

Commandes réseau sous Linux

Fiche de synthèse

① VUE D'ENSEMBLE

Les commandes modernes, `ip` et `ss`, remplacent peu à peu les commandes historiques `ifconfig`, `netstat` et `route`, encore fréquentes dans les sujets.

Commande	Couche	Rôle
<code>ip a</code>	accès réseau	configuration des interfaces
<code>ping</code>	internet (ICMP)	tester la connectivité
<code>traceroute</code>	internet	chemin d'un paquet
<code>nslookup</code> , <code>dig</code>	application (DNS)	résoudre un nom de domaine
<code>ss</code>	transport	connexions et ports
<code>ip neigh</code> , <code>arp</code>	accès réseau (ARP)	table ARP

② CONFIGURATION : IP A

`ip a` affiche chaque interface avec son adresse MAC (après `link/ether`), son adresse IP et son masque (`inet 192.168.1.42/24`) et son adresse de diffusion (`brd 192.168.1.255`).

- `lo` est la boucle locale, d'adresse `127.0.0.1` : la machine communique avec elle-même.
- L'adresse de diffusion a tous les bits de la partie hôte à 1 ; un paquet qui lui est envoyé atteint toutes les machines du réseau local. L'adresse réseau a tous ces bits à 0.
- Ces deux adresses ne sont attribuées à aucune machine : avec h bits de partie hôte, un réseau accueille au plus $2^h - 2$ machines, soit 254 pour un masque `/24`.

③ CONNECTIVITÉ : PING

`ping -c 4 192.168.1.1` envoie quatre paquets ICMP et attend les réponses. Pour chacune, il affiche `icmp_seq`, numéro du paquet, `ttl`, nombre de routeurs que le paquet peut encore traverser, et `time`, temps d'aller-retour en millisecondes ; puis le taux de perte.

Message	Interprétation
Destination Host Unreachable	la machine ne répond pas sur son réseau local : éteinte, débranchée ou inexistante
Network is unreachable	aucune route vers la destination
100% packet loss	un pare-feu bloque, ou la machine distante est injoignable
perte partielle	liaison instable ou saturée

④ CHEMIN : TRACEROUTE

Chaque routeur diminue de 1 le TTL d'un paquet ; à 0, il le détruit et renvoie un message ICMP *Time Exceeded*. `traceroute` envoie un paquet avec un TTL de 1, détruit par le premier routeur, qui se fait connaître ; puis un TTL de 2, et ainsi de suite jusqu'à la destination. Chaque ligne affichée donne un routeur et trois temps d'aller-retour ; * * * signale un routeur qui ne répond pas.

⑤ NOMS DE DOMAINE : NSLOOKUP ET DIG

Le DNS traduit un nom de domaine en adresse IP, par le port UDP 53. `nslookup www.python.org` indique le serveur DNS qui a répondu et l'adresse obtenue ; *non-authoritative answer* signifie que la réponse vient du cache d'un serveur. `dig www.python.org +short` n'affiche que l'adresse ; sans `+short`, il détaille la réponse, dont le type d'enregistrement, `A` pour une adresse IPv4.

⑥ CONNEXIONS : SS

`ss -tln` liste les ports TCP en écoute, avec des numéros plutôt que des noms : par exemple 22 pour SSH, 80 pour HTTP, 631 pour l'impression.

⑦ TABLE ARP : IP NEIGH

Le protocole ARP trouve l'adresse MAC qui correspond à une adresse IP du réseau local. `ip neigh`, ou `arp -a`, affiche les correspondances mémorisées : *REACHABLE* si elle est récente et confirmée, *STALE* si elle est ancienne, *INCOMPLETE* si la requête ARP est restée sans réponse.

À retenir.

- `ip a` montre la configuration ; `ping` teste la connectivité ; `traceroute` exploite le TTL pour révéler les routeurs traversés.
- `nslookup` et `dig` interrogent le DNS ; `ss` liste les ports en écoute ; `ip neigh` affiche la table ARP.