

TIP 1.10

Diagnostiquer un problème de connexion réseau

Fiche de révision - Support utilisateur

1. Méthode générale

Le diagnostic réseau doit progresser du poste vers le service final. Chaque test doit répondre à une question précise afin de localiser le niveau de panne.

Méthode à retenir

Connexion → Configuration IP → Passerelle → Communication distante → DNS → Application

2. Commencer par l'étendue

Situation	Orientation
Un seul poste	Câble, Wi-Fi, carte réseau, configuration IP locale.
Plusieurs postes	DHCP, VLAN, switch, Wi-Fi ou autre infrastructure commune.
Un site entier	Passerelle, routage, lien WAN/Internet ou infrastructure centrale.

3. Vérifier la connexion

En Ethernet : câble, prise, dock et voyants de lien. En Wi-Fi : Wi-Fi activé, bon SSID, signal suffisant et mode avion désactivé. Toujours vérifier la couche physique avant de modifier la configuration IP.

4. Lire la configuration IP

Commande / élément	Rôle
ipconfig /all	Afficher IPv4, masque, passerelle, DNS et état DHCP.
Adresse IPv4	Identifie le poste sur le réseau IP.
Masque	Définit la partie réseau et la partie hôte.
Passerelle	Permet de joindre les autres réseaux.
DNS	Traduit les noms en adresses IP.

5. APIPA

Une adresse 169.254.x.x est généralement une adresse APIPA. Elle indique que Windows n'a pas obtenu de configuration IPv4 via DHCP. Cela oriente vers le lien réseau, la prise, le VLAN, le DHCP ou un équipement intermédiaire.

Important : APIPA ne signifie pas automatiquement « serveur DHCP en panne ». Il faut vérifier la chaîne réseau.

6. Tests réseau essentiels

Test	Ce qu'il vérifie
ping 127.0.0.1	Pile TCP/IP locale du poste.
ping passerelle	Communication IP locale jusqu'à la passerelle.
ping IP distante	Connectivité IP/routage vers une destination distante.
nslookup nom	Résolution DNS et serveur DNS utilisé.
Test-NetConnection -Port	Connectivité TCP vers un port précis.

7. DHCP et DNS

Service	À retenir
DHCP	Attribue généralement automatiquement l'adresse IP, le masque, la passerelle et les DNS.
DNS	Permet de traduire un nom en adresse IP. Si une IP fonctionne mais pas un nom, la piste DNS devient prioritaire.

8. Commandes utiles

Commande	Usage
ipconfig /release	Libérer le bail DHCP dans un contexte adapté.
ipconfig /renew	Demander une nouvelle configuration DHCP.
ipconfig /displaydns	Afficher le cache DNS local.
ipconfig /flushdns	Vider le cache DNS local dans un diagnostic ciblé.

9. Ping : à interpréter correctement

Un ping réussi ne prouve pas qu'un service applicatif fonctionne. Un ping qui échoue ne prouve pas toujours qu'un équipement est hors ligne : ICMP peut être filtré. Le test doit être complété par le protocole ou le port réellement utilisé.

10. Réseau ou droits ?

« Serveur inaccessible » oriente vers la connectivité. « Accès refusé » peut indiquer que la communication fonctionne mais que les droits ou l'authentification posent problème.

11. Exemple de diagnostic

Observation	Interprétation
169.254.34.87, pas de passerelle	APIPA : échec d'obtention de configuration DHCP.
Collègue fonctionnel	Incident probablement local au poste, câble ou prise.
Nouveau câble → 192.168.10.63	Le lien réseau est rétabli ; poursuivre passerelle puis DNS.
Passerelle + Internet OK	Le câble initial est une cause probable.

12. À retenir

Le diagnostic réseau doit progresser par couches.
Connexion physique/Wi-Fi → configuration IP → passerelle → connectivité distante → DNS → application. Documenter les commandes utilisées, leurs résultats et l'éventuelle escalade vers l'équipe réseau.