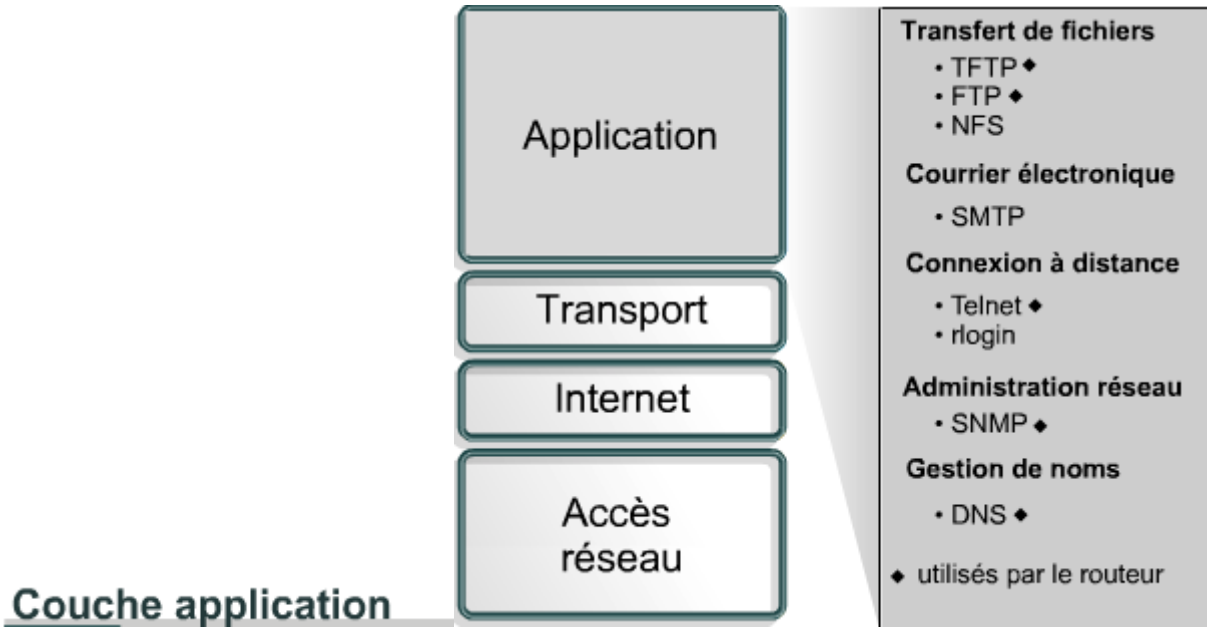
Decimal	Keyword	Description
0		Réservé
1-4		Non attribué
5	RJE	Protocole RJE (Soumission de travaux à distance)
7	ECHO	Écho
9	DISCARD	Élimination
11	USERS	Utilisateurs actifs
13	DAYTIME	Heure du jour
15	NETSTAT	Qui est actif ou NETSTAT
17	QUOTE	Citation du jour
19	CHARGEN	Générateur de caractères
20	FTP-DATA	Protocole FTP (données)
21	FTP	Protocole FTP
23	TELNET	Connexion en mode terminal
25	SMTP	Protocole SMTP (Simple Mail Transfer Protocol)
37	TIME	Heure du jour
39	RLP	Protocole RLP (Resource Location Protocol)
42	NAMESERVER	Serveur de noms d'hôte
43	NICNAME	Protocole Who Is
53	DOMAIN	Serveur de noms de domaine
67	BOOTPS	Serveur de protocole Bootstrap
68	BOOTPC	Client de protocole Bootstrap
69	TFTP	Protocole TFTP (Trivial File Transfer Protocol)
75		Tout service de sortie privé
77		Tout service RJE privé
79	FINGER	Finger
80	HTTP	Protocole HTTP (HyperText Transfer Protocol)
95	SUPDUP	Protocole SUPDUP
101	HOSTNAME	Serveur de noms d'hôte NIC
102	ISO-TSAP	ISO-TSAP
113	AUTH	Service d'authentification
117	UUCP-PATH	Service de chemin UUCP
123	NTP	Protocole NTP (Network Time Protocol)
137	NetBIOS	Service de noms
139	NetBIOS	Service de datagramme
143	IMAP	Protocole IMAP (Interim Mail Access Protocol)
150	NetBIOS	Service de session
156	SQL	Serveur SQL
161	SNMP	Protocole SNMP (Simple Network Management Protocol)
179	BGP	Protocole BGP (Border Gateway Protocol)
190	GACP	Protocole GACP (Gateway Access Control Protocol)
194	IRC	IRC (Internet Relay Chat)
197	DLS	Directory Location Service
224-241		Non attribué
242-255		Non attribué



1.2 La couche application

1.2.1 Introduction à la couche application du modèle TCP/IP

Les couches session, présentation et application du modèle OSI sont regroupées dans la couche application du modèle TCP/IP. Cela signifie que la représentation, le code et le contrôle du dialogue sont traités au niveau de la couche application TCP/IP. Cette structure permet de garantir un maximum de flexibilité dans la couche application du modèle TCP/IP pour les développeurs d'applications.



Les protocoles TCP/IP qui prennent en charge le transfert des fichiers, la messagerie et la connexion à distance sont probablement les protocoles que connaissent le mieux les utilisateurs d'Internet. Ils comprennent les applications suivantes:

- DNS
- FTP
- HTTP
- SMTP
- SNMP
- Telnet

1.2.2 DNS

Internet repose sur un système d'adressage hiérarchique qui permet un routage basé sur des classes d'adresses plutôt que sur des adresses individuelles. Le problème pour l'utilisateur est de faire correspondre l'adresse désirée avec le site Internet. Il est difficile de retenir l'adresse IP d'un site, car l'adresse numérique n'a aucun rapport apparent avec le contenu du site. Imaginez la difficulté que cela représenterait de mémoriser les adresses IP de dizaines, de centaines, voire de milliers de sites Web.

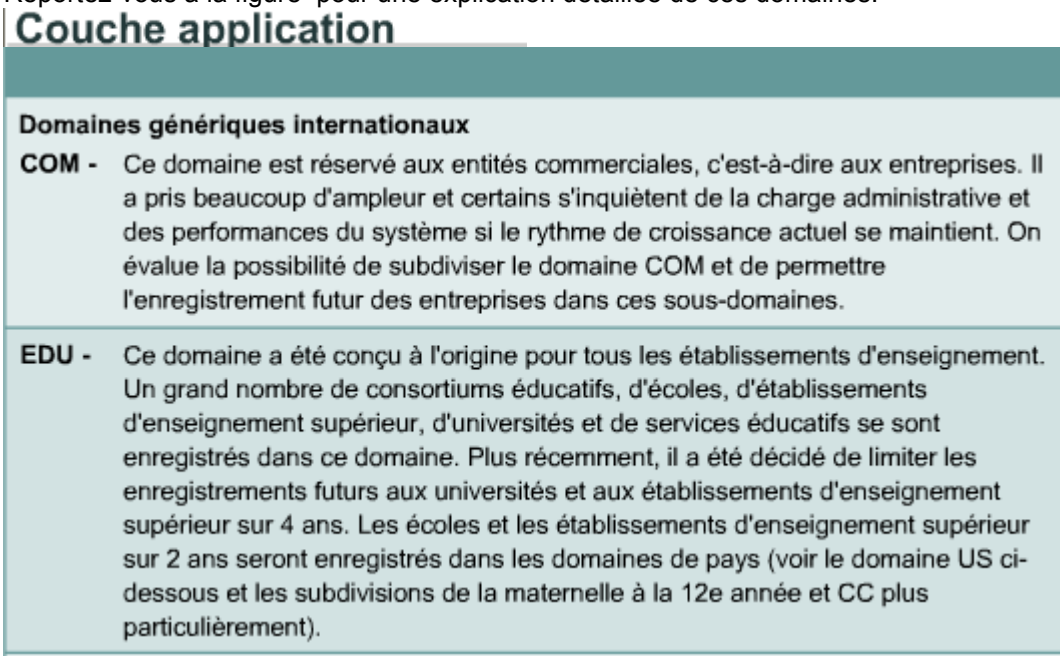
Afin de pouvoir créer un lien entre le contenu d'un site et son adresse, un système de noms de domaine a été établi. Le système de noms de domaine (DNS) est utilisé sur Internet pour convertir en adresses IP les noms de domaine et leurs nœuds de réseau annoncés publiquement. Un domaine est un groupe d'ordinateurs associés en fonction de leur proximité géographique ou du type d'informations qu'ils contiennent. Un nom de domaine est une chaîne de caractères, de nombres, ou les deux. Il s'agit généralement d'un nom ou d'une abréviation qui est associé à l'adresse numérique d'un site Internet. Il existe plus de 200 domaines de niveau supérieur sur Internet, notamment:

.ma– Maroc
.us – États-Unis
.fr – France

Il existe aussi des noms génériques, notamment:

.edu – sites éducatifs
.com – sites commerciaux
.gov – sites gouvernementaux
.org – sites d'organisations à but non lucratif
.net – service de réseau

Reportez-vous à la figure pour une explication détaillée de ces domaines.



Couche application

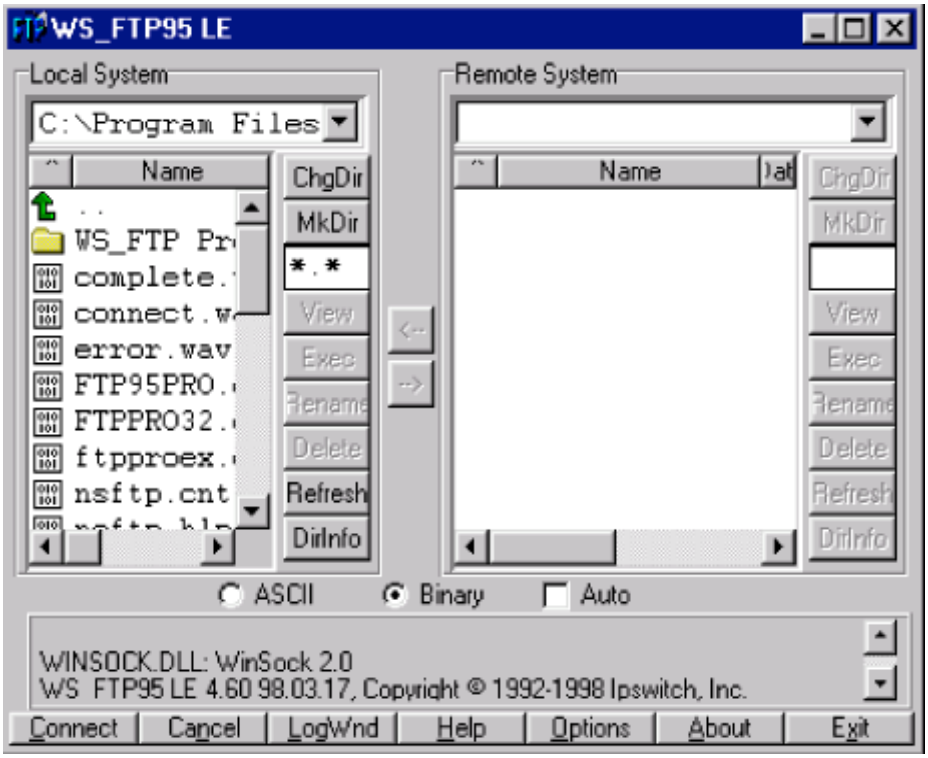
Domaines génériques internationaux
COM - Ce domaine est réservé aux entités commerciales, c'est-à-dire aux entreprises. Il a pris beaucoup d'ampleur et certains s'inquiètent de la charge administrative et des performances du système si le rythme de croissance actuel se maintient. On évalue la possibilité de subdiviser le domaine COM et de permettre l'enregistrement futur des entreprises dans ces sous-domaines.
EDU - Ce domaine a été conçu à l'origine pour tous les établissements d'enseignement. Un grand nombre de consortiums éducatifs, d'écoles, d'établissements d'enseignement supérieur, d'universités et de services éducatifs se sont enregistrés dans ce domaine. Plus récemment, il a été décidé de limiter les enregistrements futurs aux universités et aux établissements d'enseignement supérieur sur 4 ans. Les écoles et les établissements d'enseignement supérieur sur 2 ans seront enregistrés dans les domaines de pays (voir le domaine US ci-dessous et les subdivisions de la maternelle à la 12e année et CC plus particulièrement).

NET -	Ce domaine est réservé aux ordinateurs des fournisseurs de réseau : les ordinateurs du NIC (Network Information Center) et du centre d'exploitation du réseau NOC (Network Operation Center), les ordinateurs administratifs et les ordinateurs des nœuds réseau. Les clients du fournisseur de réseau ont leur propre nom de domaine (pas dans le domaine de niveau supérieur NET).
ORG -	Ce domaine de niveau supérieur est réservé aux organisations qui n'entrent dans aucune autre catégorie. Certaines organisations non gouvernementales peuvent être classées dans cette catégorie.
INT -	Ce domaine est destiné aux organismes établis par des traités internationaux ou aux bases de données internationales.
Domaines génériques spécifiques des États-Unis	
GOV -	Ce domaine était à l'origine destiné à tous les bureaux ou agences gouvernementaux. Plus récemment, il a été décidé de n'y enregistrer que les agences du gouvernement fédéral américain. Les agences locales et fédérales sont inscrites sous le domaine du pays.
MIL -	Ce domaine est utilisé par l'armée américaine.
Exemple de domaine de pays	
US -	En tant qu'exemple de domaine de pays, le domaine US permet l'enregistrement de toutes sortes d'entités aux États-Unis, en fonction de la géographie politique, c'est-à-dire selon une hiérarchie <nom-entité>.<localité>. <code état>. US. Par exemple, IBM.Armonk.NY.US. En outre, des branches du domaine US ont été prévues au sein de chaque État pour les écoles maternelles, primaires et secondaires, les collèges publics (CC), les écoles techniques (TEC), les agences d'état (STATE), les conseils de gouvernement (COG), les bibliothèques (LIB), les musées (MUS) et plusieurs autres types génériques

1.2.3 FTP and TFTP

FTP est un service orienté connexion fiable qui utilise le protocole TCP pour transférer des fichiers entre des systèmes qui le prennent en charge. L'objectif principal du protocole FTP est d'échanger des fichiers dans les deux sens (importation et exportation) entre un ordinateur serveur et des ordinateurs clients. Lorsque vous importez des fichiers à partir d'un serveur, FTP établit d'abord une connexion de contrôle entre le client et le serveur. Puis une seconde connexion permet de transférer les données d'un ordinateur à l'autre. Le transfert des données peut se faire en mode ASCII ou binaire. Ces modes déterminent le codage des fichiers de données qui, dans le modèle OSI, constitue une tâche de la couche présentation. Une fois le fichier transféré, la connexion de données est automatiquement interrompue. La commande de liaison est fermée dès que l'utilisateur met fin à la session en se déconnectant, après avoir terminé de copier et de transférer ses fichiers.

Application FTP



TFTP est un service non orienté connexion qui se sert du protocole UDP (*User Datagram Protocol*). Il est utilisé sur le routeur pour transférer des fichiers de configuration et des images de la plate-forme logicielle IOS Cisco, ainsi que pour transférer des fichiers entre des systèmes qui le prennent en charge. Ce protocole, conçu pour être léger et facile à mettre en œuvre, est dépourvu de la plupart des fonctionnalités de FTP. Il peut lire ou écrire des fichiers vers ou depuis un serveur distant, mais il ne permet pas d'afficher le contenu des répertoires ni d'assurer l'authentification des utilisateurs. Il est utile dans certains LAN, car il s'exécute plus rapidement que le protocole FTP. Son fonctionnement est par ailleurs fiable dans un environnement stable.

1.2.4 http

Le protocole HTTP (*Hypertext Transfer Protocol*) est le support du Web, la partie la plus utilisée d'Internet et celle qui connaît la plus forte croissance. L'expansion phénoménale du Web s'explique principalement par la facilité avec laquelle il permet d'accéder aux informations. Un navigateur Web est une application de type client-serveur, c'est-à-dire qu'il requiert un composant client et un composant serveur pour pouvoir fonctionner. Il présente des pages Web contenant des données multimédia : texte, graphique, son et vidéo. Les pages Web sont créées avec un langage de formatage appelé HTML (*HyperText Markup Language*). Le code HTML indique au navigateur comment présenter une page Web pour obtenir un aspect particulier. Outre le contenu, le langage HTML spécifie la disposition du texte, des fichiers et des objets qui sont transférés depuis le serveur Web jusqu'au navigateur Web.

Les liens hypertexte (ou hyperliens) facilitent la navigation sur le Web. Il peut s'agir d'un objet, d'un mot, d'une phrase ou d'une image sur une page Web. Lorsque vous cliquez sur ce lien, une nouvelle page Web est affichée dans le navigateur. La page Web contient une adresse URL (*Uniform Resource Locator*) qui est souvent cachée dans sa description HTML.

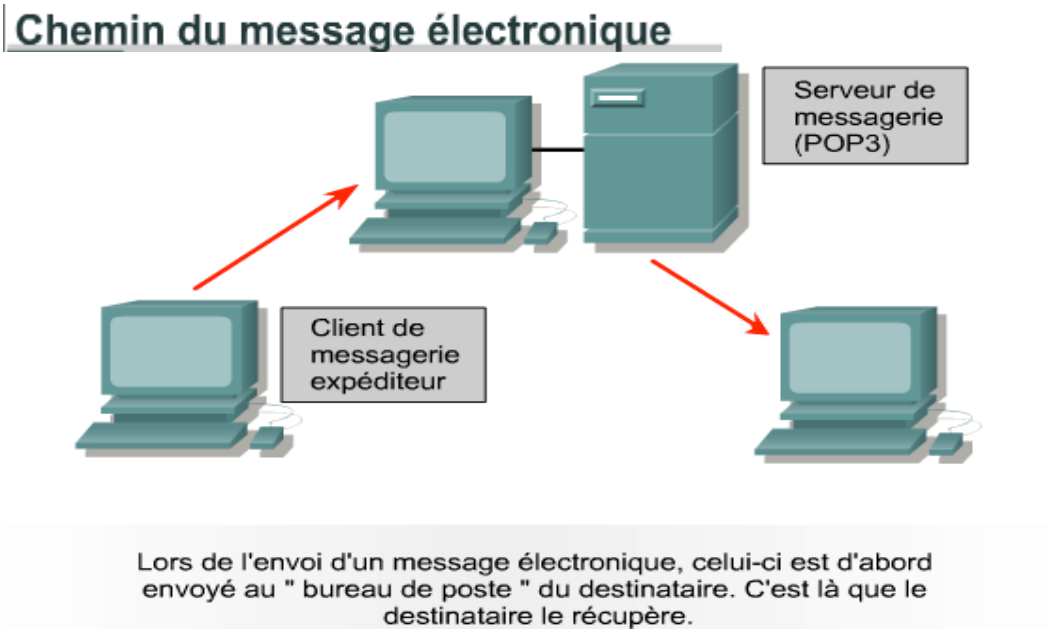
Dans l'URL http://www.fsk-uit.ma/Master/, la partie «http://» indique au navigateur le protocole à utiliser. La seconde partie, «www», indique le nom de l'hôte ou le nom d'un ordinateur précis doté d'une adresse IP spécifique. Enfin, le suffixe « /Master/ » précise l'emplacement exact du dossier sur le serveur qui contient la page Web.

Un navigateur Web s'ouvre généralement sur une page de démarrage ou page d'accueil. L'adresse URL a été enregistrée dans les données de configuration du navigateur et peut être modifiée quand bon vous semble. Dans cette page d'accueil, vous pouvez soit cliquer sur un hyperlien, soit taper une adresse URL dans la barre d'adresse du navigateur. Le navigateur Web examine alors le protocole pour savoir s'il a besoin d'ouvrir un autre programme, puis détermine l'adresse IP du serveur Web à l'aide du système DNS. Ensuite, les couches transport, réseau, liaison de données et physique établissent une session avec le serveur Web. Les données transférées vers le serveur HTTP contiennent le nom du dossier où est stockée la page Web. Les données peuvent également contenir le nom de fichier d'une page HTML. En l'absence de nom, le nom par défaut indiqué dans la configuration du serveur est utilisé.

Le serveur répond à la demande en transmettant au client Web tous les fichiers texte, audio, vidéo et graphique indiqués dans la page HTML. Le navigateur client rassemble tous ces fichiers pour créer une image de la page Web et met fin à la session. Si vous cliquez sur une autre page située sur le même serveur, ou sur un serveur différent, la procédure reprend depuis le début.

1.2.5 SMTP

Les serveurs de messagerie communiquent entre eux à l'aide du protocole SMTP (*Simple Mail Transfer Protocol*) pour envoyer et recevoir des messages électroniques. Ce protocole transporte les messages au format ASCII à l'aide de TCP.



Lors de l'envoi d'un message électronique, celui-ci est d'abord envoyé au " bureau de poste " du destinataire. C'est là que le destinataire le récupère.

Lorsqu'un serveur de messagerie reçoit un message destiné à un client local, il le stocke jusqu'à ce que le client le récupère. Les clients de messagerie peuvent récupérer leur courrier de plusieurs manières : soit ils se servent de programmes qui accèdent directement aux fichiers du serveur de messagerie, soit ils font appel à l'un des nombreux protocoles réseau. Les protocoles de client de messagerie les plus répandus sont POP3 et IMAP4, qui utilisent tous deux TCP pour transporter les données. Bien que les clients de messagerie récupèrent le courrier via ces protocoles, ils utilisent pratiquement toujours le protocole SMTP pour l'envoi des messages. L'envoi et la réception de courrier faisant appel à deux protocoles différents, voire deux serveurs différents, les clients de messagerie peuvent très bien effectuer une tâche, mais pas l'autre. Il est par conséquent préférable de résoudre les problèmes d'envoi de courrier indépendamment des problèmes de réception.

Lorsque vous vérifiez la configuration d'un client de messagerie, assurez-vous que les paramètres SMTP et POP, ou IMAP, sont correctement configurés. Pour tester l'accès à un serveur de messagerie, établissez une connexion Telnet au port SMTP (25) ou au port POP3 (110). Le format de commande suivant est utilisé sur la ligne de commande Windows pour tester l'accès au service SMTP du serveur de messagerie à l'adresse IP 192.168.10.5:

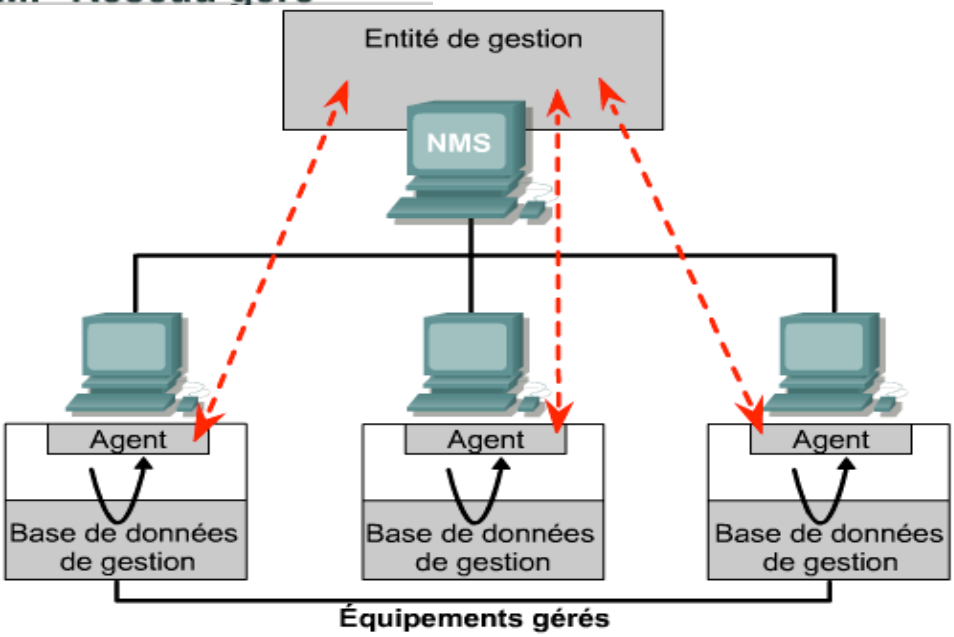
```
C:\>telnet 192.168.10.5 25
```

Le protocole SMTP ne propose guère d'options de sécurité et ne nécessite aucune authentification. Généralement, les administrateurs n'autorisent que les hôtes appartenant à leur réseau à utiliser leur serveur SMTP pour l'envoi ou le transit de courrier. Cela dans le but d'éviter que des utilisateurs non autorisés n'utilisent leurs serveurs comme relais de messagerie.

1.2.6 SNMP

Le protocole SNMP (*Simple Network Management Protocol*) est un protocole de la couche application qui facilite l'échange d'information de gestion entre les équipements du réseau. Il permet aux administrateurs réseau de gérer les performances du réseau, de diagnostiquer et de résoudre les problèmes, ainsi que d'anticiper la croissance du réseau. SNMP se sert du protocole UDP de la couche transport.

SNMP-Réseau géré



Un réseau géré à l'aide de SNMP comprend les trois principaux composants suivants:

- **Le système d'administration de réseaux *(NMS, Network Management System)*:** le composant NMS exécute les applications qui contrôlent et surveillent les unités gérées. Il fournit la quantité de ressources mémoire et de traitement requises pour la gestion du réseau. Tout réseau géré doit comprendre au moins un composant NMS.
- **Les unités gérées:** ces unités sont des nœuds du réseau contenant un agent SNMP et résidant sur un réseau géré. Elles collectent et stockent des informations de gestion qu'elles mettent à la disposition des composants NMS via SNMP. Ces unités gérées, parfois appelées éléments du réseau, peuvent être des routeurs, des serveurs d'accès, des commutateurs, des ponts, des concentrateurs, des ordinateurs hôtes ou des imprimantes.

Les agents: les agents sont des modules logiciels de gestion du réseau résidant sur les unités gérées. Ils contiennent les données locales des informations de gestion et les convertissent en un format compatible avec SNMP.

1.2.7 Service Telnet

Le logiciel client Telnet permet de se connecter à un hôte Internet distant sur lequel est exécutée une application serveur Telnet, puis d'exécuter des commandes à partir de la ligne de commande. Un client Telnet est qualifié d'hôte local. Le serveur Telnet, qui utilise un logiciel spécial appelé «démon», est considéré comme l'hôte distant.

Pour établir une connexion à partir d'un client Telnet, il convient de sélectionner une option de connexion. Une boîte de dialogue vous invite généralement à entrer un nom d'hôte et un type de terminal. Le nom d'hôte est l'adresse IP ou le nom DNS de l'ordinateur distant. Le type de terminal décrit le mode d'émulation de terminal qui doit être utilisé par le client Telnet. La connexion Telnet n'exige aucun traitement de la part de l'ordinateur émetteur qui se contente de transmettre à l'ordinateur distant les caractères tapés au clavier et d'afficher l'écran résultant sur le moniteur local. Les opérations de traitement et de stockage sont entièrement exécutées par l'ordinateur distant.

Telnet fonctionne au niveau de la couche application du modèle TCP/IP. Il opère donc au niveau des trois couches supérieures du modèle OSI. La couche application traite les commandes. La couche présentation gère le formatage, généralement ASCII. La couche session effectue la transmission. Dans le modèle TCP/IP, toutes ces fonctions sont regroupées dans la couche application

Résumé :

Le rôle principal de la couche transport (couche 4 du modèle OSI) est de transporter et de contrôler le flux d'informations de la source à la destination, et ce de manière fiable et précise.

La couche transport multiplexe les données des applications de couche supérieure en un flux de paquets de données. Elle se sert de numéros de port (socket) pour identifier les différentes conversations et livrer les données aux applications appropriées.
Le protocole TCP (*Transmission Control Protocol*) est un protocole orienté connexion qui assure le contrôle du flux ainsi que la fiabilité. Il fait appel à un échange en trois étapes pour établir un circuit synchronisé entre les applications utilisateur. Chaque datagramme est numéroté avant la transmission. Au niveau de la station de réception, le protocole TCP assemble le segment en un message complet. Si un numéro de séquence est absent de la série, le segment correspondant est retransmis.
Le contrôle de flux garantit qu'un nœud transmetteur ne pourra pas saturer le nœud récepteur. La méthode la plus simple employée par TCP est l'utilisation d'un signal « non prêt » pour avertir l'unité émettrice de la saturation des tampons mémoires de l'unité réceptrice. Lorsque le récepteur peut accepter de nouvelles données, il envoie l'indicateur de transport «prêt».
Un accusé de réception positif avec retransmission est une autre technique employée par le protocole TCP pour garantir une transmission fiable des données. Si l'émetteur devait attendre un accusé de réception après l'envoi de chacun des paquets, le débit des données serait considérablement ralenti. Le fenêtrage est donc utilisé pour permettre la transmission de plusieurs paquets avant qu'un accusé de réception ne soit nécessaire. Les tailles de fenêtre TCP varient au cours de la durée de vie d'une connexion.
Un accusé de réception positif avec retransmission est une autre technique employée par le protocole TCP pour garantir une transmission fiable des données. Si l'émetteur devait attendre un accusé de réception après l'envoi de chacun des paquets, le débit des données serait considérablement ralenti. Le fenêtrage est donc utilisé pour permettre la transmission de plusieurs paquets avant qu'un accusé de réception ne soit nécessaire. Les tailles de fenêtre TCP varient au cours de la durée de vie d'une connexion.
Si aucun contrôle de flux et aucun accusé de réception ne sont requis pour une application, comme dans le cas d'une transmission de broadcast, le protocole UDP (*User Datagram Protocol*) peut remplacer le protocole TCP. UDP est un protocole de transport non orienté connexion de la pile de protocoles TCP/IP qui permet la simultanéité de plusieurs conversations, sans toutefois fournir d'accusés de réception ou de garantie de livraison. Un en-tête UDP est donc plus petit qu'un en-tête TCP du fait de l'absence des informations de contrôle.
Certains des protocoles et des applications opérant au niveau de la couche application sont bien connus des utilisateurs d'Internet:

- **Système DNS *(Domain Name System)*:** système utilisé dans les réseaux IP pour traduire le nom des nœuds du réseau en adresses IP.
- **Protocole FTP *(File Transfer Protocol)*:** protocole utilisé pour le transfert des fichiers entre les réseaux.
- **Protocole HTTP *(Hypertext Transfer Protocol)*:** protocole utilisé pour fournir des documents en langage HTML (*HyperText Markup Language*) à une application cliente, telle qu'un navigateur Web.
- **Protocole SMTP *(Simple Mail Transfer Protocol)*:** protocole permettant l'utilisation de services de messagerie électronique.
- **Protocole SNMP *(Simple Network Management Protocol)*:** protocole utilisé pour surveiller et contrôler les équipements du réseau, ainsi que pour gérer les configurations, la collecte de statistiques, les performances et la sécurité.

Telnet: utilisé pour se connecter à un hôte distant sur lequel est exécutée une application serveur Telnet, puis pour exécuter des commandes depuis la ligne de commande.