

# Chapitre : Services réseaux

**Définition :** Les services du réseau informatique se sont des informations généralement de type client-serveur. Ces services se basent sur la notion de port pour la différenciation entre eux que soit au niveau du client soit au niveau du serveur. Ils peuvent être communiqués à travers de l'un des protocoles réseaux (UDP ou TCP) en fonction du type d'information.

**Le protocole TCP (Transmission Control Protocol) :** est un protocole de la couche transport du modèle OSI caractérisé fiable et adapté aux services qui ont la contrainte du temps réel. Il permet d'organiser les données reçues de la couche application (appelés Data) sous forme d'un nouveau PDU (unité de données du protocole) nommé Segment. En particulier, la couche transport offre une nouvelle adresse du service sur un équipement appelée numéro de port pour différencier un flux de données entre une requête et une réponse.

## 1. Format d'un segment TCP :

### Structure de segment TCP

Nbre bits	16	16	32	32	4	6	6
	Port source	Dest. Port	Numéro de séquence	Numéro d'accusé de réception	HLEN	Réservé	Bits code

16	16	16	0 ou 32	
Fenêtre	Total de contr.	Pointeur d'urgence	Option	Données...

© Cisco Systems, Inc. 1999

- port source - numéro du port demandeur
- port de destination - numéro du port demandé
- numéro de séquence - numéro utilisé pour assurer la bonne séquence des données entrantes.
- numéro d'accusé de réception - prochain octet TCP attendu
- HLEN - nombre de mots de 32 bits contenus dans l'en-tête
- réservé - réglé à zéro (champ inutilisé actuellement mais prévu pour l'avenir)
- bits de code – qui détermine la nature du segment (URG=1 si le champ « pointeur urgent est positionné », ACK=1 si le champ « n° d'acquittement est significatif », EOM=1 indique la fin du message, RST = 1 sert à réinitialiser la connexion, SYN=1 sert à établir la connexion (demande), FIN =1 indique que l'émetteur n'a plus de données (fermeture))
- fenêtre - nombre d'octets que l'émetteur est prêt à accepter
- total de contrôle – erreur calculée sur l'en-tête et les données
- pointeur d'urgence - indique la fin des données urgentes

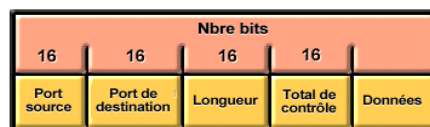
- option un - taille maximale d'un segment TCP
- données - données du protocole de couche supérieure

Le protocole TCP offre la numérotation des segments, l'accusé de réception ; il y a retransmission des segments en cas perte.

**Le protocole UDP (User Datagram Protocol)** : est un protocole de la couche transport caractérisé non fiable (pas de contrôle des pertes des données) par rapport au service. Il est adapté aux services non temps réel (échange des données même hors connexion en même temps entre les deux correspondants).

## 2. Format du segment :

### La structure du segment UDP



● Pas de champs de séquence ou d'accusé de réception

© Cisco Systems, Inc. 1999

Le protocole UDP n'offre pas de numérotation des segments, ni d'accusés de réception ; il n'y a pas non plus de retransmission. C'est la couche application qui doit assurer la fiabilité au besoin.

## 3. Identification d'un flux sur un équipement (adressage au niveau transport) :

L'identification des services est réalisée par les protocoles TCP et UDP par des numéros de port pour transmettre de l'information aux couches supérieures. Les numéros de port servent à distinguer les différentes conversations/flux qui circulent simultanément sur le réseau. Le numéro de port est un champ (source/destination) dans l'entête du segment TCP et UDP. Il est codé sur 16 bits en binaire ce qui donne la plage en décimal des 0 à  $2^{16}$  ports possibles. Les numéros inférieurs à 255 sont réservés aux applications publiques. Les numéros de 255 à 1023 sont attribués aux entreprises pour les applications à commercialiser. 1024 à 49151 sont des numéros de ports inscrits et 49152 à 65535 sont des ports dynamiques ou privés.

Chaque protocole utilise des numéros différents. Par exemple, pour TCP on trouve la valeur 21 pour le service de transfert de fichier FTP, la valeur 23 pour identifier le service d'accès à distance Telnet. Pour l'UDP, on trouve la valeur 69 pour identifier le service non temps réel TFTP.

**Client - serveur :**

Les services/informations qui circulent sur le réseau sont généralement de type client-serveur. Le périphérique demandant les informations est nommé client et celui répondant à la demande est nommé serveur. Les processus client et serveur sont considérés comme faisant partie de la couche application du modèle OSI. Le client commence l'échange en demandant des données au serveur, qui répond en envoyant un ou plusieurs flux de données au client. Les protocoles TCP/UDP de couche application décrivent le format des requêtes et des réponses entre clients et serveurs.

Exemple de réseau client/serveur, citons un environnement d'entreprise dans lequel les employés utilisent un serveur de messagerie d'entreprise pour envoyer, recevoir et stocker leur courriel. Le client de messagerie situé sur l'ordinateur d'un employé envoie une demande au serveur de messagerie pour tout courriel non lu. Le serveur répond en envoyant le courriel requis au client.

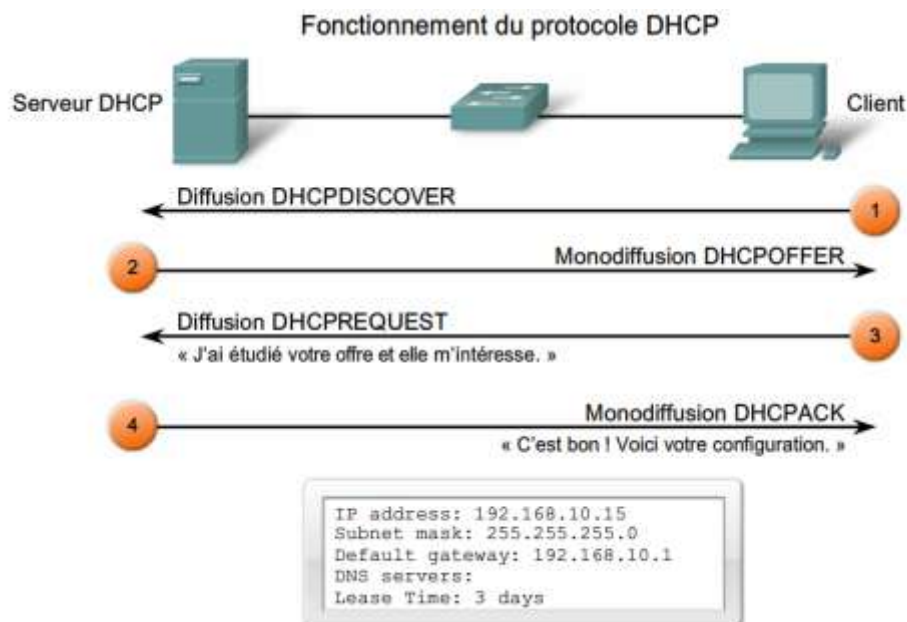
- a. Service d'affectation dynamique d'adresses IP (DHCP : Dynamic Host Configuration Protocol) : Tous les périphériques qui se connectent à un réseau informatique ont besoin d'une adresse IP valide. Les administrateurs réseau attribuent des adresses IP statiques aux routeurs, serveurs et aux autres périphériques réseau dont les emplacements (physique et logique) ne changeront sans doute pas. Les administrateurs entrent manuellement les adresses IP statiques lorsqu'ils configurent l'accès des périphériques au réseau. Les adresses statiques permettent également aux administrateurs de gérer ces périphériques à distance.

Cependant, dans une entreprise, les ordinateurs changent souvent d'emplacement, physiquement et logiquement. Il est impossible pour les administrateurs d'attribuer de nouvelles adresses IP chaque fois qu'un employé change de bureau ou de place. Les ordinateurs de bureau clients n'ont pas besoin d'une adresse statique ; une station de travail peut utiliser n'importe quelle adresse au sein d'une plage d'adresses connue. Cette plage appartient généralement à un sous-réseau ou à un réseau informatique. Une station de travail appartenant à un sous-réseau spécifique peut se voir attribuer n'importe quelle adresse d'une plage spécifiée.

- D'autres éléments tels que le masque de sous-réseau, la passerelle par défaut et le serveur de noms de domaine (DNS) se voient attribuer une valeur qui est commune à ce sous-réseau ou à l'ensemble du réseau administré. Par exemple, tous les hôtes d'un même sous-réseau reçoivent différentes adresses IP hôte, mais reçoivent le même masque de sous-réseau, la même adresse IP de passerelle par défaut et la même adresse d'un serveur DNS.
- En règle générale, les administrateurs préfèrent qu'un serveur réseau fournisse les services DHCP car ces solutions sont évolutives et relativement faciles à gérer. Cependant, dans le cas d'une petite filiale, d'un petit bureau ou d'un bureau à domicile, un routeur Cisco peut être configuré pour fournir les services DHCP, évitant ainsi l'achat d'un serveur dédié qui est recommandé à des entreprises de grande taille.
- Fonctionnement du service DHCP :

1. Le client (port DHCP 68) envoie en broadcast sur le réseau une requête DHCP DISCOVER pour trouver les serveurs DHCP disponibles (diffusion via l'adresse MAC de destination FF:FF:FF:FF:FF:FF).
2. Le serveur DHCP (port DHCP 67) ayant répondu en premier renvoie une requête DHCP OFFER pour fournir les informations au client.
3. Le client renvoie une requête DHCP REQUEST pour signaler aux autres serveurs DHCP qu'il a déjà choisi un serveur.
4. Le serveur DHCP choisi confirme au client avec un DHCP ACK.

Exemple :

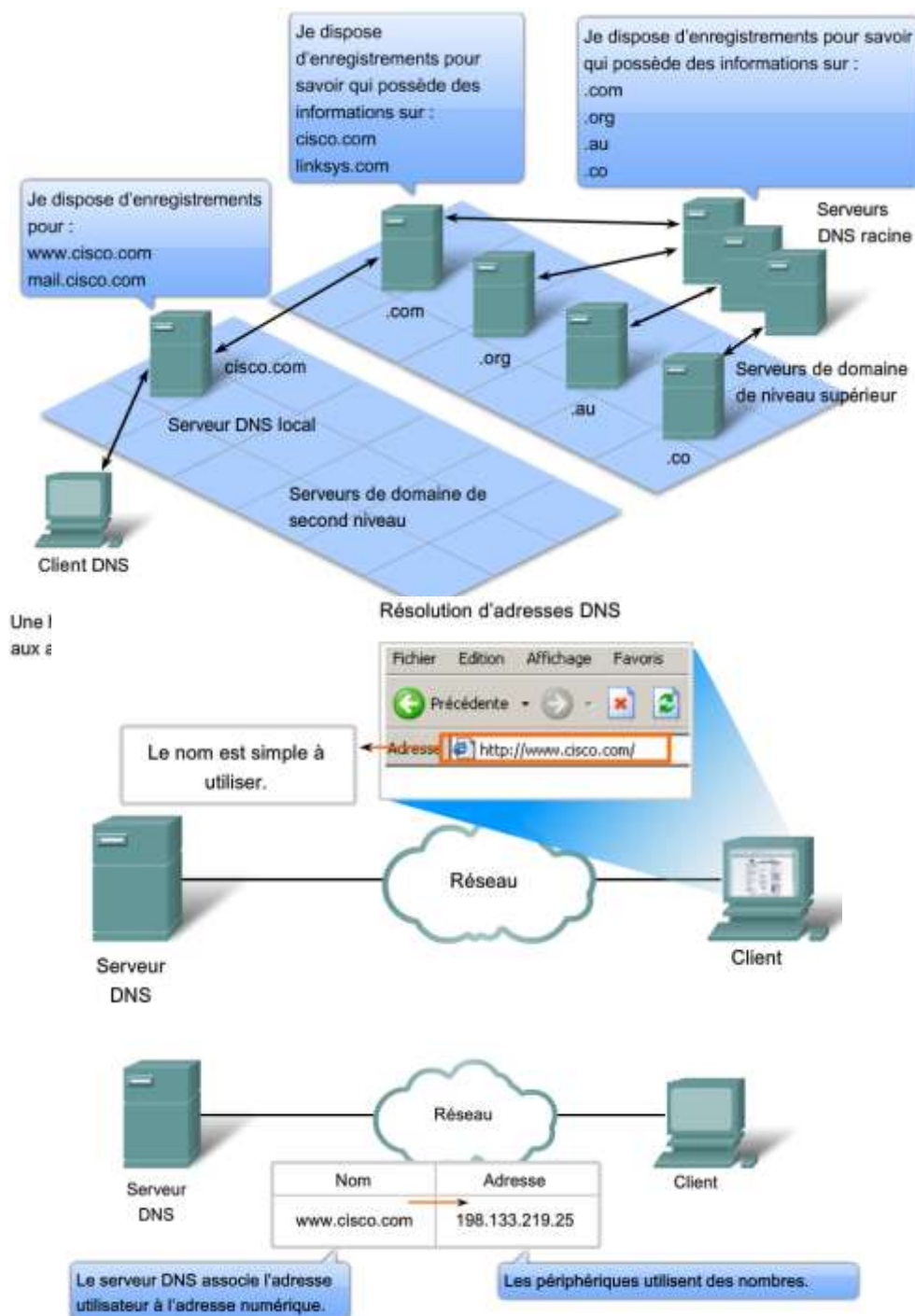


- b. Service de résolution de noms de domaine (DNS : Domain Name System)
- Est un ensemble de caractères masquant une adresse **IP** sur le réseau. Sur un réseau informatique il existe un serveur local de gestion de noms de domaines. Chaque client

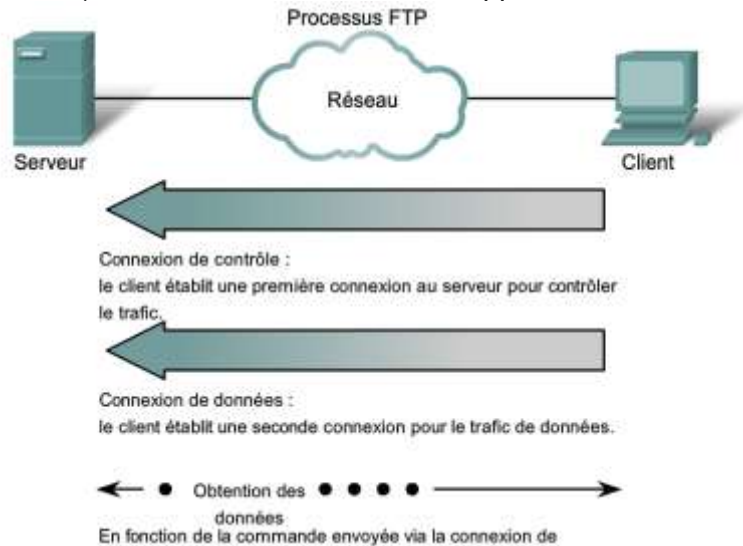
(machine/station) quand contacte le serveur (port UDP DNS 53) pour la résolution d'un nom d'une machine.

Exemple :

- 1- PC>ping [www.uit.ac.ma](http://www.uit.ac.ma), la requête est envoyée au serveur DNS local, si le nom existe le serveur DNS répond en fournissant @IP associée au nom [www.uit.ac.ma](http://www.uit.ac.ma).
- 2- PC>ping [www.google.com](http://www.google.com), DNS local contact le DNS racine ./, puis la racine redirige la requête vers le [domaine.com](http://domaine.com). Ensuite, cette adresse sera stockée dans le cache DNS du PC et du serveur DNS local pour le futur contact de toutes les machines du LAN.



- c. Service de transfert de fichier FTP (File Transfer Protocol) : est un protocole de communication destiné au partage de fichiers sur un réseau informatique. Il permet, depuis un ordinateur (client), de copier des fichiers vers un autre ordinateur (serveur) du réseau, ou encore de supprimer ou de modifier des fichiers sur

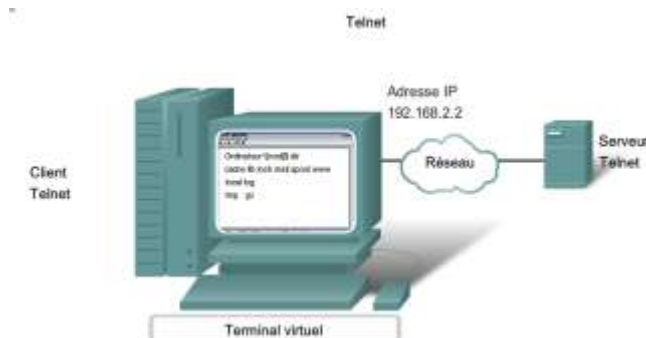


- d. Service d'accès à distance Telnet (23) : Telnet (terminal network ou telecommunication network) avec port 23. Une connexion TELNET s'appuie sur une connexion TCP pour transmettre des données dans lesquelles s'intercalent des séquences de contrôle TELNET. Le protocole TELNET est bâti selon trois principes essentiels :

- le concept de terminal réseau virtuel (Network Virtual Terminal) ;
- le principe d'options négociées ;
- une "vue" symétrique de chaque entité d'extrémité (processus ou terminal).

Par défaut le service Telnet utilise les sessions virtuelles.

Exemple :

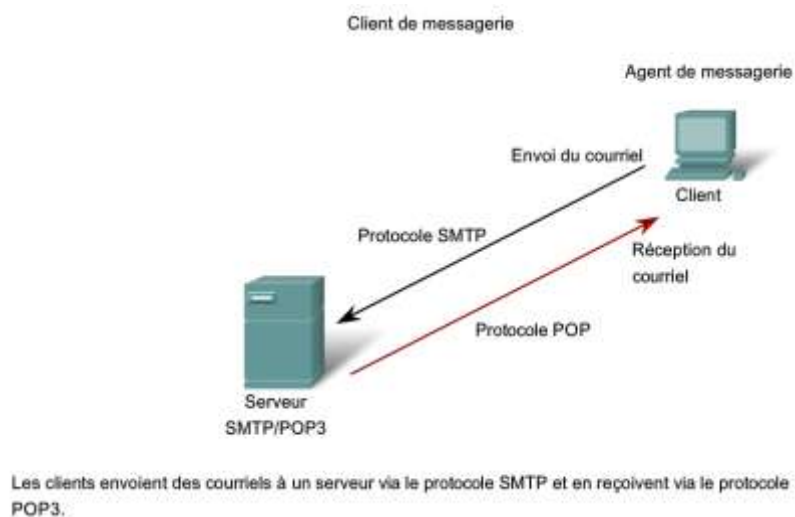


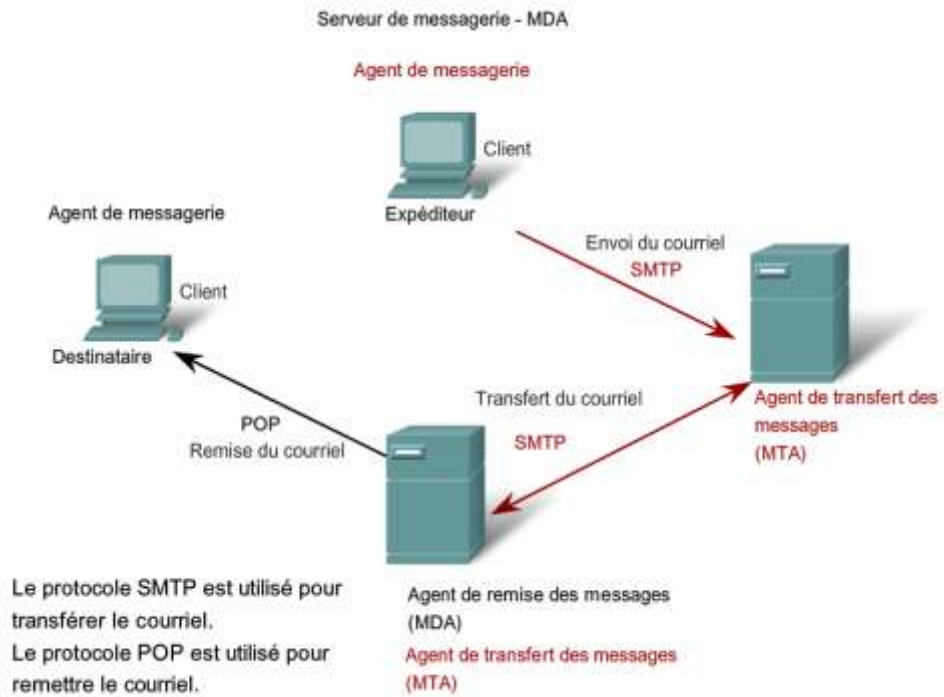
- e. Service d'accès à distance sécurisé SSH (22) : SSH est le protocole le plus sécurisé pour établir une communication avec un équipement distant routeur/switch. Les communications sont chiffrées sur le port 22.
- f. Service d'envoi/réception d'email : POP (110), SMTP (25), IMAP (143)

Chaque entreprise a un serveur de gestion des courriers électroniques pour ses clients. On distingue deux types de services : service d'envoi et de réception d'un courrier électronique. Le service d'envoi est géré par le protocole SMTP (Simple Mail Transfer Protocol) sur le port 143. Le service de réception d'un courrier électronique est assuré par l'un des protocoles : POP, POP3 ou IMAP.

POP (Post Office Protocol) : permet la lecture et le téléchargement des courriers sur la machine cliente. POP3 permet la lecture et/ou le téléchargement des courriers sur la machine cliente.

IMAP (Internet Message Access Protocol) est permet la lecture sans téléchargement de courriers.





**Remarque :** des exercices pratiques et théoriques seront abordés durant les séances des travaux pratiques et dirigés.