

## TP 5.2 – Diagnostic et Réparation d'un Problème de Connexion Réseau

Vous êtes technicien au sein du **lycée Saint rémi**, dans l'équipe chargée du parc informatique. Un enseignant vous signale que son poste "n'a plus Internet du tout, ni sur le Wi-Fi, ni sur le câble". Votre mission est de **diagnostiquer méthodiquement** la panne.  
Votre arme : le terminal.  
Votre méthode : calme, précision, et un soupçon de mauvaise foi contrôlée.

### Partie 1 – Vérification de la configuration locale (ipconfig)

---

**Commande principale**  
**ipconfig /all**

**Travail demandé**

1. Relever :
  - o l'adresse IPv4

192.168.28.62

- o le masque

255.255.255.0

- o la passerelle

192.168.28.253

- o le DNS configuré

193.49.251.6

54.38.53.123

8.8.8.8

- o l'interface active (Ethernet / Wi-Fi)

Carte Ethernet Eth 1 - Realtek : DHCP activé et passerelle par défaut activé

2. Identifier **ce qui semble anormal** dans la configuration si :
  - o l'adresse commence par 169.254.x.x
  - o la passerelle n'est pas configurée
  - o aucun DNS n'apparaît
3. Quelle première action technique serait pertinente si l'adresse IP n'est pas obtenue automatiquement ?

ipconfig /release

ipconfig /renew

### Partie 2 – Pings de diagnostic

---

**Commandes à tester**  
**ping 127.0.0.1**  
**ping <IP passerelle locale>**  
**ping 8.8.8.8**  
**ping google.com**

**Questions**

1. Que signifie un ping OK sur 127.0.0.1 mais KO sur la passerelle ?

Un ping KO sur la passerelle (192.168.x.x) signifie que le problème se situe **entre votre PC et le routeur**.

2. Comment interpréter un ping OK vers la passerelle mais KO vers 8.8.8.8 ?

8.8.8.8 est une adresse IP publique (le serveur DNS de Google). Un ping KO vers cette adresse indique que **votre routeur ne transmet pas correctement votre requête vers Internet** ou que le trafic de réponse est bloqué. L'adresse 8.8.8.8 est presque toujours active, l'échec est donc sur le chemin.

Pinger **google.com** (un nom de domaine) échoue. Votre ordinateur doit **traduire** le nom google.com en une adresse IP via un serveur DNS. Si cela échoue, c'est que la résolution DNS est défectueuse.

3. Que conclure si certains pings montrent des délais très élevés (250ms+) ou une perte de paquets ?

- Délai élevé (Latence)** : Indique que les paquets prennent beaucoup de temps à faire l'aller-retour. Cela peut être dû à une surcharge du routeur, à une mauvaise qualité de la liaison WiFi, ou à une congestion chez le fournisseur d'accès ou à des points intermédiaires (surtout pour les pings externes).
- Perte de paquets** : Indique que des paquets sont abandonnés en chemin. C'est souvent le signe d'une mauvaise qualité de la connexion physique (câble endommagé, mauvaise réception WiFi) ou d'une saturation sévère du réseau.

4. Quelle piste envisager si le ping IP externe fonctionne mais pas le ping DNS ?

Comme dans la question 3, si vous pouvez pinger une IP externe (ex. 8.8.8.8), le réseau fonctionne. L'échec du ping par nom (DNS) confirme que le problème est le service de traduction.

### Partie 3 – Analyse du chemin réseau (tracert)

---

**Commande**  
**tracert google.com**

#### Questions

1. Notez le nombre de sauts (hop).

12

2. Que signifie un \* sur un ou plusieurs sauts ?

- Signification** : Le routeur ciblé **n'a pas renvoyé le message ICMP** (Internet Control Message Protocol) que tracert attend.
- Cause Principale** : Le plus souvent, le routeur est **intentionnellement configuré pour ne pas répondre aux requêtes de ping (ICMP)** à des fins de sécurité (pour masquer sa présence ou éviter les attaques).

3. Comment reconnaître si le blocage se situe :

- sur le réseau local
- chez le FAI
- chez Google

**Sur le réseau local** Le **saut 1** (votre passerelle par défaut, ex. 192.168.1.1) échoue (\* \* \* ou KO). C'est le premier point de défaillance. **Chez le FAI** Les **sauts 2 à 5** (ou les premiers sauts après votre passerelle) affichent systématiquement \* \* \*, et le traçage s'arrête complètement (il n'y a plus de sauts ultérieurs). **Chez Google (Destination)** Tous les sauts intermédiaires sont OK, mais le dernier saut (le **routeur de bordure de Google**) ou la destination finale affiche **Délai d'attente dépassé** ou un temps très élevé.

4. Pourquoi certains routeurs ne répondent jamais mais la connexion fonctionne quand même ?

Les routeurs intermédiaires sont configurés pour **ne pas répondre aux paquets de contrôle (ICMP)**, mais ils continuent de relayer le trafic de données normal (TCP/UDP).

5. Comment repérer un point de congestion réseau via tracert ?

Au lieu d'un délai progressif (ex. 10 ms, 12 ms, 15 ms, 18 ms...), vous verrez une rupture (ex. 15 ms, 18 ms, **250 ms, 255 ms, 260 ms...**). Le point de congestion est le **saut juste avant** l'augmentation drastique. La latence n'a pas nécessairement besoin d'être au-dessus de 250 ms ; toute augmentation soudaine de 10x ou plus (ex. 5 ms à 50 ms) est suspecte.

## Partie 4 – Surveillance locale des connexions (netstat)

---

Commande

**netstat -ano**

Questions

1. Comment savoir si un processus monopolise la bande passante ?
2. Trouvez une connexion suspecte (port inhabituel, IP étrangère, etc.).
3. Associez un PID trouvé dans netstat au processus dans le **Gestionnaire des tâches**.
4. Comment cette approche peut-elle aider à résoudre un problème réseau ?

## Partie 5 – Test de résolution DNS (nslookup)

---

Commandes

**nslookup google.com**

**nslookup microsoft.com 8.8.8.8**

Questions

1. Quelle adresse IP est retournée pour chaque domaine ?
2. En testant un DNS externe (8.8.8.8), comment isoler un problème de DNS interne ?
3. Que signifie un message "server not found" ?
4. Pourquoi nslookup peut réussir alors que ping échoue ?
5. Que faire si le DNS interne renvoie de mauvaises adresses ?
6. Comment nslookup permet-il de diagnostiquer un filtrage par pare-feu ?

## Partie 6 – Procédures de réparation réseau

---

1. Réinitialisation de la configuration IP

**ipconfig /release**

**ipconfig /renew**

Utilité : résoudre un conflit IP, relancer le DHCP, forcer une nouvelle attribution.

2. Purge de la résolution DNS

**ipconfig /flushdns**

Utile : si un site pointe vers une mauvaise IP ou après un changement de DNS.

3. Vérification et activation de l'interface

**netsh interface show interface**

**netsh interface set interface "Ethernet" enable**

4. Réinitialisation complète de la pile TCP/IP

**netsh int ip reset**

**netsh winsock reset**

Utilité : résoudre les problèmes "fantômes" liés aux sockets, filtres logiciels, VPN mal désinstallés, etc.

5. Test après réparation Reprendre Partie 2, puis Partie 5 pour valider le retour de la connectivité.