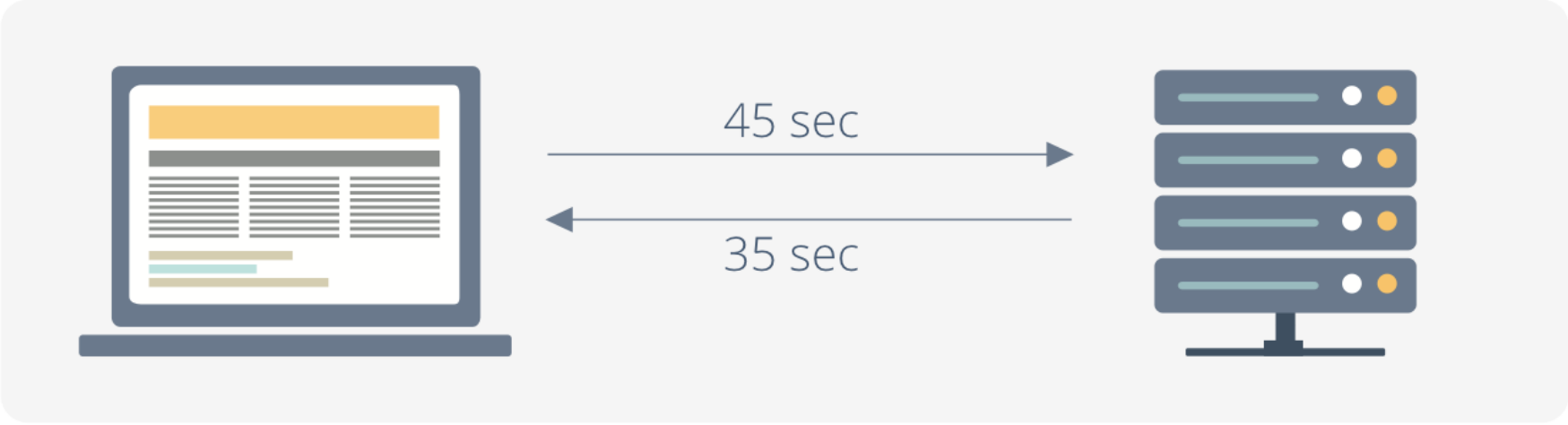
Introduction aux outils de diagnostic réseau

Les commandes linux réseau de base

- Les commandes Linux essentielles pour collecter des informations réseau et tester les connexions réseau serons utilisées. Ces compétences sont cruciales pour les administrateurs de systèmes et les professionnels du réseau afin de diagnostiquer et résoudre les problèmes réseau
- Ces commandes permettent de **visualiser la configuration IP**, de **tester la connectivité**, de **contrôler les routes**, et d'**analyser les connexions actives**. Elles sont indispensables pour les administrateurs systèmes et pour tout utilisateur qui souhaite comprendre ou dépanner son réseau

ping

- ping est probablement l’outil de diagnostic réseau le plus basique. Il utilise des paquets ICMP pour tester la connectivité entre l’hôte local et un hôte distant.
- **Usage typique** : Pour vérifier si un hôte spécifique est accessible.
- **Exemple** :
- ping google.com
- Cela enverra des paquets ICMP à google.com et affichera les temps de réponse.



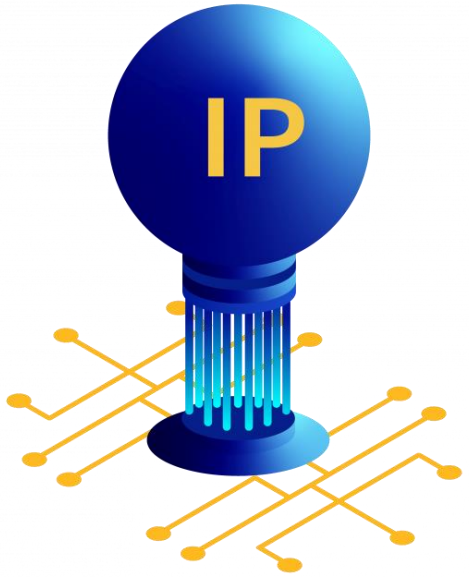
ifconfig (Interface Configuration)

- La commande ifconfig est utilisé pour configurer, gérer et interroger les paramètres des interfaces réseau.
- **Usage typique** : Pour afficher ou configurer les paramètres de l’interface réseau.

- Affiche les détails des interfaces dont l’adresse IP, le masque de sous-réseau et l’état.

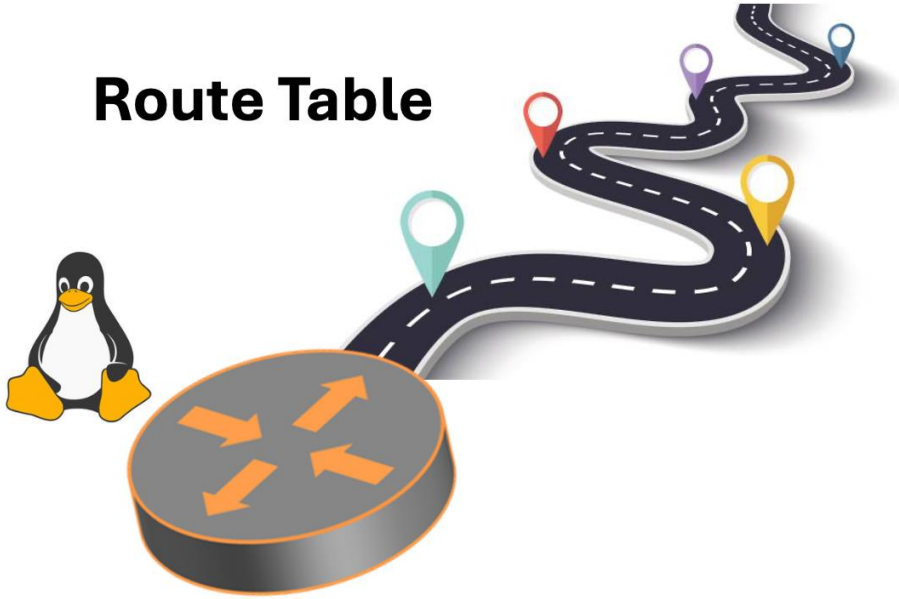
ip

- La commande ip est une alternative à ifconfig. Elle sert à afficher et à manipuler des routes, des adresses réseau, des interfaces, etc.
- **Usage typique** : Pour gérer les adresses IP et les routes.
- Affiche toutes les interfaces réseau et leurs adresses IP.



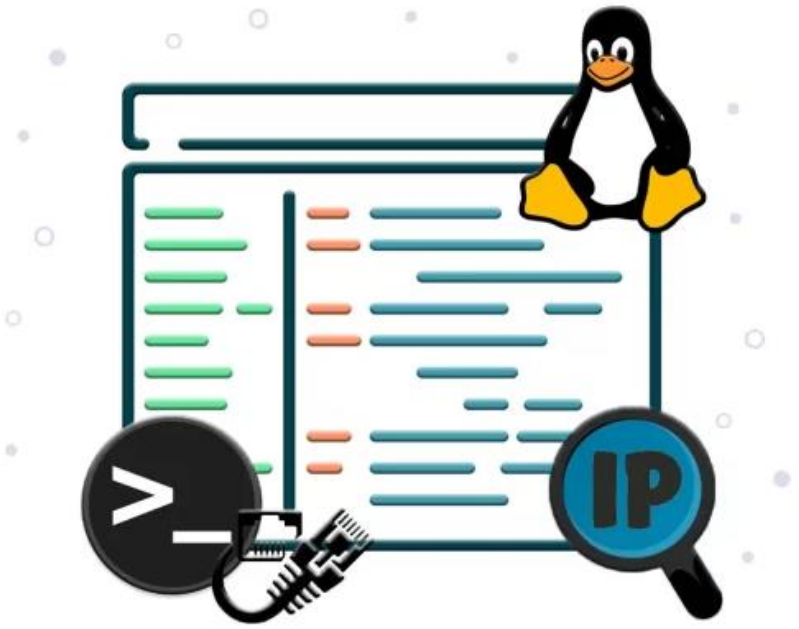
route

- La commande route est utilisée pour afficher et manipuler la table de routage IP du noyau.
- **Usage typique** : Pour afficher ou modifier les routes de réseau.
- Affiche la table de routage sans résoudre les noms.



traceroute

- La commande traceroute trace la route que prennent les paquets pour atteindre une destination réseau.
- **Usage typique** :
- Pour diagnostiquer les problèmes de routage et les délais.
- Exemple : Affiche le chemin emprunté par les paquets pour atteindre google.com.



nslookup (Name Server Lookup)

- La commande nslookup est un outil utilisé pour interroger les serveurs DNS afin d’obtenir des informations sur les enregistrements DNS pour un domaine ou une adresse IP spécifique.
- **Usage typique** : C’est un outil essentiel pour le diagnostic des problèmes de DNS.

arp (Address Resolution Protocol)

- La commande arp est un outil utilisé sous Linux pour afficher et manipuler la table ARP, qui associe les adresses IP aux adresses MAC des machines présentes sur le réseau local.
- **Usage typique** :
- Vérifier les correspondances IP ↔ MAC avec arp -n.
- Diagnostiquer des problèmes de communication réseau en observant si une machine est correctement résolue au niveau de la couche liaison.
- Détecter des anomalies comme des doublons ou des usurpations d’adresse (ARP spoofing).

ip addr (IP Address Management)

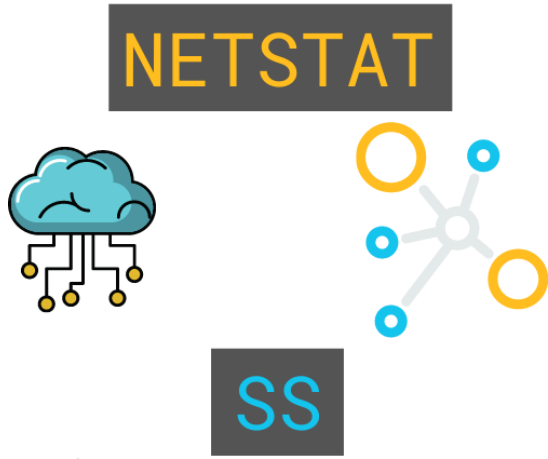
- La commande ip addr est un outil du paquet **iproute2** utilisé sous Linux pour afficher et gérer les adresses IP des interfaces réseau. Elle remplace l'ancienne commande ifconfig.
- **Usage typique** :
- Vérifier les adresses IP attribuées aux interfaces (ip addr show).
- Ajouter ou supprimer une adresse IP sur une interface (ip addr add 192.168.1.10/24 dev eth0).
- Diagnostiquer la configuration réseau de base d'une machine Linux.

Netstat (Network Statistics)

- **Afficher les connexions réseau actives**

- La commande netstat est un outil puissant pour afficher les statistiques réseau et les connexions reseau actives sur le systeme.
- La commande **netstat** est utilisée pour afficher les connexions réseau actives, les ports en écoute, ainsi que les statistiques des protocoles.
- **Usage typique** :
- Diagnostiquer les connexions ouvertes, vérifier quels services utilisent le réseau, et analyser les ports en écoute

ss (Socket Statistics)



- La commande ss est un outil sous Linux utilisé pour afficher des informations détaillées sur les sockets réseau (TCP, UDP, UNIX). Elle est plus moderne et plus rapide que l'ancienne commande netstat.
- **Usage typique** :
- Lister les connexions réseau actives (ss -t pour TCP, ss -u pour UDP).
- Afficher les ports en écoute (ss -ltn).
- Diagnostiquer les services qui utilisent le réseau (ss -tulnp).
- Surveiller l'état des connexions pour analyser la performance ou détecter des problèmes.

host

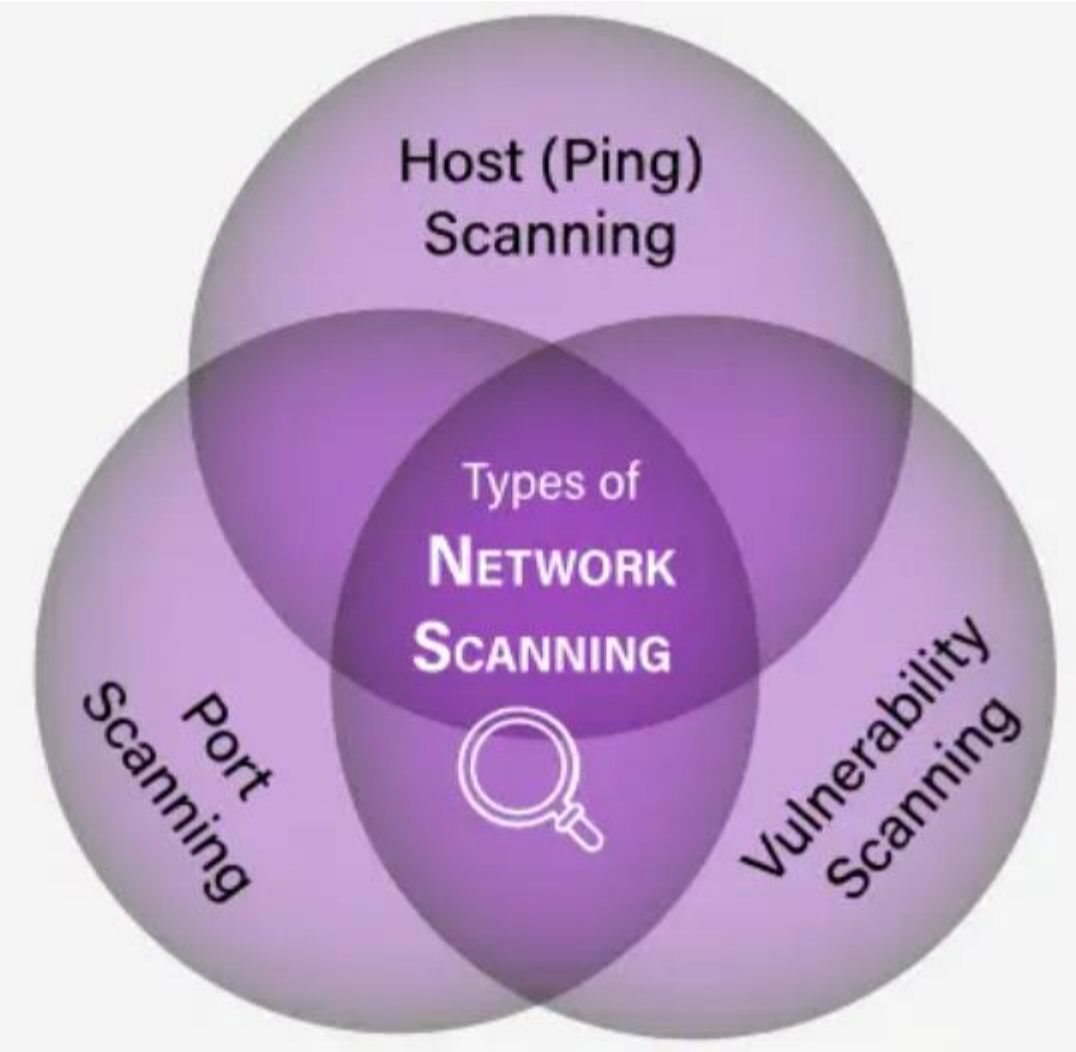
- La commande **host** est un outil simple pour effectuer des requêtes DNS et obtenir des informations sur un nom de domaine ou une adresse IP.
- **Usage typique** : Vérifier la résolution DNS d'un domaine (ex. host google.com) ou trouver l'adresse IP associée.
- Le fichier /etc/hosts est un fichier local qui associe manuellement des noms d'hôtes à des adresses IP.
- Peut contenir par exemple :
  - 127.0.0.1 localhost
  - 192.168.1.10 serveur1
- Il est consulté avant d'interroger un serveur DNS.

ifdown /ifup

- La commande **ifdown** permet de désactiver une interface réseau spécifiée dans la configuration système.
- **Usage typique** :
- Arrêter temporairement une interface réseau (ex. ifdown eth0) pour modifier sa configuration ou résoudre un problème.
- ifdown <interface> → Désactive l'interface réseau spécifiée.
- Exemple : sudo ifdown eth0
- L'interface eth0 est arrêtée et perd son adresse IP.
- ifup <interface> → Active l'interface réseau spécifiée en appliquant la configuration définie dans /etc/network/interfaces.
- Exemple :sudo ifup eth0
- L'interface eth0 est réactivée avec son adresse IP et ses paramètres.

nmap (Network Mapper)

- La commande **nmap** est un outil puissant de scan réseau permettant de découvrir les hôtes et services actifs sur un réseau.
- **Usage typique** :
- Scanner un réseau pour identifier les machines actives, les ports ouverts et les services disponibles (ex. audit de sécurité).



Sous Windows

- **Informations et diagnostic**
- ipconfig → Affiche la configuration IP de la machine (adresse IP, masque, passerelle).
- ipconfig /all → Affiche les détails complets (DNS, DHCP, adresse MAC).
- ping adresse → Teste la connectivité vers une machine (ex. ping google.com).
- tracert adresse → Affiche le chemin parcouru par les paquets jusqu'à la destination.
- nslookup nom_de_domaine → Vérifie la résolution DNS d'un nom de domaine.

Sous Windows

- **Services et gestion**
- netsh interface ip show config → Affiche la configuration IP des interfaces.
- netsh wlan show profiles → Liste les profils Wi-Fi enregistrés.
- netsh wlan show interfaces → Affiche l’état de la connexion Wi-Fi.

Sous Windows

- **Routage et connexions**
- route print → Affiche la table de routage.
- netstat -an → Liste les connexions réseau actives et les ports en écoute.
- netstat -r → Affiche les routes IP.
- arp -a → Affiche la table ARP (association IP ↔ MAC).

Fonction / Outil	Linux (commande)	Windows (commande)	Description
Afficher config IP	ip addr show / ifconfig	ipconfig / ipconfig /all	Voir adresses IP, masque, passerelle
Tester connectivité	ping	ping	Vérifier si une machine est joignable
Tracer le chemin réseau	tracepath / traceroute	tracert	Afficher les routeurs traversés
Résolution DNS	host / nslookup	nslookup	Vérifier la résolution d'un domaine
Table ARP	arp -n	arp -a	Associer IP ↔ adresse MAC
Table de routage	ip route show	route print	Voir les routes et passerelles
Ports ouverts / connexions	netstat -tulnp / ss -tulnp	netstat -an	Vérifier les connexions et ports en écoute
Désactiver interface	ifdown eth0	netsh interface set interface name="Ethernet" admin=disable	Arrêter une interface réseau
Scanner réseau	nmap	(outil tiers, ex. Nmap Windows)	Découvrir hôtes et ports ouverts
Réinitialiser config réseau	systemctl restart networking	ipconfig /release + ipconfig /renew	Réinitialiser la configuration IP

Exercice 1

- Quelle commande permet d’afficher toutes les interfaces réseau et leurs adresses IP sous Linux ?
- Quelle est la différence entre ip addr et ifconfig ?
- Que signifie le champ lo dans la liste des interfaces ?
- Quelle est la différence entre une adresse IP privée et une adresse IP publique ?
- Quelle commande permet d’ajouter manuellement une adresse IP à une interface ?
- Quelle commande permet d’afficher la table de routage ?
- Comment ajouter une route statique avec la commande ip route ?
- À quoi sert la commande ping et que teste-t-elle ?
- Quelle est la différence entre ping et traceroute ?
- Que permet d’observer la commande arp -n ?
- Quelle commande permet de voir les ports en écoute?

Exercice 1

- Quelle commande permet d’afficher toutes les interfaces réseau et leurs adresses IP sous Linux ?
- Quelle est la différence entre ip addr et ifconfig ?
- Que signifie le champ lo dans la liste des interfaces ?
- Quelle est la différence entre une adresse IP privée et une adresse IP publique ?
- Quelle commande permet d’ajouter manuellement une adresse IP à une interface ?
- Quelle commande permet d’afficher la table de routage ?
- Comment ajouter une route statique avec la commande ip route ?
- À quoi sert la commande ping et que teste-t-elle ?
- Quelle est la différence entre ping et traceroute ?
- Que permet d’observer la commande arp -n ?
- Quelle commande permet de voir les ports en écoute?

TP1 : Configuration IP et test de connectivité

- Pour savoir attribuer une adresse IP et vérifier la communication.
  - Afficher les interfaces réseau avec ip addr show.
  - Attribuer une adresse IP statique avec sudo ip addr add 192.168.1.10/24 dev ens33.
  - Verifier avec ip addr show ens33.
  - Vérifier la passerelle par défaut avec ip route.
  - Tester la connectivité avec ping 192.168.1.10 et ping 8.8.8.8 (Google DNS)

TP2 : Utilisation des outils de diagnostic réseau

- Pour analyser un réseau:
  - Utiliser ping pour tester la boucle locale (interface lo)
  - Employer traceroute pour voir le chemin vers une adresse (ex. traceroute google.com).
  - Observer la table ARP avec arp -n.
  - Vérifier les ports ouverts avec netstat -tulnp ou ss -tulnp.