Couche transport

# TCP et UDP

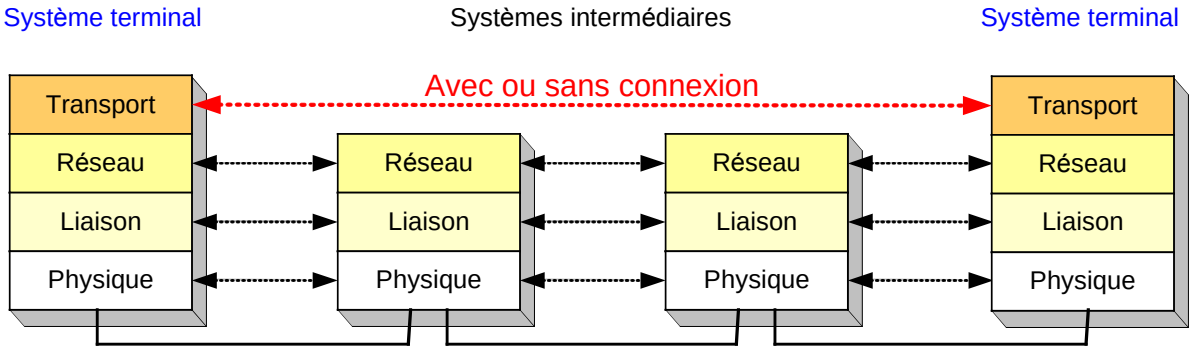
# Objectifs

- Savoir différencier TCP et UDP au niveau de leurs fonctionnalités et de leur utilisation
- Pouvoir expliquer le système de numéros de ports utilisé par TCP et UDP
- Pouvoir expliquer ce qu'est le port scanning et comment cette technique est utilisée avec TCP et UDP

# 4. Couche transport

## Transmission de bout en bout, entre les terminaux

- Optimiser le transport des données
  - Ne pas surcharger le récepteur ou le réseau
  - Découper les données de la couche supérieure en unités plus petites
- Service fiable
  - Avec établissement d'une connexion
  - S'assurer que tous les paquets arrivent correctement au destinataire
- Service non fiable
  - Sans connexion, plus simple
  - Ne retransmet pas les paquets perdus



# Protocoles couche transport

- 2 protocoles sont principalement utilisés par la couche transport:
  - TCP, qui offre un service fiable
  - UDP, qui offre un service non-fiable
- Ces deux protocoles proposent des fonctionnalités différentes et sont utilisés dans des situations différentes
- La couche transport utilise des numéros de ports comme «adresses» pour identifier les différentes applications
- UDP et TCP utilisent des numéros de ports et peuvent utiliser les mêmes

# Numéros de ports

- Il y a 65535 ports qui peuvent être utilisés en même temps par TCP et UDP
- Les ports 1 à 1023 sont généralement utilisés pour des applications définies:
  - SMTP (mail): port 25 TCP
  - DNS (traduit nom de domaine en adresse IP): 53 UDP
  - HTTP: 80
  - …
- Les ports 1024 à 65535 peuvent être utilisés pour n'importe quelle application

# UDP (User Datagram Protocol)

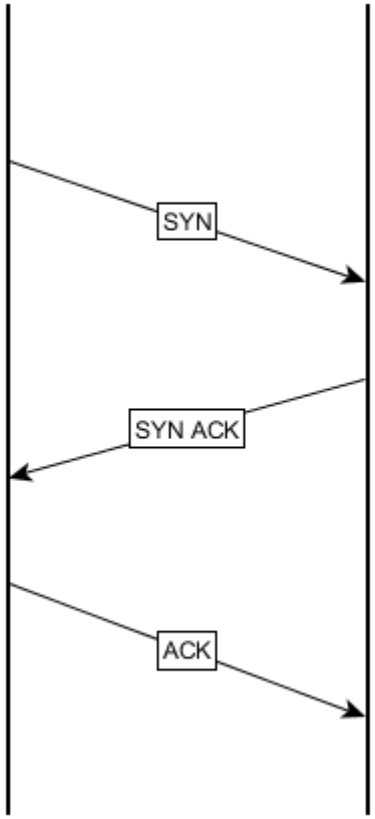
- Fonctionnalités:
  - Adressage d'applications à l'aide de numéros de port
  - Contrôle d'erreur optionnel
  - Transmission non fiable:
    - Sans connexion
    - Sans acquittement ou retransmission
    - Sans contrôle du débit
- Utilisé pour:
  - Les transmission multimédia (tolèrent quelques pertes)
  - Les transmissions multicast
  - Les échanges courts (comme DNS)

# TCP (Transmission Control Protocol)

- Fonctionnalités:
  - Transmission fiable de bout en bout:
    - Numéros de séquence
    - Acquittements
    - Retransmission
  - Etablissement et terminaison de connexions
  - Régulation du débit:
    - Contrôle de flux: adaptation de la vitesse au récepteur
    - Contrôle de congestion: adaptation de la vitesse au réseau
- Utilisé pour:
  - Les cas où la fiabilité est requise (la plupart des cas)

# Etablissement de connexions TCP

- Three way handshake (connexion en trois temps)



# Port scanning

- Il y a 3 états possibles pour un port:
  - Ouvert: une application tourne sur ce port et accepte les connexions TCP ou les datagrammes UDP
  - Fermé: aucune application ne tourne sur ce port
  - Filtré: état inconnu, le système ne retourne pas d'information
- Avec TCP, il suffit de faire un three way handshake sur tous les ports pour vérifier si ils sont ouverts:
  - Ouvert: réponse SYN/ACK
  - Fermé: réponse RST
  - Filtré: pas de réponse

# Port scanning

- UDP: Pas de connexion, scan plus difficile
- Nécessite de créer des datagrammes spécifiques en fonction de l'application visée
- Si la réponse attendue est la bonne le port est ouvert
- Beaucoup plus long et difficile que le scan TCP

- De manière générale le port scanning permet d'obtenir beaucoup d'informations sur un système
- Connaitre les applications présentes peut permettre de savoir comment l'attaquer