

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
L'adresse IPv4 est 192.168.28.42
 - le masque
Le masque de sous-réseau est 255.255.255.0
 - la passerelle
La passerelle par défaut est 192.168.28.253
 - le DNS configuré
Le DNS est : 193.49.251.6
54.38.53.123
8.8.8.8
 - l'interface active (Ethernet / Wi-Fi)
L'interface active est Carte Ethernet Eth 1 - Realtek
2. Identifier **ce qui semble anormal** dans la configuration si :
 - l'adresse commence par 169.254.x.x
Une adresse commençant par 169.254 est une adresse APIPA, cela signifie que nous auront un problème de réseau
 - la passerelle n'est pas configurée
Si la passerelle n'est pas connecté il sera donc impossible d'accéder à internet
 - aucun DNS n'apparaît
Sans DNS, il est impossible de communiquer avec internet même si l'adresse et la passerelle était bonne
3. Quelle première action technique serait pertinente si l'adresse IP n'est pas obtenue automatiquement ?

De vérifier si la connexion physique est bien établie, généralement les problèmes viennent de la connexion physique. Une fois fais, le serveur DHCP redonne une adresse IP valide (ex 192.168.29.39). Il serait intéressant aussi de taper la commande **ipconfig /release**

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

```

C:\Users\etudinfo>ping 127.0.0.1

Envoi d'une requête 'Ping' 127.0.0.1 avec 32 octets de données :
Réponse de 127.0.0.1 : octets=32 temps<1ms TTL=128
Réponse de 127.0.0.1 : octets=32 temps<1ms TTL=128
Réponse de 127.0.0.1 : octets=32 temps<1ms TTL=128
Réponse de 127.0.0.1 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 127.0.0.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

C:\Users\etudinfo>ping 192.168.28.253

Envoi d'une requête 'Ping' 192.168.28.253 avec 32 octets de données :
Réponse de 192.168.28.253 : octets=32 temps=1 ms TTL=64
Réponse de 192.168.28.253 : octets=32 temps=1 ms TTL=64
Réponse de 192.168.28.253 : octets=32 temps<1ms TTL=64
Réponse de 192.168.28.253 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 192.168.28.253:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms

C:\Users\etudinfo>ping 8.8.8.8

Envoi d'une requête 'Ping' 8.8.8.8 avec 32 octets de données :
Réponse de 8.8.8.8 : octets=32 temps=62 ms TTL=114
Réponse de 8.8.8.8 : octets=32 temps=61 ms TTL=114
Réponse de 8.8.8.8 : octets=32 temps=60 ms TTL=114
Réponse de 8.8.8.8 : octets=32 temps=51 ms TTL=114

Statistiques Ping pour 8.8.8.8:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 51ms, Maximum = 62ms, Moyenne = 58ms

C:\Users\etudinfo>ping google.com

Envoi d'une requête 'ping' sur google.com [142.250.179.110] avec 32 octets de données :
Réponse de 142.250.179.110 : octets=32 temps=35 ms TTL=114
Réponse de 142.250.179.110 : octets=32 temps=42 ms TTL=114
Réponse de 142.250.179.110 : octets=32 temps=56 ms TTL=114
Réponse de 142.250.179.110 : octets=32 temps=49 ms TTL=114

Statistiques Ping pour 142.250.179.110:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 35ms, Maximum = 56ms, Moyenne = 45ms

C:\Users\etudinfo>

```

Questions

1. Que signifie un ping OK sur 127.0.0.1 mais KO sur la passerelle ?
Le problème vient d'entre le pc et le réseau, cela veut dire qu'il y'a pas de problème à l'intérieur du pc
2. Comment interpréter un ping OK vers la passerelle mais KO vers 8.8.8.8 ?
Cela veut dire que notre PC vas bien jusqu'au routeur mais que le routeur lui, n'arrive pas à Internet. Il y'a d'autre possibilité pour que le ping soit KO vers 8.8.8.8, il se peut aussi que la connexion entre le routeur et mon fournisseur soit couper et/ou que la passerelle n'a pas de sortie vers internet.
PC → Routeur(Correct)
Routeur → Internet(Incorrect)
3. Et si 8.8.8.8 répond mais pas google.com ?
« google.com » est un nom de domaine pas une adresse IP. Si le PC n'a pas réussi à le déchiffrer cela veut dire que le DNS ne fonctionne pas.
4. Que conclure si certains pings montrent des délais très élevés (250ms+) ou une perte de paquets ?
Cela veut dire que la connexion Internet est mauvaise, du a peut-être un réseau saturé, une distante importante, un problème matériel et/ou problème physique
5. Quelle piste envisager si le ping IP externe fonctionne mais pas le ping DNS ?
Vérifier si le DNS est configurée, si non il faut ajouter un DNS
Tester un autre DNS
Vérifier le pare-feu ou les restrictions réseau
Redémarrer la connexion réseau

Partie 3 – Analyse du chemin réseau (tracert)

Commande

tracert google.com

```
C:\Users\etudinfo>tracert google.com

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

  1      1 ms      <1 ms      <1 ms      192.168.28.253
  2      1 ms      1 ms      1 ms      10.96.9.245
  3     10 ms     10 ms     11 ms     172.18.128.93
  4     11 ms     11 ms     11 ms     10.251.0.2
  5     11 ms     11 ms     11 ms     routeur-upjv.ac-amiens.fr [195.221.156.15]
  6     13 ms     12 ms     13 ms     194.167.1.141
  7     13 ms     13 ms     12 ms     vl221-be2-ren-nr-compiegne-rtr-091.noc.renater.fr [193.51.181.190]
  8     14 ms     13 ms     64 ms     xe-0-0-8-ren-nr-paris2-rtr-131.noc.renater.fr [193.51.177.206]
  9     15 ms     14 ms     14 ms     192.178.70.144
 10     18 ms     14 ms     16 ms     72.14.233.195
 11     14 ms     14 ms     14 ms     142.251.49.135
 12     14 ms     14 ms     14 ms     par21s20-in-f14.1e100.net [142.250.179.110]

Itinéraire déterminé.

C:\Users\etudinfo>
```

Questions

1. Notez le nombre de sauts (hop).
Il y'a 12 sauts
2. Que signifie un * sur un ou plusieurs sauts ?
Cela peut signifier : Un routeur ou équipement qui ne répond pas aux requêtes ICMP
Problème de réseau temporaire
Pas forcément un problème critique
3. Comment reconnaître si le blocage se situe :
 - o sur le réseau local
Ping vers la passerelle → KO
Ping vers une IP externes → KO
Traceroute ne vas pas au-delà de la passerelles
 - o chez le FAI
Ping vers la passerelle → OK
Ping vers une IP externes → KO
Traceroute s'arrête directement après les premiers sauts
 - o chez Google
Ping vers 8.8.8.8 → OK
Pings vers google.com → KO
Traceroute arrive à arriver jusqu'au dernier sauts mais pas jusqu'à la destinations finals
4. Pourquoi certains routeurs ne répondent jamais mais la connexion fonctionne quand même ?
Car il se peut que cela se produit : Sécurité et filtrage ICMP, Priorité au routage plutôt qu'aux réponses de diagnostic, Réponse retardée ou filtrée
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.