



Département : ITG

Filière : ARI - 2<sup>ème</sup> année - S3

Année universitaire: 2023-2024

Module: Sys. & Réseaux Informatiques Avancés  
(M11)

Elément: Systèmes d'exploitation avancés (E2)

Support de cours

# SYSTÈMES D'EXPLOITATION AVANCÉS



## CHAPITRE VI: GESTION DE RÉSEAUX

# Plan

- ☐ **INTRODUCTION**
- ☐ **CONFIGURATION RÉSEAU**
- ☐ **GESTION DES CONNEXIONS**
- ☐ **SÉCURITÉ RÉSEAU**
- ☐ **GESTION DE LA BANDE PASSANTE**
- ☐ **DIAGNOSTIC ET DÉPANNAGE**
- ☐ **GESTION DES PÉRIPHÉRIQUES RÉSEAU**

# Introduction

Dans les **systèmes d'exploitation**, la **gestion de réseaux** désigne les mécanismes et les outils intégrés dans un système d'exploitation, permettant de superviser et d'améliorer les opérations réseau d'un ordinateur ou d'un ensemble d'ordinateurs.

→ Ces fonctionnalités sont cruciales pour faciliter la communication et le partage de données entre les diverses machines d'un réseau informatique.



# Introduction

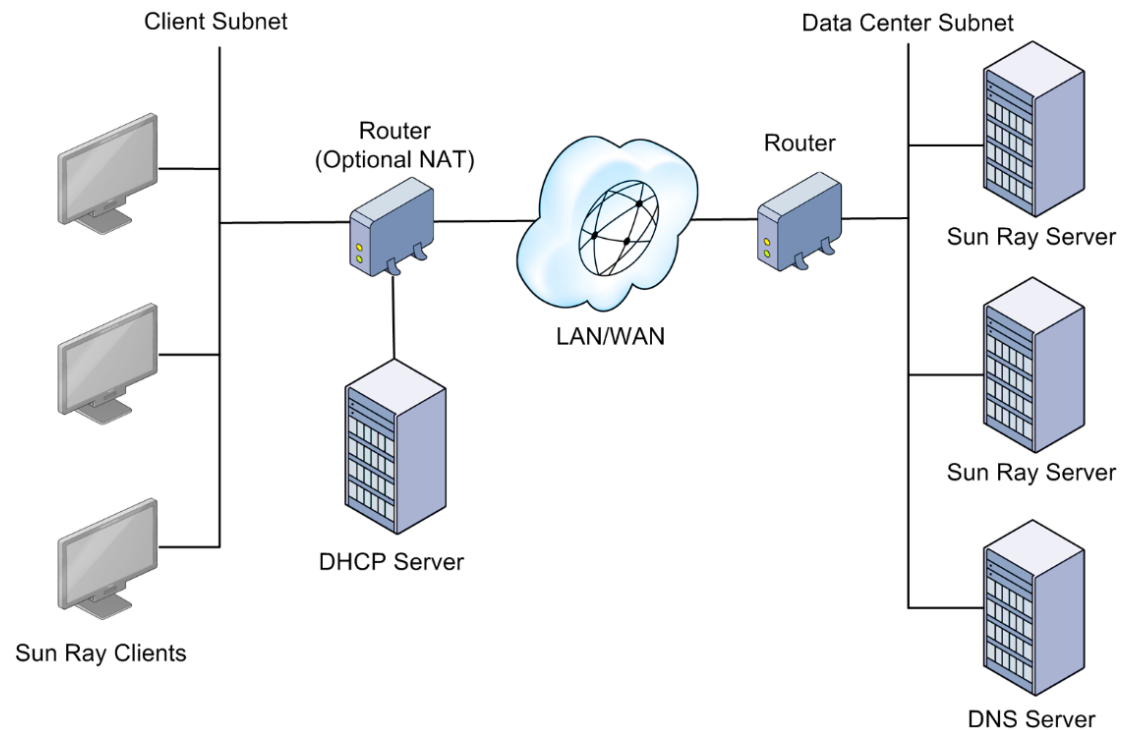
La **gestion de réseaux** dans un système d'exploitation peut inclure diverses tâches et fonctionnalités telles que :

- ☐ Configuration réseau
- ☐ Gestion des connexions
- ☐ Sécurité réseau
- ☐ Gestion de la bande passante
- ☐ Diagnostic et dépannage
- ☐ Gestion des périphériques réseau

Ces fonctionnalités peuvent varier en fonction du système d'exploitation spécifique utilisé, mais l'objectif principal de la gestion de réseaux dans un système d'exploitation est d'assurer une **communication** réseau **fiable**, **sécurisée** et **efficace** entre les ordinateurs et les périphériques d'un réseau.

# Configuration réseau

- La configuration réseau dans un système d'exploitation permet aux utilisateurs de spécifier les paramètres réseau de leur ordinateur. Cela inclut **l'adresse IP** (Internet Protocol), le **masque** de sous-réseau, la **passerelle** par défaut et les **serveurs DNS** (Domain Name System).
- Ces paramètres sont essentiels pour permettre à l'ordinateur de communiquer efficacement avec d'autres appareils sur le réseau.

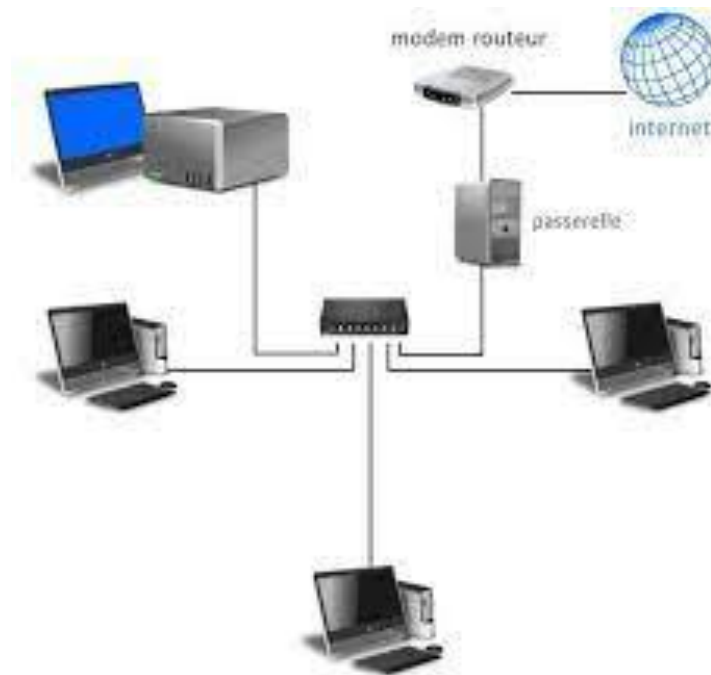


# Configuration réseau

- **Adresse IP** (Internet Protocol) : Il s'agit d'un identifiant unique attribué à chaque appareil sur un réseau. Cette adresse permet aux appareils de se reconnaître et de communiquer entre eux sur Internet ou dans un réseau local.
- **Masque de sous-réseau** : Ce paramètre détermine quelle partie de l'adresse IP identifie le réseau et quelle partie identifie l'appareil spécifique. Il permet de subdiviser les réseaux en sous-réseaux plus petits, facilitant ainsi une gestion plus efficace des adresses IP.
- **Passerelle par défaut** : Il s'agit de l'adresse IP du routeur ou du périphérique réseau qui permet à l'ordinateur de se connecter à des réseaux externes, tels qu'Internet. Toutes les données qui ne sont pas destinées au réseau local sont dirigées vers cette passerelle par défaut.
- **Serveurs DNS** (Domain Name System) : Ces serveurs traduisent les noms de domaine en adresses IP. Lorsque vous saisissez un nom de domaine (comme `www.exemple.com`) dans votre navigateur, un serveur DNS est utilisé pour trouver l'adresse IP correspondante. Cela permet à votre ordinateur de localiser le serveur web approprié et d'établir la connexion.

# Gestion des connexions

- Surveille les connexions réseau actives sur l'ordinateur.
- Permet aux utilisateurs de visualiser les connexions établies.
- Offre la possibilité de les modifier ou de les interrompre si nécessaire.
- Inclut les connexions filaires telles qu'Ethernet et les connexions sans fil telles que Wi-Fi.



# Sécurité réseau

Les systèmes d'exploitation intègrent des fonctionnalités de sécurité essentielles pour protéger les réseaux informatiques telles que :

- Le **pare-feu**
- Les **outils de détection des intrusions**





## ❑ Pare-feu

- Contrôle le trafic entrant et sortant du réseau.
- Permet aux administrateurs de définir des règles pour autoriser ou bloquer certains types de connexions.
- Protège contre les accès non autorisés et les attaques provenant de l'extérieur du réseau.

## ❑ Outils de détection des intrusions

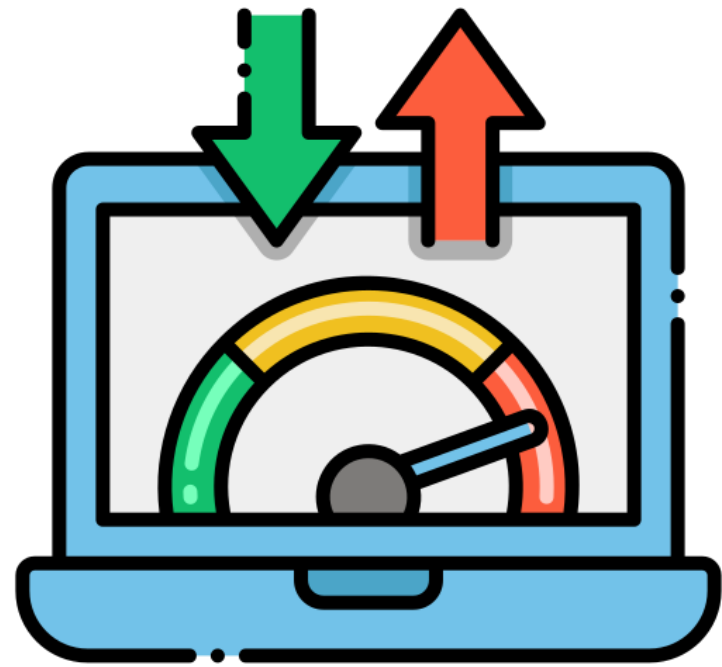
- Identifient et préviennent les activités suspectes sur le réseau.
- Surveillent les schémas de trafic et les comportements inhabituels.
- Alertent les administrateurs en cas de tentative d'intrusion ou de comportement anormal.
- Aident à prévenir les attaques telles que les scans de ports, les attaques par force brute et les tentatives d'accès non autorisé.

Ces fonctionnalités de sécurité garantissent l'intégrité, la confidentialité et la disponibilité des données en protégeant le réseau contre les menaces potentielles.

# Gestion de la bande passante

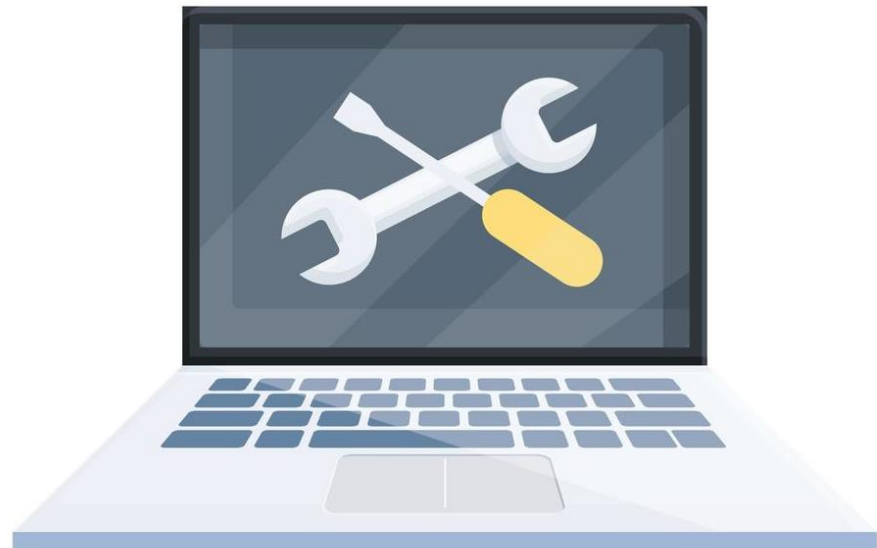
## → Gestion de la bande passante

- Certains systèmes d'exploitation proposent des outils de gestion de la bande passante.
- Ces outils permettent de prioriser certains types de trafic réseau par rapport à d'autres.
- Garantit que les applications critiques bénéficient d'une bande passante suffisante pour fonctionner correctement.



# Diagnostic et dépannage

- Les outils de diagnostic intégrés identifient les problèmes de réseau.
- Testent la connectivité avec d'autres appareils.
- Mesurent la latence pour évaluer la réactivité du réseau.
- Fournissent des informations sur les erreurs de connexion.
- Ces outils sont essentiels pour résoudre les problèmes de réseau, assurant une performance optimale et une connectivité fiable.



# Gestion des périphériques réseau

- Permet de gérer les cartes réseau, les routeurs et les commutateurs.
- Les utilisateurs peuvent configurer ces périphériques selon les besoins du réseau.
- Offre la possibilité de mettre à jour les pilotes pour assurer la compatibilité et les performances optimales.
- Permet d'effectuer d'autres tâches de maintenance liées aux composants matériels du réseau.
- Cette fonctionnalité garantit le bon fonctionnement et la sécurité des périphériques réseau, assurant ainsi une connectivité stable et fiable.

