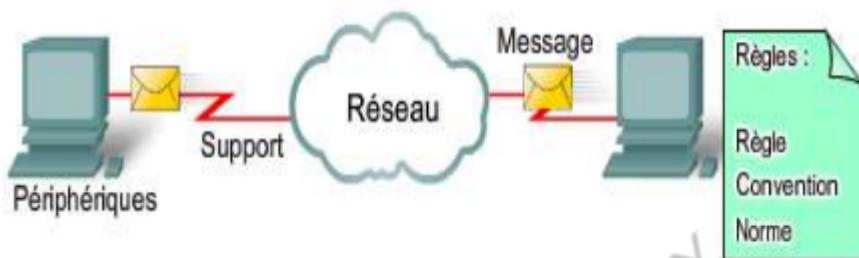


## Rappels sur les réseaux TCP/IP

### 1. Les éléments d'un réseau

Un réseau informatique est constitué de **quatre éléments fondamentaux** :

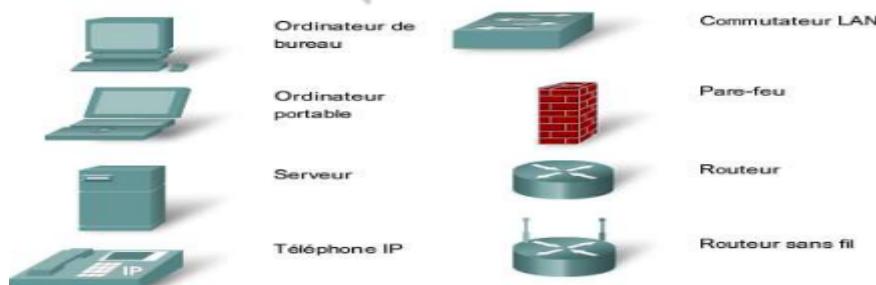
- **Les périphériques** : ordinateurs, routeurs, commutateurs, serveurs, etc.
- **Les messages** : informations échangées (pages web, courriels, appels...).
- **Les protocoles** : règles qui régissent la communication entre les périphériques.
- **Les supports** : fils de cuivre, fibres optiques, ondes radio (Wi-Fi), etc.



### 2. Les périphériques

Ce sont tous les équipements connectés au réseau, comme :

- **Les ordinateurs, smartphones et tablettes** : qui utilisent le réseau pour naviguer, envoyer des courriels, etc.
- **Les routeurs et commutateurs** : qui gèrent et dirigent le trafic réseau.
- **Les serveurs** : qui fournissent des services (web, mail, fichiers, etc.).



### 3. Les messages

Les données échangées dans un réseau peuvent être :

- Des pages web (HTTP/HTTPS)
- Des courriels (SMTP, IMAP, POP3)
- Des messages instantanés (WhatsApp, Messenger, etc.)
- Des appels VoIP (Skype, Zoom, etc.)
- D'autres formes de communication

## 4. Les supports de transmission

Les données peuvent circuler via différents supports :

- **Câbles en cuivre** (Ethernet, ADSL)
- **Fibres optiques** (Internet haut débit)
- **Ondes radio** (Wi-Fi, Bluetooth, 4G, 5G)

## 5. Les protocoles

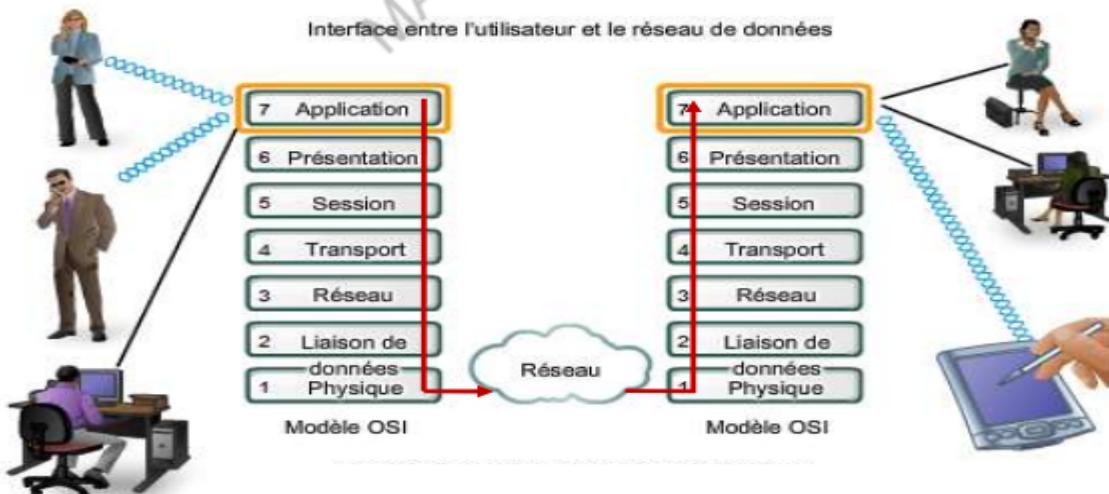
Les **protocoles** sont les règles qui définissent comment les messages sont envoyés et reçus. Par exemple :

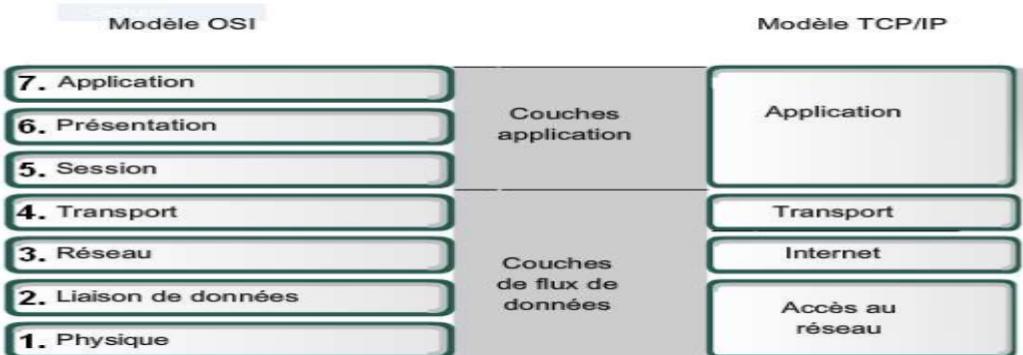
- **TCP/IP** : le protocole de base d'Internet.
- **HTTP/HTTPS** : utilisé pour les pages web.
- **SMTP/POP3/IMAP** : utilisés pour les courriels.
- **DNS** : traduit les noms de domaine en adresses IP.
- **FTP** : permet le transfert de fichiers.

## 6. Modèles de communication

Deux modèles principaux sont utilisés pour structurer les réseaux :

1. **Modèle OSI** (Open Systems Interconnection) :
  - Divisé en 7 couches (Application, Présentation, Session, Transport, Réseau, Liaison, Physique).
2. **Modèle TCP/IP** :
  - Plus simple, basé sur 4 couches : Application, Transport, Réseau, Liaison.

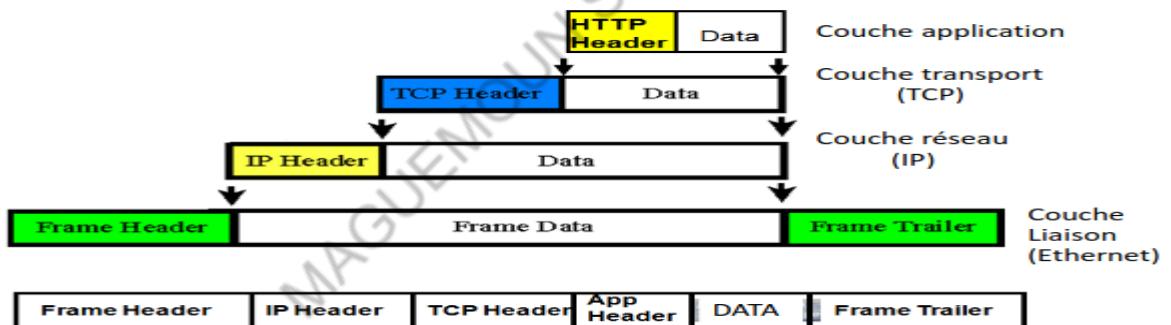




## 7. Encapsulation des protocoles

Chaque couche du modèle TCP/IP ajoute ses propres informations aux messages envoyés.

- **Couche Application** : définit la communication entre les logiciels (ex. : HTTP, FTP, DNS).
- **Couche Transport (TCP)** : gère la transmission fiable des données.
- **Couche Réseau (IP)** : s'occupe du routage des paquets.
- **Couche Liaison (Ethernet, Wi-Fi)** : gère la transmission des bits sur le support physique.



## 8. Protocoles de la couche Application TCP/IP

Ces protocoles permettent aux applications d'échanger des données :

- **DNS (Domain Name System)** : convertit les noms de domaine en adresses IP.
- **HTTP (Hypertext Transfer Protocol)** : transfert des pages web.
- **SMTP (Simple Mail Transfer Protocol)** : envoie des courriels.
- **Telnet** : accès distant à un serveur.
- **FTP (File Transfer Protocol)** : transfert de fichiers.

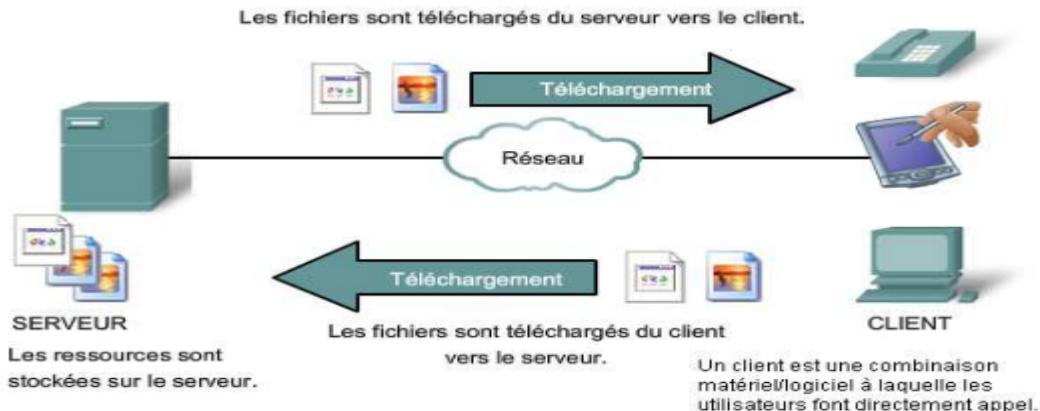
## 9. Modèle Client/Serveur

La plupart des communications sur Internet suivent ce modèle :

- **Le client** : envoie une requête (ex. : navigateur web demandant une page).
- **Le serveur** : répond avec les données demandées.

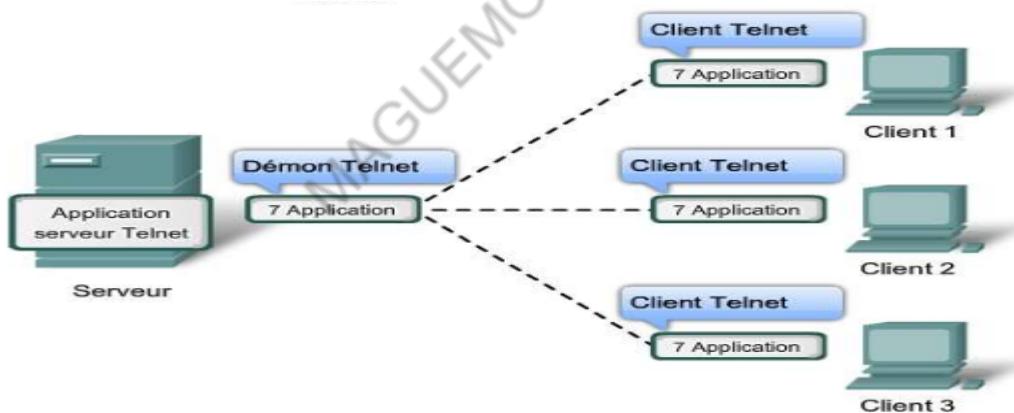
## Avantages du modèle Client/Serveur :

- ✓ Administration centralisée.
- ✓ Meilleure gestion de la sécurité.
- ✓ Performances optimisées.



## ✓ Explication de l'image

- Le client envoie une requête au serveur (ex. : « Je veux télécharger fichier.pdf »).
- Le serveur vérifie si le fichier est disponible et autorisé au téléchargement.
- Le fichier est envoyé en plusieurs paquets via TCP/IP.
- Le client reconstitue le fichier et peut l'utiliser.



## Telnet et le Modèle Client/Serveur

- Telnet est un protocole de communication qui permet d'accéder à distance à un serveur via une interface en ligne de commande.
- Il fonctionne en mode client/serveur :
  - Le client (ordinateur 1, 2 ou 3) se connecte au serveur Telnet.
  - Le serveur exécute les commandes envoyées et renvoie une réponse.
  - Cette connexion se fait via le port 23 (TCP).

## ✓ Explication de l'image

- Trois clients (1, 2, 3) sont connectés au même serveur Telnet.

- Chaque client envoie des commandes au serveur via une session Telnet.
- Le serveur exécute ces commandes et renvoie la réponse au client concerné.

### 👉 Utilité de Telnet

- Permet d'**administrer un serveur à distance**.
- Utile pour **configurer des équipements réseau** (routeurs, switchs).
- Moins sécurisé que SSH (car il n'utilise pas de chiffrement).

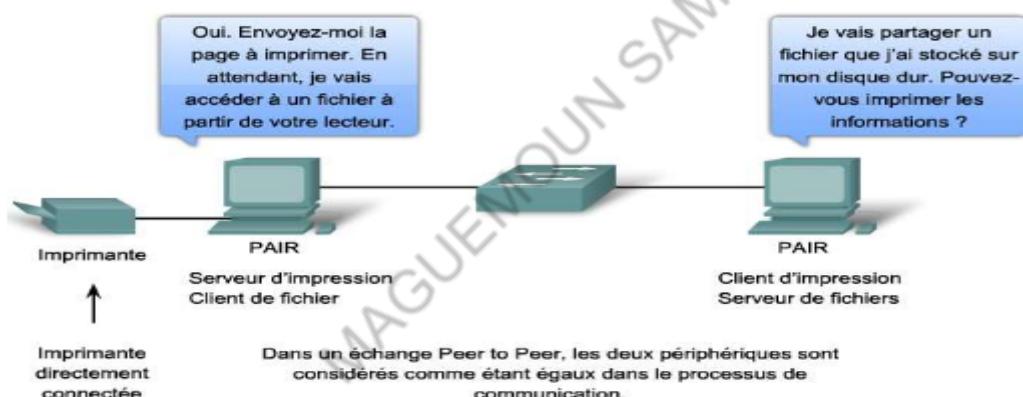
## 10. Modèle Peer-to-Peer (P2P)

Contrairement au modèle Client/Serveur, dans un réseau P2P :

- Chaque appareil (appelé **homologue**) peut être à la fois **client et serveur**.
- Il n'y a **pas de serveur centralisé**.

Exemples :

- **Partage de fichiers** (ex. : BitTorrent).
- **Jeux en réseau** sans serveur central.



### Le modèle Peer-to-Peer (P2P)

- Contrairement au modèle Client/Serveur, ici **chaque périphérique** du réseau peut agir **à la fois comme client et comme serveur**.
- Il n'y a **pas de serveur central** : les pairs (ordinateurs, imprimantes, etc.) communiquent directement entre eux.

### ✓ Explication de l'image

- Deux ordinateurs (Pairs 1 et 2) sont connectés entre eux.
- Une imprimante est aussi partagée dans le réseau P2P.
- Chaque ordinateur peut :
  - Partager des fichiers avec l'autre pair.
  - Accéder à l'imprimante sans passer par un serveur dédié.

## Comment ça fonctionne ?

1. **Partage de fichiers entre les pairs :**
  - Le **Pair 1** peut envoyer un fichier directement au **Pair 2**, et vice versa.
  - Pas besoin de passer par un serveur central.
2. **Impression en réseau :**
  - Les **deux pairs peuvent utiliser la même imprimante** connectée au réseau.
  - Ils envoient leurs documents directement, sans passer par un serveur d'impression.

## Avantages du modèle P2P illustré ici

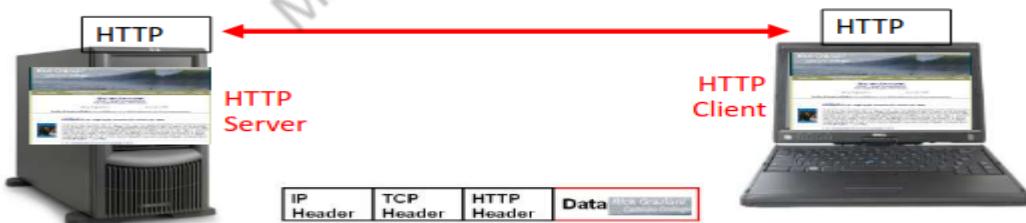
- **Facilité de partage** : Pas besoin de serveur, les fichiers et périphériques sont accessibles directement.
- **Économie de ressources** : Pas de serveur à entretenir, moins de coûts.
- **Flexibilité** : Chaque périphérique peut jouer plusieurs rôles (client/serveur).

## Exemples concrets

- **Réseau domestique** : Partage d'une imprimante et de fichiers entre plusieurs PC.
- **Petite entreprise** : Connexion entre ordinateurs sans infrastructure complexe.
- **Partage de fichiers en ligne** : Réseaux comme BitTorrent.

## 11. Protocole HTTP (HyperText Transfer Protocol)

- Permet d'afficher les pages web.
- Fonctionne en mode **client/serveur** (navigateur ↔ serveur web).
- Utilise le **port 80** (ou 443 pour HTTPS).
- Suit un **modèle requête/réponse**.



## 12. Protocole FTP (File Transfer Protocol)

- Utilisé pour **transférer des fichiers** entre un client et un serveur.
- Fonctionne avec deux connexions TCP :
  - **Port 21** : pour le contrôle (authentification, navigation).
  - **Port 20** : pour le transfert des fichiers.

Commandes FTP courantes :

- **get** : télécharger un fichier depuis le serveur.
- **put** : envoyer un fichier vers le serveur.

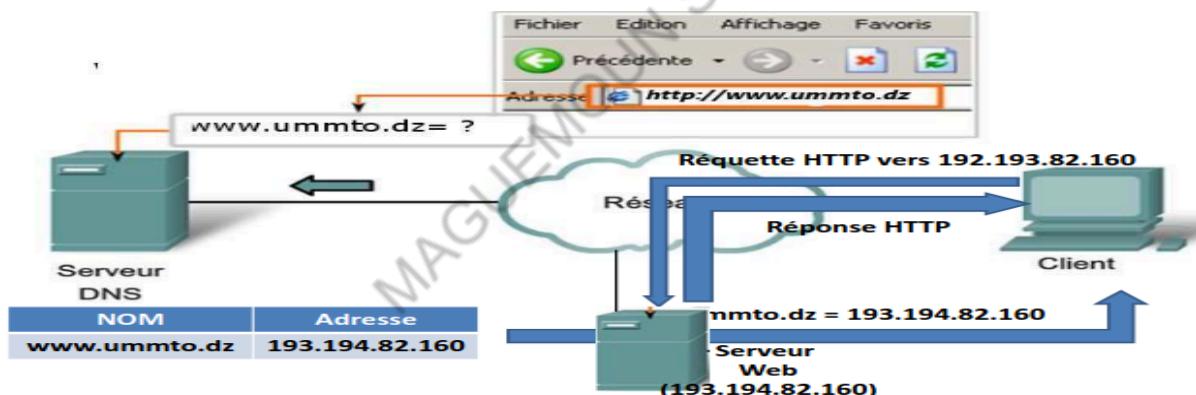


### 13. Protocole DNS (Domain Name System)

- Convertit un **nom de domaine** (ex. : [www.google.com](http://www.google.com)) en **adresse IP** (ex. : 142.250.190.78).
- Fonctionne via **les ports 53 UDP/TCP**.

Exemple de fonctionnement :

- Un utilisateur entre [www.ummtto.dz](http://www.ummtto.dz) dans son navigateur.
- Une requête est envoyée au **serveur DNS** pour obtenir l'adresse IP.
- Le serveur DNS répond avec **193.194.82.160**.
- L'ordinateur se connecte à **193.194.82.160** pour charger le site.

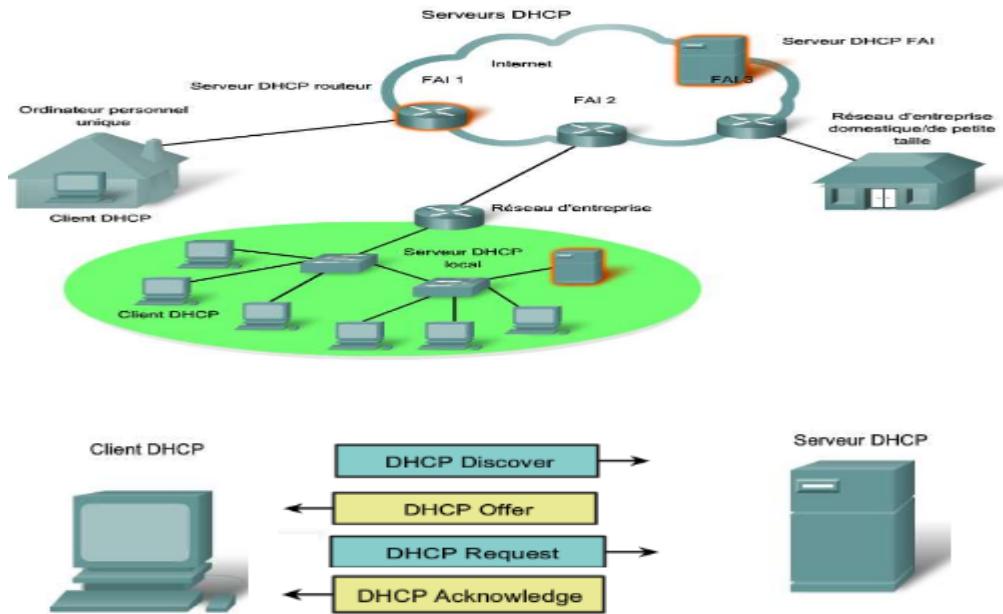


### 14. Protocole DHCP (Dynamic Host Configuration Protocol)

- Assigné **dynamiquement** une adresse IP aux périphériques d'un réseau.
- Fonctionne via **le port UDP 67**.

Étapes du processus DHCP :

- DHCP Discover** : le client envoie une demande d'adresse IP.
- DHCP Offer** : le serveur DHCP propose une adresse IP.
- DHCP Request** : le client accepte l'offre.
- DHCP Acknowledgment** : le serveur confirme l'attribution.



## 15. Problème réseau (Exemple de dépannage)

Si un utilisateur ne peut pas accéder à [www.ummto.dz](http://www.ummto.dz), mais qu'il peut accéder en entrant directement l'**adresse IP**, le problème est lié au **DNS**.

👉 Solution : vérifier la configuration DNS ou essayer un autre serveur DNS (ex. : Google DNS 8.8.8.8).

Remarque :

Le **hub** est un simple répéteur : il transmet les données à tous les ports sans distinction, ce qui peut engendrer des collisions. Le **switch**, plus intelligent, envoie les données uniquement vers le port du destinataire, réduisant ainsi le trafic inutile. Le **routeur**, quant à lui, connecte plusieurs réseaux entre eux (ex. : un réseau local à Internet) et décide du meilleur chemin pour acheminer les données.

**QCM :**

1 Quelle couche OSI est associée à l'adressage IP ?

✓ Réponse : Couche 3

- 1
- 2
- 3
- 4

2 Quel type d'adressage se trouve au niveau de la couche 2 du modèle OSI ? (Choisissez deux réponses.)

✓ Réponses : Physique, MAC

- Logique

- Physique
- MAC
- IP
- Port

3 Quel terme définit un ensemble donné de règles qui déterminent l'élaboration du format des messages et le processus d'encapsulation utilisés pour acheminer des données ?

Réponse : Le protocole

- La segmentation
- Le protocole
- Le multiplexage
- La QoS
- Le rassemblement

4 Parmi les éléments suivants, indiquez les protocoles associés à la couche 4 du modèle OSI (Choisissez deux réponses.)

Réponses : TCP, UDP

- IP
- TCP
- FTP
- TFTP
- UDP

5 Quelles sont les couches du modèle OSI composant la couche application du modèle TCP/IP ? (Choisissez trois réponses.)

Réponses : Session, Présentation, Application

- Liaison de données
- Réseau
- Transport
- Session
- Présentation
- Application

6 Quels protocoles utilisent l'authentification et le chiffrement pour sécuriser les transmissions de données entre le client et le serveur ? (Choisissez deux réponses.)

Réponses : HTTPS, SSH

- HTTP
- DNS
- HTTPS
- SNMP

- SSH

7 Un administrateur réseau tente de résoudre le problème d'accès à [www.ummto.dz](http://www.ummto.dz), la saisie de l'adresse IP dans le navigateur permet d'accéder correctement à la page. Quel est l'origine du problème ?

Réponse : DNS

- DHCP
- DNS
- CDP
- HTTP
- HTTPS
- SSL

8 Qu'est-ce qu'un réseau informatique ?

- A. Un ensemble de périphériques connectés à un ordinateur
- B. Un système permettant la communication entre plusieurs appareils
- C. Un logiciel permettant d'accéder à Internet
- D. Un câble reliant deux ordinateurs

Réponse : B

9 Quels sont les avantages d'un réseau informatique ? (Choisissez trois réponses.)

- A. Partage de fichiers
- B. Communication rapide
- C. Protection totale contre les virus
- D. Partage de ressources (imprimantes, stockage, etc.)

Réponses : A, B, D

10 Quelle est la principale différence entre un réseau LAN et WAN ?

- A. Le LAN est plus rapide que le WAN
- B. Le WAN est limité à un bâtiment
- C. Le LAN couvre une petite zone tandis que le WAN couvre une large zone
- D. Le LAN utilise Internet tandis que le WAN ne l'utilise pas

Réponse : C

11 Dans un réseau en étoile, quel élément centralise les connexions ?

- A. Un serveur
- B. Un routeur
- C. Un switch ou un hub
- D. Un ordinateur maître

Réponse : C

**12** Quel appareil est utilisé pour connecter différents réseaux entre eux ?

- A. Switch
- B. Hub
- C. Routeur
- D. Modem

 Réponse : C

**13** Quel est le rôle du protocole DNS ?

- A. Attribuer dynamiquement une adresse IP
- B. Traduire les noms de domaine en adresses IP
- C. Chiffrer les communications sur Internet
- D. Transmettre les emails

 Réponse : B

**14** Quelle est la fonction principale du protocole DHCP ?

- A. Convertir un nom de domaine en adresse IP
- B. Assurer la transmission des emails
- C. Attribuer automatiquement des adresses IP
- D. Établir des connexions sécurisées

 Réponse : C

**15** Quelle adresse IPv4 est réservée pour le réseau local (loopback) ?

- A. 255.255.255.255
- B. 192.168.1.1
- C. 127.0.0.1
- D. 10.0.0.1

 Réponse : C

**16** Quelle est la taille d'une adresse IPv6 ?

- A. 16 bits
- B. 32 bits
- C. 64 bits
- D. 128 bits

 Réponse : D

**17** Quel est le rôle du protocole HTTP ?

- A. Transférer des fichiers entre un client et un serveur
- B. Établir une connexion sécurisée entre deux appareils

- C. Transférer des pages Web
- D. Assurer l'envoi des emails

 **Réponse :** C

**18) Quelle est la différence entre TCP et UDP ?**

- A. TCP est plus rapide qu'UDP
- B. TCP assure une transmission fiable, UDP est plus rapide mais sans garantie
- C. UDP est utilisé pour les emails, TCP pour le Web
- D. UDP est sécurisé alors que TCP ne l'est pas

 **Réponse :** B

**19) Quelle couche du modèle OSI est responsable du transport fiable des données ?**

- A. Couche réseau
- B. Couche transport
- C. Couche application
- D. Couche physique

 **Réponse :** B

**20) À quoi sert une adresse MAC ?**

- A. Identifier un appareil sur un réseau local
- B. Identifier un site web sur Internet
- C. Traduire un nom de domaine en adresse IP
- D. Chiffrer les données envoyées

 **Réponse :** A

**21) Quel protocole est utilisé pour envoyer des emails ?**

- A. HTTP
- B. FTP
- C. SMTP
- D. DHCP

 **Réponse :** C

**22) Quel est le rôle d'un pare-feu (firewall) ?**

- A. Accélérer la connexion Internet
- B. Filtrer et sécuriser le trafic réseau
- C. Traduire les adresses IP
- D. Attribuer des adresses IP dynamiques

 **Réponse :** B

**[23] Dans quel cas utilise-t-on le modèle Peer-to-Peer (P2P) ?**

- A. Lorsqu'un serveur central contrôle toutes les communications
- B. Pour les connexions entre clients et serveurs web
- C. Pour le partage direct de fichiers entre utilisateurs sans serveur central
- D. Pour envoyer des emails

 Réponse : C

**[24] Quel type de câble est utilisé pour une connexion Ethernet standard ?**

- A. Fibre optique
- B. Coaxial
- C. RJ45 (câble twisted pair)
- D. USB

 Réponse : C

**[25] Quelle est la différence entre un switch et un hub ?**

- A. Un switch est plus lent qu'un hub
- B. Un hub envoie les données à tous les appareils, un switch les dirige intelligemment
- C. Un switch ne fonctionne qu'avec le Wi-Fi
- D. Un hub peut crypter les données, un switch non

 Réponse : B

**[26] Quelle est la plage d'adresses IP privées pour les réseaux locaux ?**

- A. 192.0.0.1 - 192.0.255.255
- B. 192.168.0.0 - 192.168.255.255
- C. 172.0.0.0 - 172.0.255.255
- D. 10.255.255.255 - 11.255.255.255

 Réponse : B

**[27] Quel service permet de prendre le contrôle à distance d'un autre ordinateur via un terminal ?**

- A. HTTP
- B. Telnet
- C. SSH
- D. FTP

 Réponse : C

**[28] Quel protocole est utilisé pour le transfert de fichiers sur un réseau ?**

- A. HTTP
- B. FTP

- C. SMTP
- D. DHCP

 **Réponse :** B

**[29] Quelle technologie est utilisée pour sécuriser les communications sur Internet ?**

- A. HTTP
- B. SSL/TLS
- C. FTP
- D. DHCP

 **Réponse :** B

**[30] Quelle commande permet de tester la connectivité entre deux appareils sur un réseau ?**

- A. nslookup
- B. ping
- C. tracert
- D. netstat

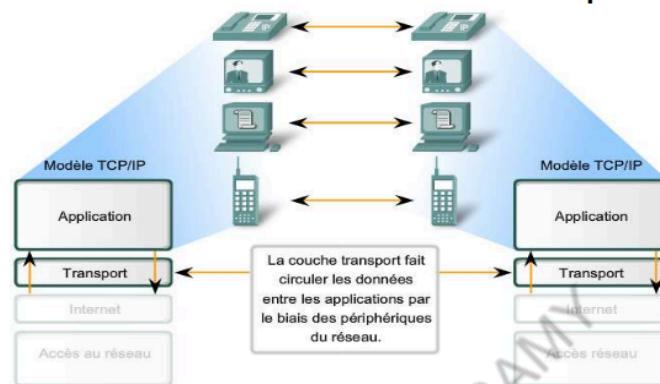
 **Réponse :** B

MAGUEMOUN SAMY

## Couche Transport

### 1/ Modèle TCP/IP

- Le modèle TCP/IP est utilisé pour organiser la communication sur les réseaux.
- Il se compose de **quatre couches** :
  1. **Application** : Interface avec l'utilisateur (ex. : HTTP, FTP, SMTP).
  2. **Transport** : Gère la transmission fiable des données (ex. : TCP, UDP).
  3. **Internet** : Acheminement des paquets via des adresses IP.
  4. **Accès réseau** : Gère la connexion physique et les protocoles de liaison.

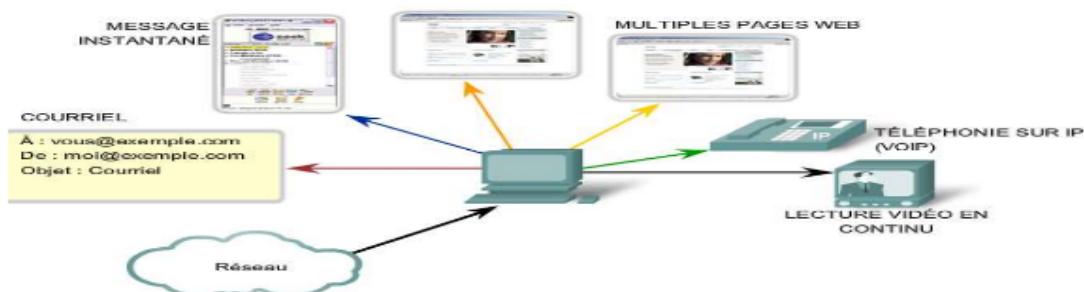


Cette image illustre le modèle TCP/IP et met en évidence la couche transport. La couche transport permet la circulation des données entre les applications en utilisant les périphériques du réseau. Elle joue un rôle clé dans l'acheminement des données entre les couches supérieures (Application) et les couches inférieures (Internet et Accès réseau).

### 2/Objectifs de la couche transport

La couche transport assure plusieurs fonctions clés :

- **Suivi des conversations individuelles** : assure la gestion simultanée et ordonnée des communications entre applications.



Cette image montre différentes applications qui utilisent la couche transport: messagerie instantanée, courriel, navigation web (plusieurs

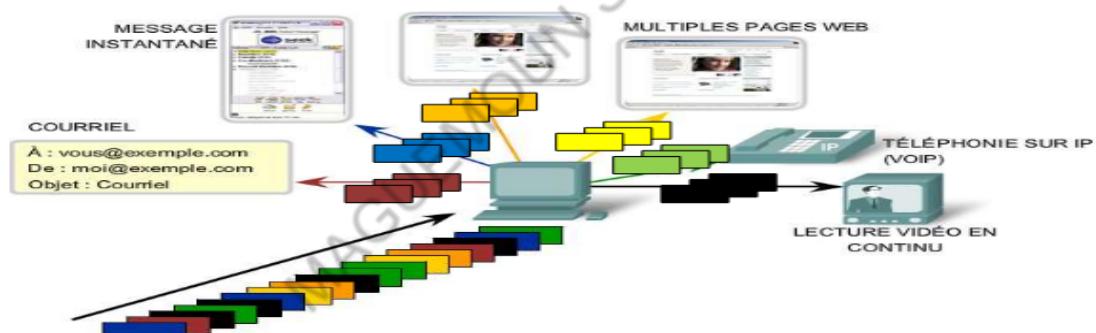
pages),téléphonie sur IP (VoIP),lecture vidéo en continu. La couche transport permet à toutes ces applications d'envoyer et recevoir des données via le réseau.

- **Segmentation des données** : Découpe les flux de données en petits segments.



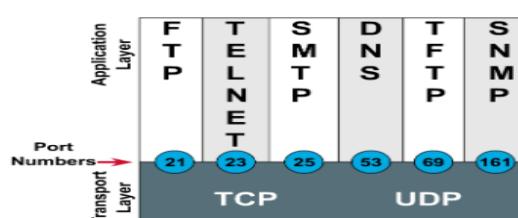
Cette image illustre comment la segmentation facilite l'utilisation du réseau par plusieurs applications simultanément. La segmentation permet de diviser les flux de données pour mieux gérer leur transport. Un contrôle d'erreur est appliqué pour s'assurer que les données reçues sont correctes.

- **Reconstitution des segments** : Réassemble les données reçues.



Ici, on observe que les segments de données sont classés par couleur selon leur application d'origine. L'ordinateur reçoit des segments de différentes applications (courriel, web, VoIP, etc.) et les traite en parallèle. Cette organisation optimise la transmission et évite les conflits entre flux de données.

- **Identification des applications** : Utilise des numéros de port pour diriger les données.

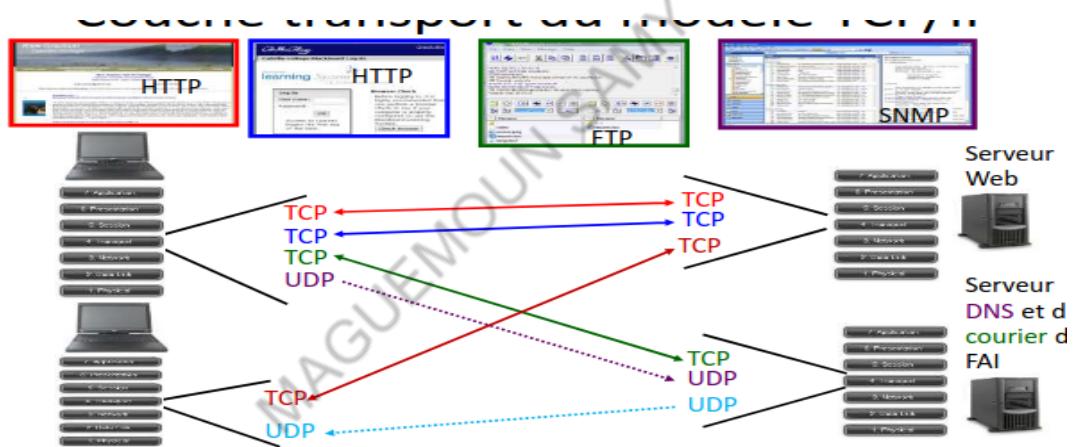


Cette image montre les principaux protocoles applicatifs et leurs numéros de ports associés. Elle illustre la séparation entre **TCP** (protocole fiable, orienté connexion) et **UDP** (protocole rapide, sans connexion). Ces ports permettent aux applications de communiquer efficacement via la couche transport.

- **Fiabilité** : Assure que toutes les données sont bien reçues et dans le bon ordre.
- **Contrôle de flux** : Régule la quantité de données envoyées pour éviter la surcharge du destinataire.
- **Livraison dans un ordre défini** : La couche transport numérote et ordonne les segments pour garantir leur réassemblage dans le bon ordre à la réception.
- **Établissement de session** : Initie et termine les connexions entre les applications.

### 3/Couche transport du modèle TCP/IP

- Les applications comme les bases de données et les courriels nécessitent une transmission fiable via TCP, tandis que d'autres, comme la vidéo en streaming, tolèrent la perte de données et utilisent UDP. TCP établit une connexion bidirectionnelle entre les hôtes, contrairement à UDP, qui fonctionne sans connexion.



L'image illustre le rôle de la couche transport du modèle TCP/IP en gérant la communication entre des applications clientes et des serveurs via les protocoles TCP et UDP. Différents services (HTTP, FTP, SNMP) utilisent TCP pour une transmission fiable, tandis que certains services comme DNS exploitent UDP pour une transmission rapide.

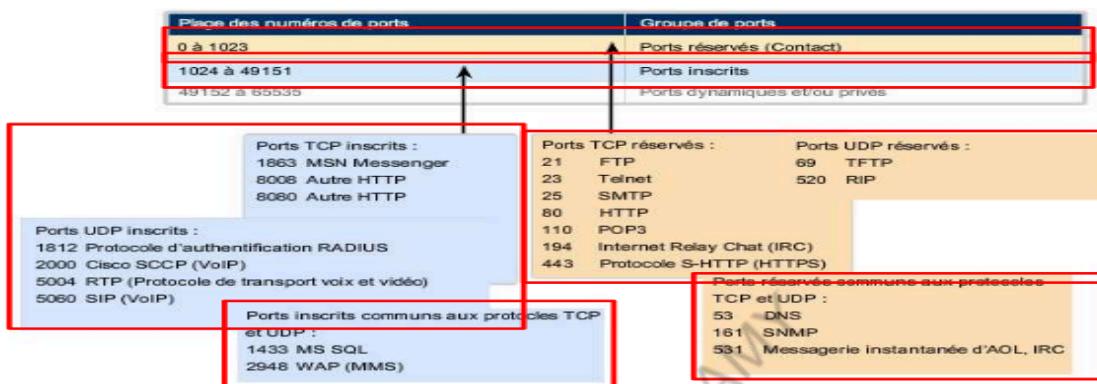
### 4/Différences entre TCP et UDP

| Fonctionnalité   | TCP                              | UDP              |
|------------------|----------------------------------|------------------|
| Connexion        | Oui                              | Non              |
| Fiabilité        | Oui                              | Non              |
| Contrôle de flux | Oui                              | Non              |
| Vitesse          | Plus lent                        | Rapide           |
| Utilisation      | Web, mail, transfert de fichiers | Vidéo, VoIP, DNS |

## 5/Numéros de port TCP et UDP

Les numéros de port permettent d'identifier les applications qui communiquent. Ils sont classés en trois catégories :

- Ports réservés (0 - 1023)** : Pour les services courants (HTTP - 80, SMTP - 25, DNS - 53).
- Ports enregistrés (1024 - 49151)** : Attribués à des applications spécifiques.
- Ports dynamiques (49152 - 65535)** : Utilisés temporairement pour les connexions clients.



Cette image explique la classification des numéros de ports dans le modèle TCP/UDP en fonction de leur utilisation.

### 1. Classification des ports :

- Ports réservés (0 à 1023)** : Utilisés pour des services bien connus comme HTTP (80), HTTPS (443), FTP (21) et DNS (53).
- Ports inscrits (1024 à 49151)** : Assignés à des applications spécifiques comme MSN Messenger (1863) et VoIP (5060).
- Ports dynamiques ou privés (49152 à 65535)** : Utilisés temporairement pour des connexions client-serveur.

### 2. Exemples de ports réservés :

- TCP** : FTP (21), HTTP (80), HTTPS (443), Telnet (23), SMTP (25), IRC (194).
- UDP** : TFTP (69), RIP (520).

### 3. Ports UDP et TCP couramment utilisés :

- UDP** : DNS (53), SNMP (161), messagerie AOL/IRC (163).
- TCP** : SQL Server (1433), WAP (2948).

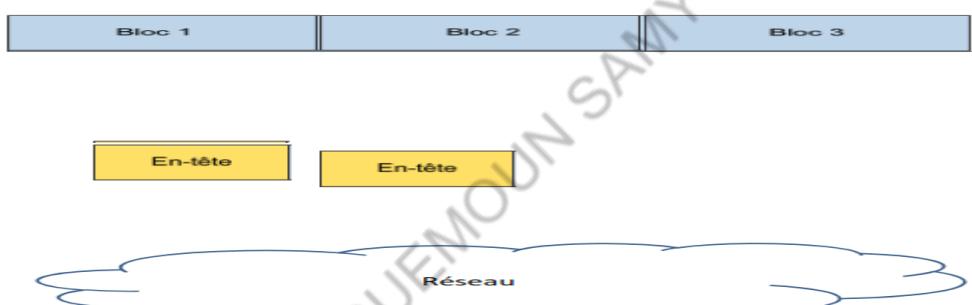
L'image montre aussi la distinction entre TCP (qui assure une connexion fiable) et UDP (plus rapide mais sans garantie de livraison).

## 6/Protocole TCP (Transmission Control Protocol)

- TCP est un **protocole fiable** qui garantit que les données arrivent complètes et dans le bon ordre.
- Il est utilisé pour les applications nécessitant une **transmission fiable** : Web, e-mails, transfert de fichiers.
- Fonctionnalités principales :
  - Livraison dans l'ordre.
  - Contrôle des erreurs et des flux.
  - Accusé de réception des paquets envoyés.

## 7/Segmentation des données par le protocole TCP

- Les **données sont découpées en segments** avant transmission.
- Chaque segment contient un en-tête avec des informations essentielles :
  - **Numéro de séquence** : Identifie l'ordre des segments.
  - **Accusé de réception (ACK)** : Confirme la bonne réception.
  - **Contrôle d'erreurs** : Vérifie l'intégrité des données.



## 8/En-tête du protocole TCP

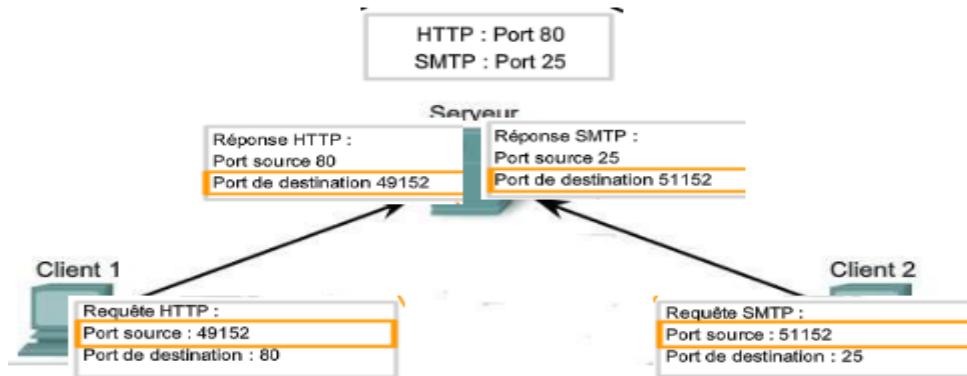
L'en-tête TCP contient plusieurs champs importants :

- **Port source/destination** : Identifie l'application d'envoi et de réception.
- **Numéro de séquence** : Indique la position du segment dans la transmission.
- **Numéro d'acquittement** : Confirme la réception des segments précédents.
- **Fenêtre de contrôle de flux** : Détermine la quantité de données pouvant être envoyée.



## 9/Fonctionnement du protocole TCP

- Chaque service utilise un numéro de port dédié.
- Le client envoie une requête au serveur avec un **port source dynamique** et un **port destination fixe**.
- Le serveur répond avec son **port source fixe** et le **port destination du client**.



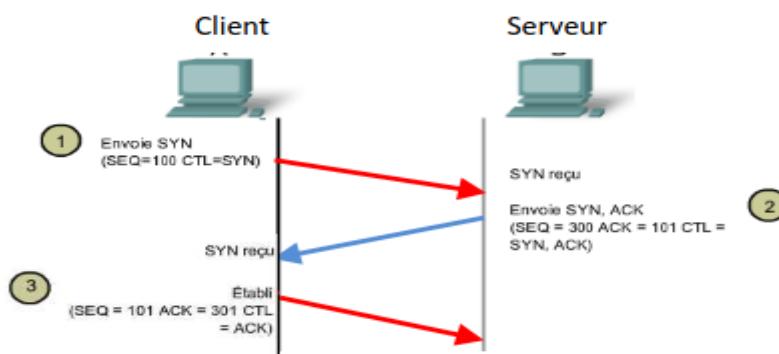
## 10/TCP est un protocole avec connexion

- TCP nécessite l'**établissement d'une connexion** avant de commencer la transmission.
- Une fois la communication terminée, TCP **ferme la connexion** proprement.
- Processus en trois phases :
  1. **Établissement de connexion**
  2. **Transmission des données**
  3. **Fermeture de la connexion**

La connexion sert à vérifier la disponibilité du périphérique et du service, ainsi qu'à initier une session de communication.

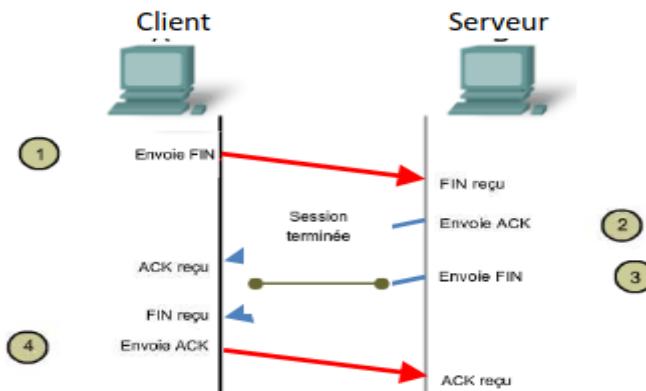
## 11/Établissement d'une session TCP

- Se fait en **trois étapes (Three-Way Handshake)** :
  1. **SYN** : Le client envoie une demande de connexion.
  2. **SYN-ACK** : Le serveur confirme la demande.
  3. **ACK** : Le client valide la connexion.

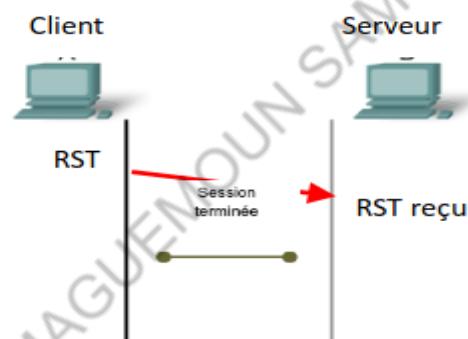


## 12/Terminaison d'une session TCP

- Un client peut envoyer un segment **FIN** pour demander la fermeture.
- Le serveur répond avec **ACK** et peut envoyer son propre **FIN**.
- La connexion se termine après confirmation finale.



## 13/Autre terminaison



L'image montre la terminaison brutale d'une session TCP où le client envoie un segment **RST** (Reset) pour interrompre immédiatement la connexion avec le serveur.

### Exercice :

Soit un échange entre A et B (A va initier l'ouverture de la connexion)

La machine B qui va fermer la connexion

Le numéro initial de A est égal à 20 et celui de B est 40

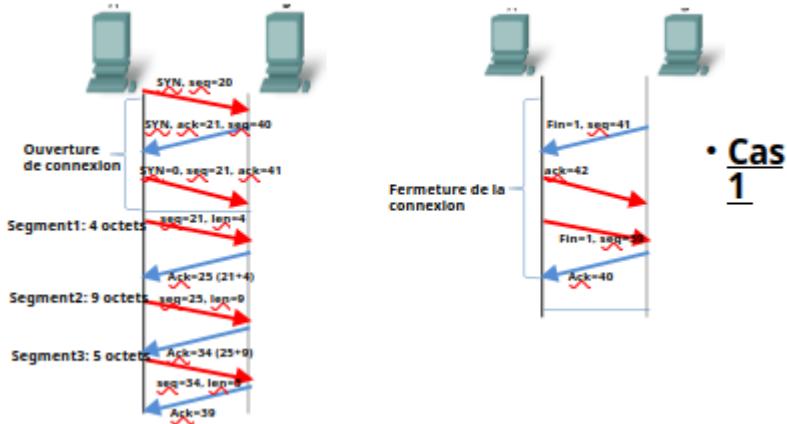
La taille de données transférée entre A et B est 18 octets

Cas1: les données sont transmises en trois segments (4, 9 et 5 octets)

Cas2: les données sont transmises en deux segments:  
segment1 de taille 10 octets et le second de taille 8 octets

Sans perte de données ni d'acquitements

Représenter le transfert TCP dans les deux cas



### • Cas 1

## 1 Ouverture de la connexion (Three-Way Handshake)

Ce processus est utilisé pour établir une connexion TCP fiable entre les deux hôtes. Il se fait en trois étapes :

1. Le client envoie un paquet SYN (Synchronize) avec un numéro de séquence initial (**seq=20**).
2. Le serveur répond avec un SYN-ACK (**seq=40, ack=21**).
3. Le client envoie un ACK (**seq=41, ack=21**), confirmant la connexion.

Après cela, la connexion est établie et les données peuvent être échangées.

## 2 Échange de données

Les segments sont transmis du client vers le serveur, avec des accusés de réception (ACK) pour garantir la bonne réception.

- Segment 1 : 4 octets envoyés (**seq=21**), accusé de réception (**Ack=25**).
- Segment 2 : 9 octets envoyés (**seq=25**), accusé de réception (**Ack=34**).
- Segment 3 : 5 octets envoyés (**seq=34**), accusé de réception (**Ack=39**).

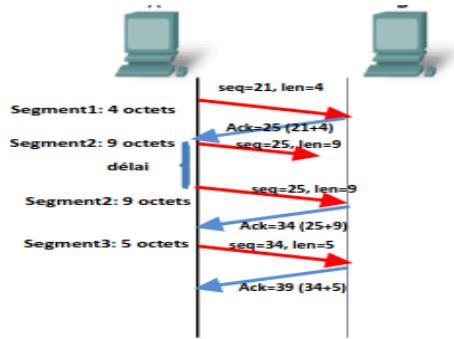
Le client envoie les données avec des numéros de séquence (**seq**) et attend un **ACK** du serveur pour chaque segment reçu.

## 3 Fermeture de la connexion (Four-Way Handshake)

La fermeture d'une connexion TCP nécessite quatre étapes :

1. Le client envoie un FIN (**seq=41**) pour indiquer qu'il veut terminer la connexion.
2. Le serveur répond avec un ACK (**ack=42**), confirmant qu'il a reçu le FIN.
3. Le serveur envoie ensuite son propre FIN (**seq=39**) pour signaler qu'il veut aussi fermer la connexion.
4. Le client répond avec un ACK final (**ack=40**), terminant ainsi la connexion.

## Cas de perte de segment

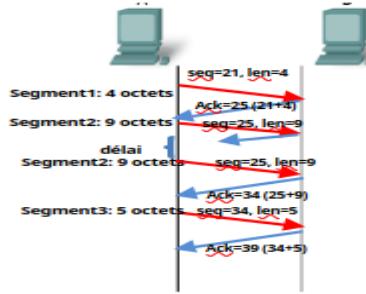


Cette image illustre un **cas de perte de segment** dans une communication **TCP** et comment le protocole gère cette situation grâce aux accusés de réception (**ACK**).

## Déroulement de la transmission

- Envoi du premier segment :**
  - Le client envoie un segment de **4 octets** (**seq=21, len=4**).
  - Le serveur le reçoit et répond avec un accusé de réception (**Ack=25**), confirmant qu'il attend la séquence **25**.
- Envoi du deuxième segment :**
  - Le client envoie un segment de **9 octets** (**seq=25, len=9**).
  - Cependant, ce segment est **perdu** à cause d'un délai ou d'une erreur de transmission.
- Attente et retransmission :**
  - Le serveur **ne reçoit pas** le segment **seq=25, len=9**, donc il **n'envoie pas de nouvel ACK**.
  - TCP détecte cette perte grâce au **timeout** ou par réception d'ACKs dupliqués.
- Retransmission du segment perdu :**
  - Après un certain délai, le client **renvoie le segment perdu** (**seq=25, len=9**).
  - Cette fois, le serveur le reçoit et envoie un accusé de réception (**Ack=34**), indiquant qu'il attend **seq=34**.
- Transmission du troisième segment :**
  - Le client continue avec l'envoi du segment suivant de **5 octets** (**seq=34, len=5**).
  - Le serveur répond avec un dernier accusé de réception (**Ack=39**), signifiant que tous les segments ont bien été reçus.

# Cas de perte d'acquittement



Cette image illustre un **cas de perte d'accusé de réception (ACK)** dans une communication TCP, et comment le protocole TCP réagit pour garantir la fiabilité de la transmission.

## ✓ Segment 1

- Le client envoie un segment de **4 octets** : seq=21, len=4.
- Le serveur reçoit le segment et envoie **Ack=25 (21+4)**, **accusant réception** du segment.

## ✓ Segment 2

- Le client envoie un segment de **9 octets** : seq=25, len=9.
- Le serveur reçoit bien le segment...
- MAIS **l'ACK est perdu** (il ne parvient pas au client).

## ⌚ Conséquence du délai

- Le client attend un accusé de réception.
- Comme il ne le reçoit pas (ACK perdu), il **retransmet le segment** : seq=25, len=9.

## ⟳ Retransmission et suite

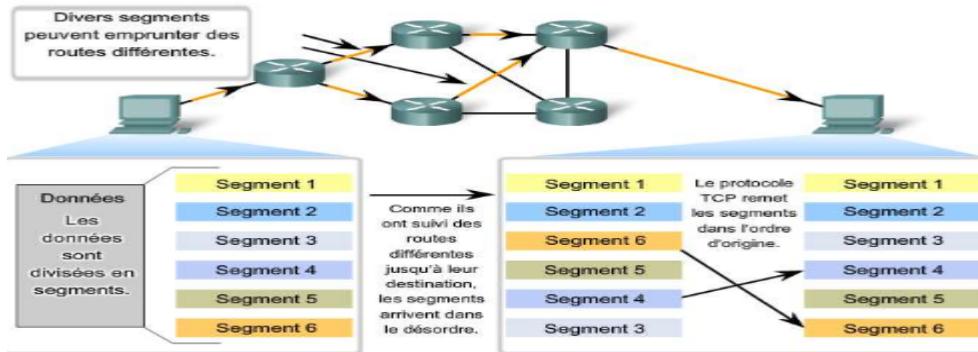
- Le serveur reçoit **deux fois** le même segment seq=25, mais comme TCP est conçu pour être fiable, il reconnaît le doublon.
- Il renvoie un nouvel ACK : **Ack=34**.

## ✓ Segment 3

- Le client envoie ensuite un segment de **5 octets** : seq=34, len=5.
- Le serveur accorde réception avec **Ack=39**.

## 14/ Ordonnancement des segments TCP

- Les segments peuvent arriver **dans le désordre**.
- TCP réassemble les segments dans le bon ordre avant de les transmettre à l'application.



### Explication de l'image: réassemblage des segments TCP

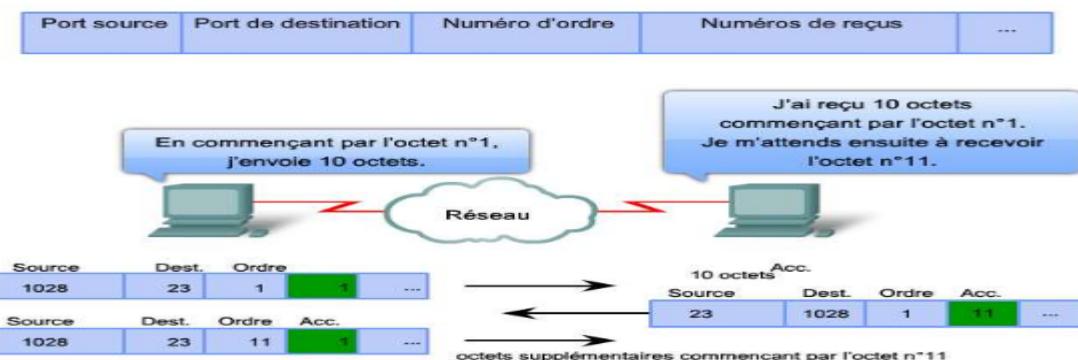
- **Principe** : Les données sont divisées en segments avant d'être envoyées sur le réseau.
- **Multiples chemins** : Les segments ne suivent pas nécessairement la même route, ce qui peut entraîner une arrivée désordonnée à destination.
- **Réassemblage par TCP** : TCP remet les segments dans l'ordre correct avant de les transmettre à l'application.

### Procédure d'ordonnancement :

TCP attribue un numéro d'ordre initial aux octets transmis, l'incrémenter à chaque envoi et stocke les segments reçus dans un tampon. Il les réordonne, conserve les segments non contigus jusqu'à complétion, puis transmet les données à l'application.

## 15/TCP est un protocole fiable

- TCP garantit la **bonne réception des données**.
- Si un segment est perdu, il est **réémis automatiquement**.



### Explication de l'image: Chaque segment contient un numéro de séquence indiquant le premier octet qu'il transporte.

**Accusé de réception (ACK)** : Le récepteur envoie un accusé pour confirmer la réception des données et indiquer quel octet il attend ensuite.

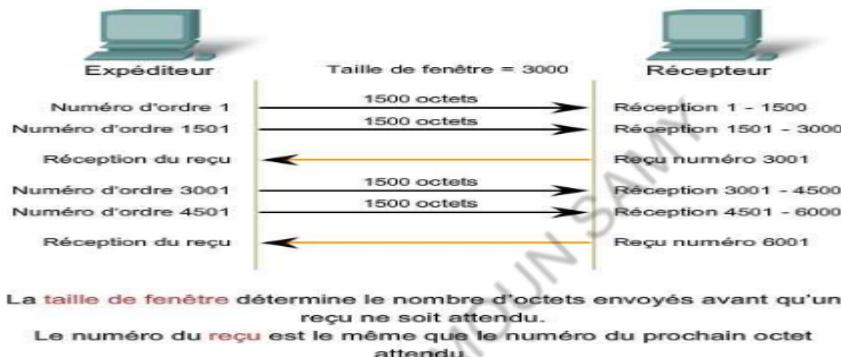
- L'émetteur envoie 10 octets, en commençant par l'octet numéro 1.
- Le récepteur reçoit ces 10 octets et attend le suivant (octet 11).
- Il envoie alors un accusé de réception indiquant qu'il attend l'octet 11, et ainsi de suite.

#### Traitement des pertes de segments:

TCP retransmet les segments non acquittés : il garde une copie des segments envoyés, attend un accusé de réception et les supprime une fois reçus. Si aucun accusé n'arrive après un délai, il retransmet les données depuis le dernier octet confirmé.

#### 16/TCP permet le contrôle de flux

- TCP ajuste le flux de données selon les ressources disponibles.
- Utilise une **fenêtre de congestion** pour limiter les données envoyées avant acquittement.
- L'émetteur envoie plusieurs segments jusqu'à atteindre cette limite, puis attend un acquittement avant de continuer.



Cette image illustre le **contrôle de flux TCP** avec le mécanisme de la **fenêtre d'envoi**. Voici les points clés :

1. **Taille de fenêtre = 3000 octets :**
  - L'émetteur peut envoyer jusqu'à 3000 octets sans attendre d'acquittement.
  - Ici, les données sont envoyées en segments de 1500 octets.
2. **Transmission des segments :**
  - L'expéditeur envoie deux segments (1500 octets chacun), atteignant la limite de 3000 octets.
  - Le récepteur reçoit les données et envoie un **accusé de réception (ACK)** indiquant qu'il attend l'octet suivant (numéro 3001).
3. **Nouvelle transmission :**
  - Une fois l'ACK reçu, l'émetteur envoie encore 3000 octets (deux segments de 1500).
  - Le récepteur acquitte en indiquant qu'il attend l'octet 6001.

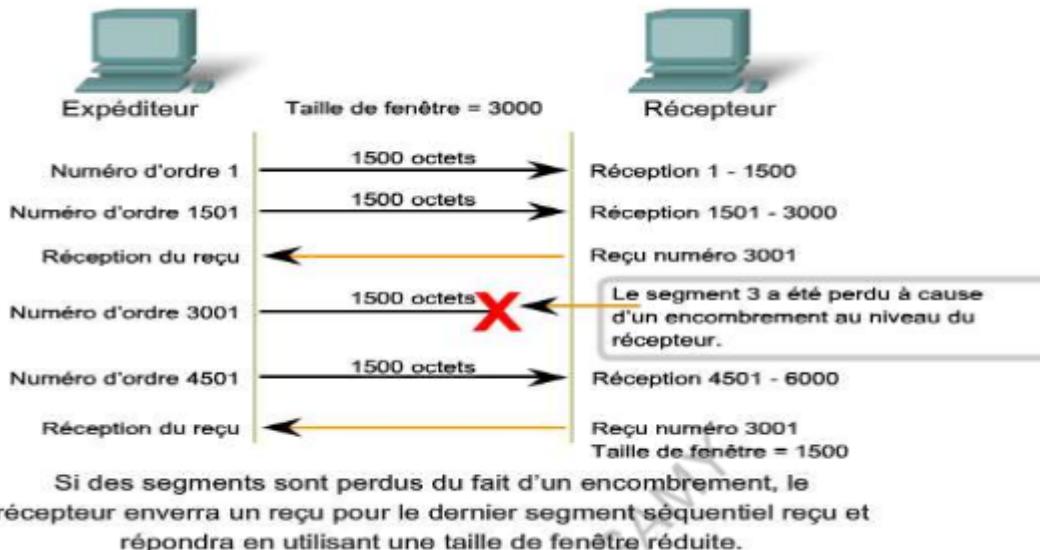
#### Conclusion :

- La fenêtre de réception définit combien de données peuvent être envoyées avant de devoir recevoir un accusé de réception.
- Le numéro d'acquittement correspond toujours au prochain octet attendu.
- Ce mécanisme optimise le débit tout en évitant une surcharge du récepteur.

## Réduction de la taille de fenêtre :

TCP ajuste dynamiquement la taille de fenêtre pour s'adapter aux conditions du réseau. En cas de congestion, la taille de fenêtre est réduite pour ralentir la transmission. Si aucune perte n'est détectée après un certain temps, la taille de fenêtre est progressivement augmentée.

Objectif : Trouver la taille de fenêtre optimale pour une transmission efficace.



L'image montre comment TCP gère la perte de segments due à l'encombrement du réseau:

- L'expéditeur envoie des segments de **1500 octets** chacun.
- Un segment est perdu (**3001 - 4500**), empêchant le récepteur d'accuser réception des suivants.
- Le récepteur répète l'accusé de réception précédent (**3001**) pour signaler la perte.
- TCP réduit la taille de fenêtre pour éviter la surcharge et retransmet le segment manquant.
- Une fois reçu, la transmission reprend normalement.

Cela illustre le **contrôle de flux TCP** et l'ajustement dynamique du débit.

## 17/Protocole UDP (User Datagram Protocol)

- **UDP est un protocole léger et rapide.**
- Il ne garantit pas la livraison des paquets ni leur ordre d'arrivée.
- Utilisé pour :
  - **DNS (Domain Name System)**
  - **Streaming vidéo**
  - **VoIP (appels Internet)**
  - **Jeux en ligne**

## Datagramme UDP



L'image représente le **format d'un datagramme UDP** (User Datagram Protocol). UDP est un protocole de transport non fiable et sans connexion, utilisé pour les transmissions rapides comme la voix sur IP ou le streaming.

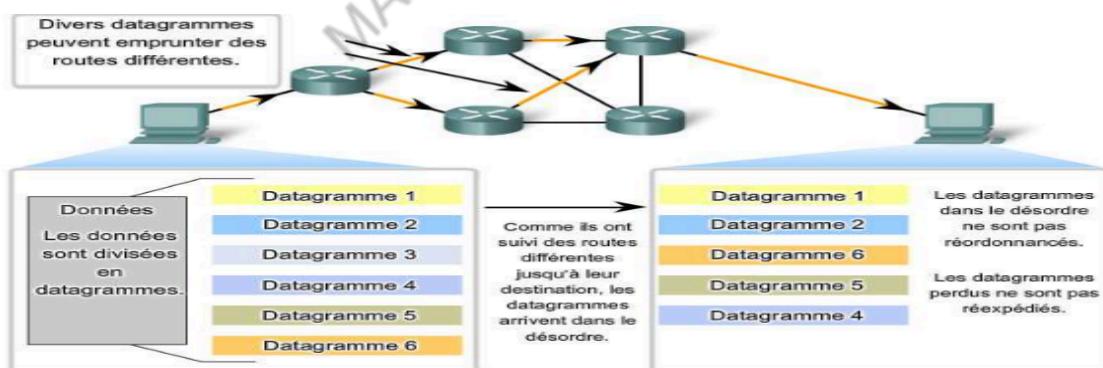
### Explication des champs :

- Port source (16 bits)** : Identifie le port de l'application émettrice.
- Port de destination (16 bits)** : Identifie le port de l'application réceptrice.
- Longueur (16 bits)** : Indique la taille totale du datagramme (en-tête + données).
- Somme de contrôle (16 bits)** : Vérifie l'intégrité des données (peut être désactivée).
- Données de la couche application** : Contenu réel transmis, de taille variable.

💡 Contrairement à TCP, **UDP ne gère pas l'ordonnancement ni la retransmission** des paquets, ce qui le rend plus rapide mais moins fiable.

### 18/UDP n'effectue pas d'ordonnancement

- Les paquets UDP peuvent arriver **dans n'importe quel ordre**.
- Aucune réorganisation n'est effectuée.



L'image illustre le fonctionnement du **protocole UDP (User Datagram Protocol)** et son mode de transmission des données.

### Explication :

- Fragmentation des données** :
  - Les données sont divisées en plusieurs **datagrammes** avant d'être envoyées sur le réseau.

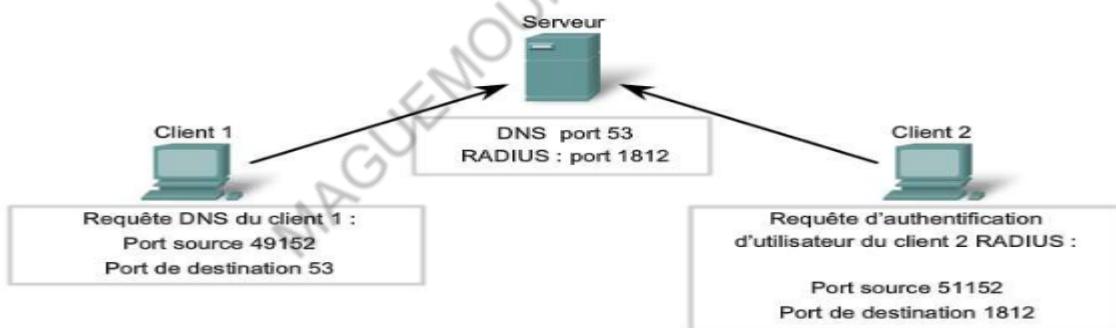
2. **Transmission sur différentes routes :**
  - Chaque datagramme peut emprunter un **chemin différent** pour atteindre sa destination.
3. **Désordre à l'arrivée :**
  - Comme ils suivent des routes distinctes, les datagrammes arrivent **dans le désordre**.
  - Contrairement à TCP, **UDP ne réordonne pas** les paquets.
4. **Absence de retransmission :**
  - Si un datagramme est perdu en cours de route, **il n'est pas renvoyé**.
  - UDP ne garantit pas la livraison des données, ce qui peut entraîner des pertes.

## Conclusion :

- UDP est plus rapide que TCP mais ne gère ni l'**ordre** ni la **fiabilité** des paquets.
- Il est souvent utilisé pour les applications où la vitesse est prioritaire, comme le **streaming, la voix sur IP (VoIP) et les jeux en ligne**.

## 19/Fonctionnement du protocole UDP

- Chaque application utilisant UDP est identifiée par un **numéro de port**.
- UDP **envoie les données immédiatement**, sans attendre d'accusé de réception.



L'image montre deux clients envoyant des requêtes à un serveur via des ports spécifiques :

- **Client 1** envoie une requête DNS au **port 53** du serveur depuis un **port source 49152**.
  - **Client 2** envoie une requête d'authentification RADIUS au **port 1812** depuis un **port source 51152**.
- Chaque client utilise un port source aléatoire, tandis que le serveur écoute sur des ports bien définis.

## 20/Conclusion

- La **couche transport** est essentielle pour la communication entre applications.
- **TCP** est utilisé quand la fiabilité est requise.
- **UDP** est préféré pour les applications nécessitant une transmission rapide.
- Le choix du protocole dépend du **besoin de l'application**.

**QCM :**

**1** Dans la couche transport, lequel des contrôles suivants permet d'éviter qu'un hôte transmette des données provoquant un dépassement de capacité des mémoires tampons de l'hôte en réception ?

- Le niveau de service Best effort
- Le chiffrement
- Le contrôle de flux**
- La compression
- La prévention d'encombrement

**2** Les systèmes d'extrémité utilisent des numéros de port pour sélectionner l'application appropriée. Quel est le plus petit numéro de port pouvant être attribué de façon dynamique par un système hôte ?

- 1
- 64
- 128
- 256
- 512
- 1024**

**3** Lors du transfert des données, quelles sont les principales responsabilités de l'hôte récepteur ? (Choisissez deux réponses.)

- Le débit
- L'encapsulation
- L'accusé de réception**
- La bande passante
- La segmentation
- Le râssemblage**

**4** Dans quelle couche du modèle TCP/IP intervient le protocole TCP ?

- La couche session
- La couche transport**
- La couche réseau
- La couche liaison de données

**5** Qu'est-ce qui détermine la quantité de données qu'une station émettrice exécutant le protocole TCP/IP peut transmettre avant de recevoir un accusé de réception ?

- La taille du segment
- Le débit de transmission
- La bande passante
- La taille de fenêtre**
- Le numéro de séquence

**6** Quelle est la fonction du numéro d'ordre inclus dans l'en-tête TCP ?

- Il râssemble les segments en données complètes.**
- Il identifie le protocole de la couche application.
- Il indique le numéro de l'octet suivant attendu.
- Il précise le nombre maximal d'octets autorisés lors d'une session.

**7** Quelle est la fonction des numéros de ports TCP/UDP ?

- Ils permettent d'indiquer le début d'un échange en trois étapes.
- Ils permettent de réorganiser les segments dans l'ordre adéquat.
- Ils permettent d'identifier le nombre de paquets pouvant être envoyés sans accusé de réception.
- Ils permettent de suivre les différentes conversations simultanées dans un réseau.

**8** Parmi les éléments suivants, indiquez les protocoles associés à la couche 4 du modèle OSI. (Choisissez deux réponses.)

- TCP
- UDP
- IP
- ICMP
- HTTP

**9** Quelle est la principale différence entre TCP et UDP ?

- TCP est orienté connexion, tandis qu'UDP est sans connexion.
- TCP est plus rapide qu'UDP.
- UDP garantit la fiabilité des données.
- TCP ne permet pas la retransmission des segments perdus.

**10** Quel mécanisme TCP garantit la livraison fiable des segments ?

- La taille de fenêtre
- L'accusé de réception (ACK)
- L'encapsulation
- La QoS

**11** Qu'est-ce qu'un handshake en trois étapes dans TCP ?

- Une procédure d'établissement de connexion entre deux hôtes.
- Un processus de fermeture de connexion
- Une technique de cryptage des données
- Une méthode pour accélérer la transmission

**12** Pourquoi TCP utilise-t-il un numéro de séquence dans ses en-têtes ?

- Pour assurer l'ordonnancement et la fiabilité des données.
- Pour identifier l'émetteur du segment
- Pour contrôler la congestion
- Pour crypter les données

**13** Quelle est la taille d'un en-tête TCP standard sans options ?

- 12 octets
- 16 octets
- 20 octets
- 32 octets

**14** Que signifie le bit SYN dans un segment TCP ?

- Il indique une demande d'établissement de connexion.
- Il signale la fin d'une transmission.

- Il permet de segmenter les paquets.
- Il contrôle le débit.

**15) Que signifie le bit FIN dans un segment TCP ?**

- Il demande une augmentation de la taille de fenêtre.
- Il indique une demande de fermeture de connexion.
- Il vérifie l'intégrité des paquets.
- Il est utilisé pour le chiffrement.

**16) Comment TCP gère-t-il la congestion du réseau ?**

- Avec des algorithmes comme Slow Start et Congestion Avoidance.
- En supprimant les paquets en excès.
- En augmentant la taille de fenêtre de façon illimitée.
- En redirigeant les paquets vers un autre chemin.

**17) Que se passe-t-il lorsqu'un segment TCP est perdu en transmission ?**

- L'émetteur abandonne la connexion.
- L'émetteur retransmet le segment après expiration du timer.
- Le destinataire envoie un message d'erreur.
- Le segment est ignoré.

**18) Pourquoi UDP est-il souvent utilisé pour la diffusion en continu ?**

- Parce qu'il est rapide et ne nécessite pas d'accusé de réception.
- Parce qu'il assure une transmission fiable.
- Parce qu'il est compatible avec TCP.
- Parce qu'il permet de compresser les paquets.

**19) Quelle commande permet de tester une connexion TCP vers un serveur ?**

- ping
- telnet [adresse] [port]
- tracert
- netstat

**20) Quelle est la principale raison pour laquelle TCP utilise une fenêtre coulissante ?**

- Pour optimiser le débit des transmissions.
- Pour crypter les données.
- Pour réduire la latence.
- Pour gérer les ports dynamiques.

**21) Quel mécanisme permet d'éviter la surcharge du réseau dans TCP ?**

- Le contrôle de congestion
- Le chiffrement des données
- Le filtrage des paquets
- L'encapsulation

**22) Quel est le rôle du flag RST dans un segment TCP ?**

- Il réinitialise immédiatement la connexion en cours.
- Il signale la fin normale d'une connexion.

- Il indique une erreur de checksum.
- Il démarre une nouvelle session.

**23** Quel type d'attaque exploite le mécanisme du handshake TCP pour surcharger un serveur ?

- Une attaque par SYN flood.
- Une attaque DDoS
- Une injection SQL
- Un Man-in-the-Middle

**24** Pourquoi TCP est-il considéré comme un protocole fiable ?

- Parce qu'il utilise des mécanismes de contrôle de flux et de retransmission.
- Parce qu'il chiffre automatiquement les données.
- Parce qu'il est plus rapide qu'UDP.
- Parce qu'il utilise des petits paquets.

**25** Quelle est la principale différence entre un socket TCP et un socket UDP ?

- Un socket TCP établit une connexion avant l'échange des données, tandis qu'un socket UDP n'établit pas de connexion.
- Un socket UDP est plus sécurisé qu'un socket TCP.
- Un socket TCP envoie des données plus rapidement.
- Un socket UDP ne peut pas être utilisé pour la communication entre machines.

**26** Quel est le rôle du champ Checksum dans un segment TCP ?

- Il chiffre les données pour garantir la sécurité.
- Il permet de vérifier l'intégrité des données transmises.
- Il identifie l'expéditeur du segment.
- Il ajuste la taille de la fenêtre TCP.

**27** Lors de l'établissement d'une connexion TCP, quelles sont les trois étapes du handshake ?

- FIN, SYN, ACK
- ACK, SYN, FIN
- SYN, SYN-ACK, ACK
- SYN, RST, ACK

**28** Dans quel cas UDP est-il préférable à TCP ?

- Lorsque la fiabilité est plus importante que la vitesse
- Lorsque la rapidité est prioritaire sur la fiabilité, comme pour le streaming ou les jeux en ligne.
- Lorsqu'il est nécessaire de contrôler le flux de données
- Lorsqu'une connexion sécurisée est requise

**29** Quelle est la longueur maximale d'un numéro de port dans TCP/UDP ?

- 8 bits
- 12 bits
- 16 bits (valeurs de 0 à 65535)
- 32 bits

**30** Quel protocole est utilisé pour transmettre des e-mails de manière fiable sur Internet ?

- TCP (utilisé par SMTP, IMAP et POP3)
- UDP
- ICMP
- FTP

MAGUEMOUN SAMY

## Adressage IPv4

### 1. Adressage IPv4

- IPv4 est le protocole d'adressage le plus utilisé sur Internet.
- Il utilise des adresses de 32 bits (ex : 192.168.1.1).
- Permet l'identification unique des machines sur un réseau.

### 2. Composantes d'une adresse IPv4

- Une adresse IPv4 est composée de :
  - **Partie réseau** : Identifie le réseau auquel appartient l'hôte.
  - **Partie hôte** : Identifie un appareil spécifique sur le réseau.
- Utilisation de masques de sous-réseau pour distinguer ces parties.



Ces deux portions peuvent être combinées pour constituer trois types d'adresse :

**Adresse réseau** : Identifie un réseau spécifique, avec tous les bits de la partie hôte à **0**.

**Adresse de diffusion** : Permet d'envoyer des données à tous les hôtes du réseau, avec tous les bits de la partie hôte à **1**.

**Adresses d'hôte** : Adresses attribuées aux appareils du réseau, avec une combinaison de **0** et **1** dans la partie hôte (sauf tout 0 ou tout 1).

### 3. Le masque de sous-réseau

- Sert à séparer la partie réseau et la partie hôte d'une adresse IP.
- Écrit en notation décimale (ex: 255.255.255.0) ou en notation CIDR (/24).
- Permet la création de sous-réseaux pour une meilleure gestion des adresses IP.

**Exemple 1:**

**Adresse IP donnée** : 10.0.0.1/24

- C'est une adresse IP de classe A, appartenant à une plage d'adresses privées.
- Le suffixe **/24** signifie que les **24 premiers bits** sont réservés à l'identification du réseau, tandis que les **8 derniers bits** sont destinés aux hôtes.

**Type d'adresse** :

- L'adresse **10.0.0.1** est une **adresse d'hôte** car elle ne correspond ni à l'adresse réseau ni à l'adresse de diffusion.

**Adresse réseau** : 10.0.0.0

- Elle est obtenue en mettant **tous les bits de la partie hôte à 0**.
- C'est l'adresse qui identifie le sous-réseau.

**Adresse de diffusion :** 10.0.0.255

- Elle est obtenue en mettant **tous les bits de la partie hôte à 1**.
- Elle permet d'envoyer des messages à tous les hôtes du réseau.

**Nombre maximal d'hôtes :**

- Avec **8 bits dédiés aux hôtes** (car /24 laisse 8 bits pour les hôtes), il y a  $2^8 = 256$  adresses possibles.
- On soustrait **2 adresses** (une pour l'adresse réseau et une pour la diffusion), ce qui donne **254 hôtes utilisables**.

**Masque de sous-réseau :** 255.255.255.0

- Il indique que les **24 premiers bits sont réservés au réseau**, laissant **8 bits pour l'adressage des hôtes**.

**Exemple 2:**

| Classe d'adresse | Plage du premier octet (décimale) | Bits du premier octet (les bits verts ne changent pas) | Parties réseau (N) et hôte (H) de l'adresse | Masque de sous-réseau par défaut (décimal et binaire) | Nombre de réseaux et d'hôtes possibles par réseau                   |
|------------------|-----------------------------------|--------------------------------------------------------|---------------------------------------------|-------------------------------------------------------|---------------------------------------------------------------------|
| A                | 1-127**                           | 00000000-01111111                                      | N.H.H.H                                     | 255.0.0.0                                             | 128 réseaux ( $2^7$ )<br>16 777 214 hôtes par réseau ( $2^{24-2}$ ) |
| B                | 128-191                           | 10000000-10111111                                      | N.N.H.H                                     | 255.255.0.0                                           | 16 384 réseaux ( $2^{14}$ ) 65 534 hôtes par réseau ( $2^{16-2}$ )  |
| C                | 192-223                           | 11000000-11011111                                      | N.N.N.H                                     | 255.255.255.0                                         | 2 097 150 réseaux ( $2^{21}$ ) 254 hôtes par réseau ( $2^{8-2}$ )   |
| D                | 224-239                           | 11100000-11101111                                      | (multidiffusion)                            |                                                       |                                                                     |
| E                | 240-255                           | 11110000-11111111                                      | (expérimental)                              |                                                       |                                                                     |

- Classe d'adresse :** L'IPv4 est divisé en **cinq classes (A, B, C, D et E)**, chacune ayant une utilisation spécifique.
- Plage du premier octet (décimale) :** Définit la plage des valeurs du premier octet qui identifie la classe.
- Bits du premier octet :**
  - Montre les **bits fixes** qui ne changent pas pour identifier la classe.
  - Par exemple, pour la classe A, le premier bit est **toujours 0**.
- Parties réseau (N) et hôte (H) de l'adresse :**
  - Indique comment l'adresse est structurée.
  - Ex : en classe A, seul le **premier octet** est réservé pour le réseau (N), les 3 autres sont pour les hôtes (H).
- Masque de sous-réseau par défaut :**
  - Définit la séparation entre **partie réseau et partie hôte**.

- Ex : **255.0.0.0** pour la classe A signifie que le premier octet est réservé pour le réseau.

## 6. Nombre de réseaux et d'hôtes possibles :

- Indique le **nombre de réseaux et d'hôtes possibles** par réseau en fonction de la classe.
- Par exemple, en classe A, il y a **128 réseaux** possibles, avec **16 777 214 hôtes** par réseau.

## Explication des classes :

### 1. Classe A (1-127) :

- **Grandes organisations et fournisseurs d'accès.**
- Peu de réseaux, mais **beaucoup d'hôtes**.

### 2. Classe B (128-191) :

- Utilisée par les **entreprises de taille moyenne**.
- Plus de réseaux que la classe A, mais moins d'hôtes.

### 3. Classe C (192-223) :

- Destinée aux **petites entreprises et réseaux locaux**.
- Beaucoup de réseaux, mais peu d'hôtes par réseau.

### 4. Classe D (224-239) :

- Réservée à la **multidiffusion (multicast)**.
- Pas utilisée pour adresser des hôtes.

### 5. Classe E (240-255) :

- **Expérimentale**, non utilisée pour un usage classique.

## 4. Limites de l'adressage par classe

- Gaspillage d'adresses IP dû à la rigidité des classes.
- Solution : **Adressage sans classe (CIDR)** qui permet une meilleure gestion.

## 5. Adresses réservées

**Adresses privées** : Réservées aux réseaux locaux, non routables sur Internet (ex: 192.168.x.x, 10.x.x.x, 172.16.x.x).

**Route par défaut (0.0.0.0)** : Utilisée lorsqu'aucune route spécifique n'est définie dans une table de routage.

**Adresse de bouclage (127.0.0.1)** : Permet de tester la connectivité locale sans passer par le réseau.

**Adresses locales-liens (169.254.x.x)** : Assignées automatiquement par un hôte en cas d'absence de DHCP.

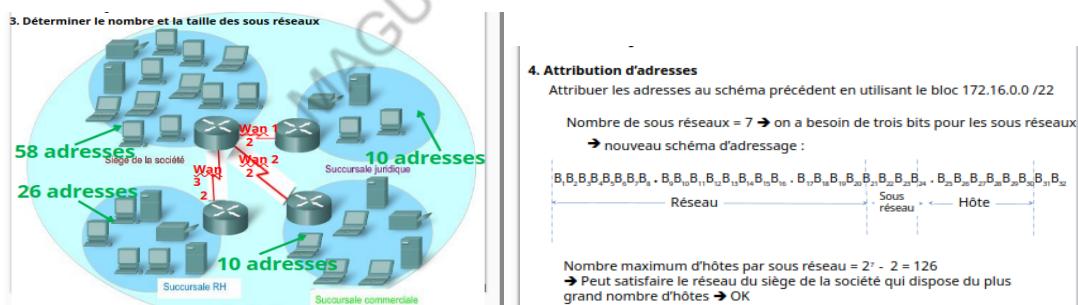
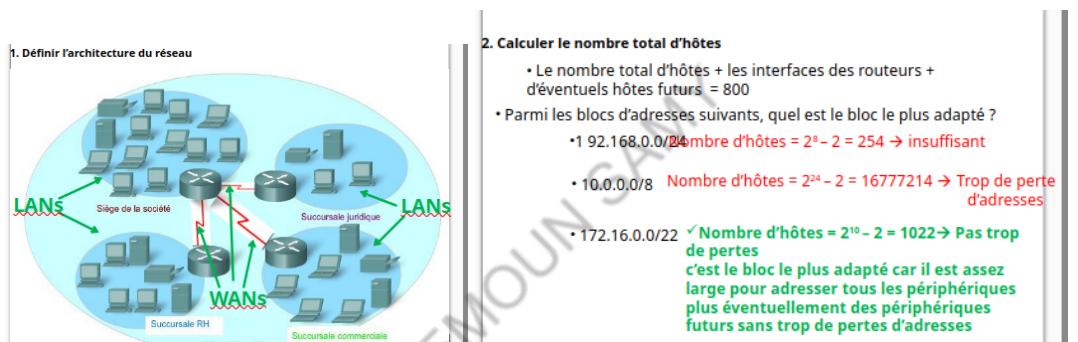
**Adresses TEST-NET (192.0.2.x)** : Utilisées uniquement pour la documentation et l'enseignement, sans routage réel.

## 6. Conception d'un plan d'adressage

- Un bloc d'adresses peut être divisé en plusieurs sous-réseaux.
  - Les sous-réseaux sont connectés via des routeurs.
  - Chaque interface de routeur a une adresse réseau unique.
  - Tous les appareils d'un sous-réseau partagent la même adresse réseau.
  - On crée des sous-réseaux en empruntant des bits de la partie hôte.
  - Plus de bits empruntés → plus de sous-réseaux disponibles.
  - Chaque bit emprunté double le nombre de sous-réseaux (1 bit → 2, 2 bits → 4, etc.).

## **7. Étapes de création de sous-réseaux (Schéma standard)**

1. **Définir l'architecture** : Nombre total d'hôtes et de sous-réseaux nécessaires.
  2. **Calculer le nombre total d'hôtes** : Utilisation de la formule  $2^n - 2$ .
  3. **Déterminer le nombre et la taille des sous-réseaux** : Basé sur les besoins de chaque segment de réseau.
  4. **Attribution d'adresses** : Assigner des plages d'adresses aux différents sous-réseaux.



| 4. Attribution d'adresses |                 |                             |                             |                      |                       |
|---------------------------|-----------------|-----------------------------|-----------------------------|----------------------|-----------------------|
| Sous réseau               | Adresse réseau  | Première adresse utilisable | Dernière adresse utilisable | Adresse de diffusion | Masque de sous réseau |
| Siège de la société       | 172.16.0.0/ 25  | 172.16.0.1                  | 172.16.0.126                | 172.16.0.127         | 255.255.255.128       |
| Succursale RH             | 172.16.0.128/25 | 172.16.0.129                | 172.16.0.254                | 172.16.0.255         | 255.255.255.128       |
| Succursale juridique      | 172.16.1.0/25   | 172.16.1.1                  | 172.16.1.126                | 172.16.1.127         | 255.255.255.128       |
| Succursale commerciale    | 172.16.1.128/25 | 172.16.1.129                | 172.16.1.254                | 172.16.1.255         | 255.255.255.128       |
| WAN 1                     | 172.16.2.0/25   | 172.16.2.1                  | 172.16.2.126                | 172.16.2.127         | 255.255.255.128       |
| WAN 2                     | 172.16.2.128/25 | 172.16.2.129                | 172.16.2.254                | 172.16.2.255         | 255.255.255.128       |
| WAN 3                     | 172.16.3.0/25   | 172.16.3.1                  | 172.16.3.126                | 172.16.3.127         | 255.255.255.128       |
| Libre                     | 172.16.3.128/25 | 172.16.3.129                | 172.16.3.254                | 172.16.3.255         | 255.255.255.128       |

## **Explication des étapes de conception du réseau**

## 1. Architecture du réseau

- **LANs** : Réseaux locaux pour le siège de la société et les succursales (juridique, RH, commerciale).
- **WANs** : Réseaux étendus reliant les différentes succursales.

## 2. Calcul du nombre total d'hôtes

- Besoin : 800 hôtes (incluant les interfaces des routeurs et une marge pour de futurs ajouts).
- Choix du bloc d'adresses :
  - **192.168.0.0/20** : Trop petit (254 hôtes).
  - **10.0.0.0/8** : Trop grand (16 millions d'hôtes, gaspillage).
  - **172.16.0.0/22** : Idéal (1022 hôtes, suffisant sans gaspillage).

## 3. Détermination des sous-réseaux

- **Siège de la société** : 58 adresses.
- **Succursale RH** : 26 adresses.
- **Succursale juridique/commerciale** : 10 adresses chacune.

## 4. Attribution des adresses

- Utilisation du bloc **172.16.0.0/22** divisé en sous-réseaux /25 (128 hôtes par sous-réseau).
- Exemples :
  - **Siège** : 172.16.0.0/25 (adresses de 172.16.0.1 à 172.16.0.126).
  - **Succursale RH** : 172.16.0.128/25 (adresses de 172.16.0.129 à 172.16.0.254).
- Les WANs et sous-réseaux libres sont également alloués avec des plages similaires.

## 8. Inconvénients du schéma standard

- Manque de flexibilité, gaspillage d'adresses dans certains sous-réseaux.
- D'où la nécessité du **VLSM**.

## 9. Le VLSM (Variable Length Subnet Masking)

- Permet d'attribuer des masques de sous-réseau de différentes tailles selon les besoins.
- Optimise l'utilisation des adresses IP.

## 10. Procédure de création de sous-réseaux en VLSM

1/Découper d'abord la plage en sous-réseaux selon le besoin le plus grand.

2/Réserver un sous-réseau pour ce besoin.

3/Découper une nouvelle plage pour le besoin suivant le plus important.

4/Réserver un sous-réseau pour ce besoin.

5/Répéter le processus jusqu'à couvrir tous les besoins.



- **WANs (liens point-à-point) :**
  - 3 liens WAN (2 adresses chacun → /30 par WAN)

## 2. Stratégie VLSM optimale

1. Allouer d'abord les grands sous-réseaux (LANs).
2. Puis découper les petits blocs pour les WANs.
3. **Bloc de départ : 172.16.0.0/22** (1022 adresses disponibles).

## 3. Découpage détaillé

### Étape 1 : Allocation des LANs

- **Siège social (58) → 172.16.0.0/26**
  - Plage : 172.16.0.0 – 172.16.0.63
  - Utilisable : 172.16.0.1 – 172.16.0.62
- **Succursale RH (26) → 172.16.0.64/27**
  - Plage : 172.16.0.64 – 172.16.0.95
  - Utilisable : 172.16.0.65 – 172.16.0.94
- **Succursale juridique (10) → 172.16.0.96/28**
  - Plage : 172.16.0.96 – 172.16.0.111
  - Utilisable : 172.16.0.97 – 172.16.0.110
- **Succursale commerciale (10) → 172.16.0.112/28**
  - Plage : 172.16.0.112 – 172.16.0.127
  - Utilisable : 172.16.0.113 – 172.16.0.126

### Étape 2 : Allocation des WANs (/30 par lien)

- Chaque lien WAN nécessite 2 adresses (1 pour chaque routeur).
- Plages WANs (dans l'espace libre restant) :
  - **WAN 1 : 172.16.0.128/30**
    - Adresses : 172.16.0.129 (Routeur A) et 172.16.0.130 (Routeur B).
    - Broadcast : 172.16.0.131.
  - **WAN 2 : 172.16.0.132/30**
    - Adresses : 172.16.0.133 (Routeur A) et 172.16.0.134 (Routeur B).
  - **WAN 3 : 172.16.0.136/30**
    - Adresses : 172.16.0.137 (Routeur A) et 172.16.0.138 (Routeur B).

## 4. Plages libres restantes

- **172.16.0.140/30** → Pour un 4ème lien WAN si besoin.
- **172.16.0.144/28** → 14 adresses (pour petites extensions).
- **172.16.0.160/27** → **172.16.1.0/24** → Réservé pour futures expansions.

### Tableau récapitulatif final

| <b>Sous-réseau</b>            | <b>Plage</b>    | <b>Masque</b>       | <b>Adresses utilisables</b> |
|-------------------------------|-----------------|---------------------|-----------------------------|
| <b>Siège social</b>           | 172.16.0.0/26   | 255.255.255.19<br>2 | 172.16.0.1 – 172.16.0.62    |
| <b>Succursale RH</b>          | 172.16.0.64/27  | 255.255.255.22<br>4 | 172.16.0.65 – 172.16.0.94   |
| <b>Succursale juridique</b>   | 172.16.0.96/28  | 255.255.255.24<br>0 | 172.16.0.97 – 172.16.0.110  |
| <b>Succursale commerciale</b> | 172.16.0.112/28 | 255.255.255.24<br>0 | 172.16.0.113 – 172.16.0.126 |
| <b>WAN 1</b>                  | 172.16.0.128/30 | 255.255.255.25<br>2 | 172.16.0.129 – 172.16.0.130 |
| <b>WAN 2</b>                  | 172.16.0.132/30 | 255.255.255.25<br>2 | 172.16.0.133 – 172.16.0.134 |
| <b>WAN 3</b>                  | 172.16.0.136/30 | 255.255.255.25<br>2 | 172.16.0.137 – 172.16.0.138 |
| <b>Libre (WAN 4)</b>          | 172.16.0.140/30 | 255.255.255.25<br>2 | 172.16.0.141 – 172.16.0.142 |

|                           |                 |                |                             |
|---------------------------|-----------------|----------------|-----------------------------|
| <b>Libre (Extensions)</b> | 172.16.0.144/28 | 255.255.255.24 | 172.16.0.145 – 172.16.0.158 |
|                           |                 | 0              |                             |

## Pourquoi cette solution ?

- Optimisation maximale** : Aucune adresse gaspillée (ex: les WANs utilisent des /30, les petits LANs des /28).
- Extensibilité** : Les plages libres permettent d'ajouter 1 WAN supplémentaire et des petits LANs.
- Clarté** : Découpage progressif sans chevauchement.

## 11. Dépannage de la couche réseau

- Utilisation d'outils et de protocoles pour tester et diagnostiquer les problèmes réseau.

### Protocole ICMP

- Utilisé pour le diagnostic réseau (ex: erreurs, indisponibilité).
- Permet l'échange de messages entre équipements réseau.

| Le protocole ICMP (Internet Control Messaging Protocol). |                               |                                                                               |                                             |                        |      |           |    |                               |
|----------------------------------------------------------|-------------------------------|-------------------------------------------------------------------------------|---------------------------------------------|------------------------|------|-----------|----|-------------------------------|
| Ethernet Header (Layer 2)                                |                               |                                                                               | IP Header (Layer 3)                         | ICMP Message (Layer 3) |      |           |    |                               |
| Ethernet Destination Address (MAC)                       | Ethernet Source Address (MAC) | Frame Type                                                                    | Source IP Add. Dest. IP Add. Protocol field | Type                   | Code | Check-sum | ID | Seq. Num. Data Ether. Tr. FCS |
| <b>Quelques messages ICMP fréquents</b>                  |                               |                                                                               |                                             |                        |      |           |    |                               |
| Type                                                     | Code                          | Description                                                                   |                                             |                        |      |           |    |                               |
| 0. Echo Reply                                            | 0                             | Réponse d'écho (utilisé par ping)                                             |                                             |                        |      |           |    |                               |
| 3. Destination Inaccessible                              | 0<br>1<br>2<br>3              | Réseau Inaccessible<br>Hôte Inaccessible<br>Protocole Inaccessible<br>... etc |                                             |                        |      |           |    |                               |
| 8. Echo Request                                          | 0                             | Demande d'Echo                                                                |                                             |                        |      |           |    |                               |
| 11. Time Exceeded                                        | 0                             | Expiration de délais pour un paquet (TTL = 0)                                 |                                             |                        |      |           |    |                               |
| ... etc                                                  |                               |                                                                               |                                             |                        |      |           |    |                               |

### Commande Ping

- Vérifie la connectivité entre deux hôtes.
- Fonctionne avec deux types de messages ICMP :
  - Echo Request** : Demande envoyée.

#### Echo Request

- L'expéditeur de ping transmet le message ICMP, "Echo Request"
  - Type = 8
  - Code = 0

| Ethernet Header (Layer 2)          |                               |            | IP Header (Layer 3)           | ICMP Message - Echo Request (Layer 3) |           |           |    |           | Ether. Tr. |     |
|------------------------------------|-------------------------------|------------|-------------------------------|---------------------------------------|-----------|-----------|----|-----------|------------|-----|
| Ethernet Destination Address (MAC) | Ethernet Source Address (MAC) | Frame Type | Source IP Add.<br>172.30.1.20 | Type<br>8                             | Code<br>0 | Check-sum | ID | Seq. Num. | Data       | FCS |
|                                    |                               |            | Dest. IP Add.<br>172.30.1.25  |                                       |           |           |    |           |            |     |

- **Echo Reply** : Réponse reçue.

#### **Echo Reply**

- Le destinataire de ping, reçoit le message ICMP, "Echo Request"
- Et retourne le message ICMP, "Echo Reply"
  - Type = 0
  - Code = 0

| Ethernet Header<br>(Layer 2)                |                                        |               | IP Header<br>(Layer 3)                                                                  | ICMP Message - Echo Reply<br>(Layer 3) |           |               |    |              |      | Ether.<br>Tr. |
|---------------------------------------------|----------------------------------------|---------------|-----------------------------------------------------------------------------------------|----------------------------------------|-----------|---------------|----|--------------|------|---------------|
| Ethernet<br>Destination<br>Address<br>(MAC) | Ethernet<br>Source<br>Address<br>(MAC) | Frame<br>Type | Source IP<br>Add.<br>172.30.1.25<br>Dest. IP Add.<br>172.30.1.20<br>Protocol field<br>8 | Type<br>0                              | Code<br>0 | Check-<br>sum | ID | Seq.<br>Num. | Data | FCS           |
|                                             |                                        |               |                                                                                         |                                        |           |               |    |              |      |               |

### Utilisation de la commande Ping

- Test de connectivité avec une autre machine.
- Détection de latence et de perte de paquets.

### Commande Traceroute (Tracert)

- Affiche le chemin emprunté par les paquets pour atteindre une destination.
- Permet d'identifier où se situent les problèmes de connexion.

QCM

**1** Regardez la commande ci-dessous et son résultat. Un administrateur réseau teste la configuration sur un ordinateur hôte. Quel est le type d'adresse correspondant à 127.0.0.1 ?

- Une adresse de bouclage  
 Une adresse locale-lien  
 Une adresse publique  
 Une adresse de route par défaut

**2** À quoi correspond la partie de l'adresse IP représentant le préfixe ?

- L'adresse réseau  
 L'adresse de diffusion (broadcast)  
 L'adresse de l'hôte  
 L'adresse de monodiffusion (unicast)

**3** Combien de chiffres binaires (bits) composent une adresse IPv6 ?

- 128 bits  
 64 bits  
 48 bits  
 32 bits

**4** Parmi les éléments suivants, indiquez les protocoles associés à la couche 4 du modèle OSI. (*Choisissez deux réponses.*)

- TCP
- UDP
- ICMP
- ARP

**5** Quelle commande permet de tester la connectivité entre deux équipements réseau ?

- ping
- tracert
- nslookup
- ipconfig

**6** Quelle est la plage d'adresses IP privées pour la classe A ?

- 10.0.0.0 à 10.255.255.255
- 192.168.0.0 à 192.168.255.255
- 172.16.0.0 à 172.31.255.255
- 169.254.0.0 à 169.254.255.255

**7** Quelle adresse IP est utilisée pour le routage par défaut ?

- 0.0.0.0
- 255.255.255.255
- 127.0.0.1
- 224.0.0.1

**8** Quelle adresse IPv4 est une adresse de diffusion (broadcast) ?

- 255.255.255.255
- 192.168.1.1
- 172.16.0.1
- 10.0.0.1

**9** Quel protocole est utilisé pour résoudre une adresse IP en adresse MAC ?

- ARP
- DHCP
- DNS
- ICMP

**10** Quel est le rôle du protocole DHCP ?

Attribuer dynamiquement des adresses IP

Résoudre les noms de domaine

Tester la connectivité réseau

Convertir une adresse IPv4 en IPv6

**11** Quelle est la longueur d'un masque de sous-réseau en notation CIDR pour un réseau de classe C standard ?

/24

/16

/8

/32

**12** Quelle commande affiche la table de routage d'un ordinateur sous Windows ?

route print

ipconfig

netstat

tracert

**13** Quelle adresse IPv6 est réservée pour le bouclage ?

::1

fe80::1

2001::1

ff02::1

**14** Quelle est la taille d'une adresse MAC ?

48 bits

32 bits

64 bits

128 bits

**15** Quel protocole est utilisé pour transférer des fichiers entre un client et un serveur ?

FTP

SNMP

SMTP

IMAP

**16) Quel protocole est utilisé pour la résolution de noms de domaine ?**

- DNS
- ARP
- DHCP
- ICMP

**17) Quelle commande permet d'afficher la configuration IP sous Linux ?**

- ifconfig
- ipconfig
- netstat
- nslookup

**18) Quel type d'adresse IPv6 commence par "fe80::" ?**

- Adresse locale-lien
- Adresse globale
- Adresse de multicast
- Adresse de loopback

**19) Quelle est la plage d'adresses IP privées de classe B ?**

- 172.16.0.0 à 172.31.255.255
- 10.0.0.0 à 10.255.255.255
- 192.168.0.0 à 192.168.255.255
- 169.254.0.0 à 169.254.255.255

**20) Quelle adresse IPv4 est une adresse de multicast ?**

- 224.0.0.1
- 192.168.1.1
- 172.16.0.1
- 10.0.0.1

**21) Quelle est la commande utilisée pour afficher les connexions réseau actives sous Windows ?**

- netstat
- ipconfig
- nslookup
- ping

**22** Quel protocole est utilisé pour envoyer des e-mails ?

- SMTP
- POP3
- IMAP
- HTTP

**23** Quel protocole permet de récupérer des e-mails depuis un serveur ?

- IMAP
- SMTP
- SNMP
- ICMP

**24** Quel protocole est utilisé pour surveiller les équipements réseau ?

- SNMP
- FTP
- DHCP
- NTP

**25** Quelle est la fonction principale du protocole ICMP ?

- Envoyer des messages d'erreur et de diagnostic
- Gérer le routage
- Convertir les adresses IP
- Assigner des adresses dynamiquement

**26** Quel est le rôle du protocole HTTPS ?

- Sécuriser les communications web
- Attribuer des adresses IP
- Convertir les noms de domaine en adresses IP
- Surveiller les équipements réseau

**27** Quel protocole est utilisé pour synchroniser l'heure des équipements réseau ?

- NTP
- SNMP
- IMAP
- DHCP

**28** Quelle commande permet de tester la résolution DNS d'un nom de domaine ?

- nslookup
- ping
- tracert
- netstat

**2) Quel est le rôle du protocole Telnet ?**

- Permettre l'accès distant à un équipement

- Envoyer des fichiers
- Surveiller le réseau
- Chiffrer les communications

**3) Quelle est la principale différence entre IPv4 et IPv6 ?**

- IPv6 utilise des adresses de 128 bits, alors qu'IPv4 utilise des adresses de 32 bits

- IPv4 prend en charge plus d'adresses que IPv6
- IPv6 est plus rapide que IPv4
- IPv4 est sécurisé par défaut, contrairement à IPv6

MAGUEMOUN SAMY