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 :
   - l'adresse IPv4
   - le masque
   - la passerelle
   - le DNS configuré
   - l'interface active (Ethernet / Wi-Fi)
2. Identifier **ce qui semble anormal** dans la configuration si :
   - l'adresse commence par 169.254.x.x
   - la passerelle n'est pas configurée
   - aucun DNS n'apparaît
3. Quelle première action technique serait pertinente si l'adresse IP n'est pas obtenue automatiquement ?

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 ?
2. Comment interpréter un ping OK vers la passerelle mais KO vers 8.8.8.8 ?
3. Et si 8.8.8.8 répond mais pas google.com ?
4. Que conclure si certains pings montrent des délais très élevés (250ms+) ou une perte de paquets ?
5. Quelle piste envisager si le ping IP externe fonctionne mais pas le ping DNS ?

Partie 3 – Analyse du chemin réseau (tracert)

Commande
tracert google.com

Questions

1. Notez le nombre de sauts (hop).
2. Que signifie un * sur un ou plusieurs sauts ?
3. Comment reconnaître si le blocage se situe :
   - sur le réseau local
   - chez le FAI
   - chez Google
4. Pourquoi certains routeurs ne répondent jamais mais la connexion fonctionne quand même ?
5. Comment repérer un point de congestion réseau via tracert ?

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.