METGY LEO SIO1

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)

```
Carte Ethernet Eth 1 - Realtek :

   Suffixe DNS propre à la connexion. . . : sio.edu
   Description. . . . . . . . . . . . . . : Realtek PCIe GbE Family Controller
   Adresse physique . . . . . . . . . . . : 18-60-24-F4-CF-5C
   DHCP activé. . . . . . . . . . . . . . : Oui
   Configuration automatique activée. . . : Oui
   Adresse IPv6 de liaison locale. . . . .: fe80::dc7:4b5e:77de:d412%4(préféré)
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.28.52(préféré)
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Bail obtenu. . . . . . . . . . . . . . : mardi 2 décembre 2025 07:06:27
   Bail expirant. . . . . . . . . . . . . : mardi 2 décembre 2025 09:06:25
   Passerelle par défaut. . . . . . . . . : 192.168.28.253
   Serveur DHCP . . . . . . . . . . . . . : 192.168.28.253
   IAID DHCPv6 . . . . . . . . . . . : 102260772
   DUID de client DHCPv6. . . . . . . . : 00-01-00-01-2E-63-32-A0-18-60-24-F4-CF-5C
   Serveurs DNS. . .  . . . . . . . . . . : 193.49.251.6
                                       54.38.53.123
                                       8.8.8.8
   NetBIOS sur Tcpip. . . . . . . . . . . : Activé
```

Identifier **ce qui semble anormal** dans la configuration si :

- l'adresse commence par 169.254.x.x
  Avec une adresse IP qui commence par 169.254 cela signifie qu'elle a été attribué automatiquement mais pas par le DHCP.
- la passerelle n'est pas configurée
  Sans passerelle il y aurait pas d'accès à internet ni aux autres réseaux.
- aucun DNS n'apparaît
  Sans DNS on ne peut pas naviguer sur internet en rentrant un site comme google.com par exemple il faudra rentrer l'ip directe du site.

2. Quelle première action technique serait pertinente si l'adresse IP n'est pas obtenue automatiquement ?
   Il faudrait regarder si le DHCP est activer ou non, faire ipconfig /release et ipconfig /renew et vérifier la connectique (câble Ethernet, prise, switch etc..) .

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 ?
   Le ping OK signifie que la carte réseau et le protocole IP fonctionnent et le KO signifie qu'il y a un problème de communication entre la machine et le réseau local.
2. Comment interpréter un ping OK vers la passerelle mais KO vers 8.8.8.8 ?

La passerelle répond, la communication locale fonctionne, par contre l'accès au réseau extérieur échoue.

3. Et si 8.8.8.8 répond mais pas google.com ?
   Le problème vient du DNS, le nom de domaine ne peut pas être résolu en adresse IP.
4. Que conclure si certains pings montrent des délais très élevés (250ms+) ou une perte de paquets ?
   Il y a une saturation du réseau, cela peut être dû à plusieurs soucis comme un DdoS, du matériel réseau défaillant etc …
5. Quelle piste envisager si le ping IP externe fonctionne mais pas le ping DNS ?
   Si une IP externe répond mais pas un nom de domaine, le problème vient forcément de la résolution DNS donc il faut reconfigurer le DNS.

Partie 3 – Analyse du chemin réseau (tracert)

Commande

tracert google.com

Questions

1. Notez le nombre de sauts (hop).

```
Détermination de l'itinéraire vers google.com [142.250.179.110]
avec un maximum de 30 sauts :
```

2. Que signifie un * sur un ou plusieurs sauts ?
   Cela signifie que le routeur n'a pas répondu à la requête.
3. Comment reconnaître si le blocage se situe :
   - sur le réseau local
   - chez le FAI
   - chez Google

   Blocage réseau local = Bloque dès le 1er hop
   Blocage chez le FAI = Bloque sur un hop intermédiaire
   Blocage chez Google = Bloque uniquement sur le dernier hop ou IP finale
4. Pourquoi certains routeurs ne répondent jamais mais la connexion fonctionne quand même ?
   Car certains routeurs filtrent volontairement les messages ICMP pour éviter les attaques de DdoS etc..
5. Comment repérer un point de congestion réseau via tracert ?
   Les temps de réponse augmentent brutalement par exemple de 12ms à 150ms sur un ou plusieurs hop.
   Plusieurs * apparaissent sur un hop précis.

Partie 4 – Surveillance locale des connexions (netstat)

Commande

netstat -ano

Questions

1. Comment savoir si un processus monopolise la bande passante ?
   En regardant les connexions TCP/UDP, si un processus apparaît beaucoup de fois dans l'un comme dans l'autre c'est qu'il utilise la bande passante de manière conséquente.
2. Trouvez une connexion suspecte (port inhabituel, IP étrangère, etc.).

```
TCP    [::1]:42050            [::]:0                 LISTENING       10568
```

3. Associez un PID trouvé dans netstat au processus dans le **Gestionnaire des tâches**.

```
C:\Users\etudinfo>tasklist /fi "pid eq 10568"

Nom de l'image                 PID Nom de la sessio Numéro de s Utilisation
========================= ======== ================ =========== ============
OneDrive.Sync.Service.exe    10568 Console                    3     55 788 Ko
```

Microsoft OneDrive Sync Service	0%	13,7 Mo	0 Mo/s	0 Mbits/s	0%	Très faible	Très faible

4. Comment cette approche peut-elle aider à résoudre un problème réseau ?

Grâce à cela on peut identifier un processus qui sature la bande passante du réseau et résoudre les problèmes en fermant certaines applications abusives.

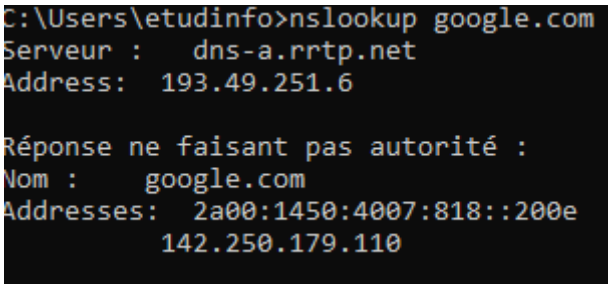
Partie 5 – Test de résolution DNS (nslookup)

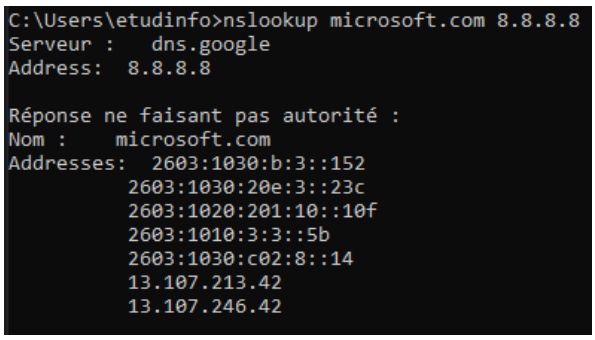
Commandes

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 ?
   Si nslookup google.com échoue mais que nslookup microsoft.com 8.8.8.8 réussi alors c'est un problème de DNS interne .
3. Que signifie un message "server not found" ?
   Le serveur DNS n'a pas pu résoudre le nom de domaine demandé.
4. Pourquoi nslookup peut réussir alors que ping échoue ?
   nslookup réussi =le nom se traduit correctement en IP
   ping qui échoue = problème de connectivité, filtrage ICMP ou firewall
5. Que faire si le DNS interne renvoie de mauvaises adresses ?
   Il faut vérifier la configuration du serveur DNS interne ou redémarrer le service DNS si nécessaire.
6. Comment nslookup permet-il de diagnostiquer un filtrage par pare-feu ?
   Oui car si une requête échoue vers le DNS externe mais qu'elle réussie vers le DNS interne alors c'est le firewall qui bloque le trafic DNS sortant.

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.