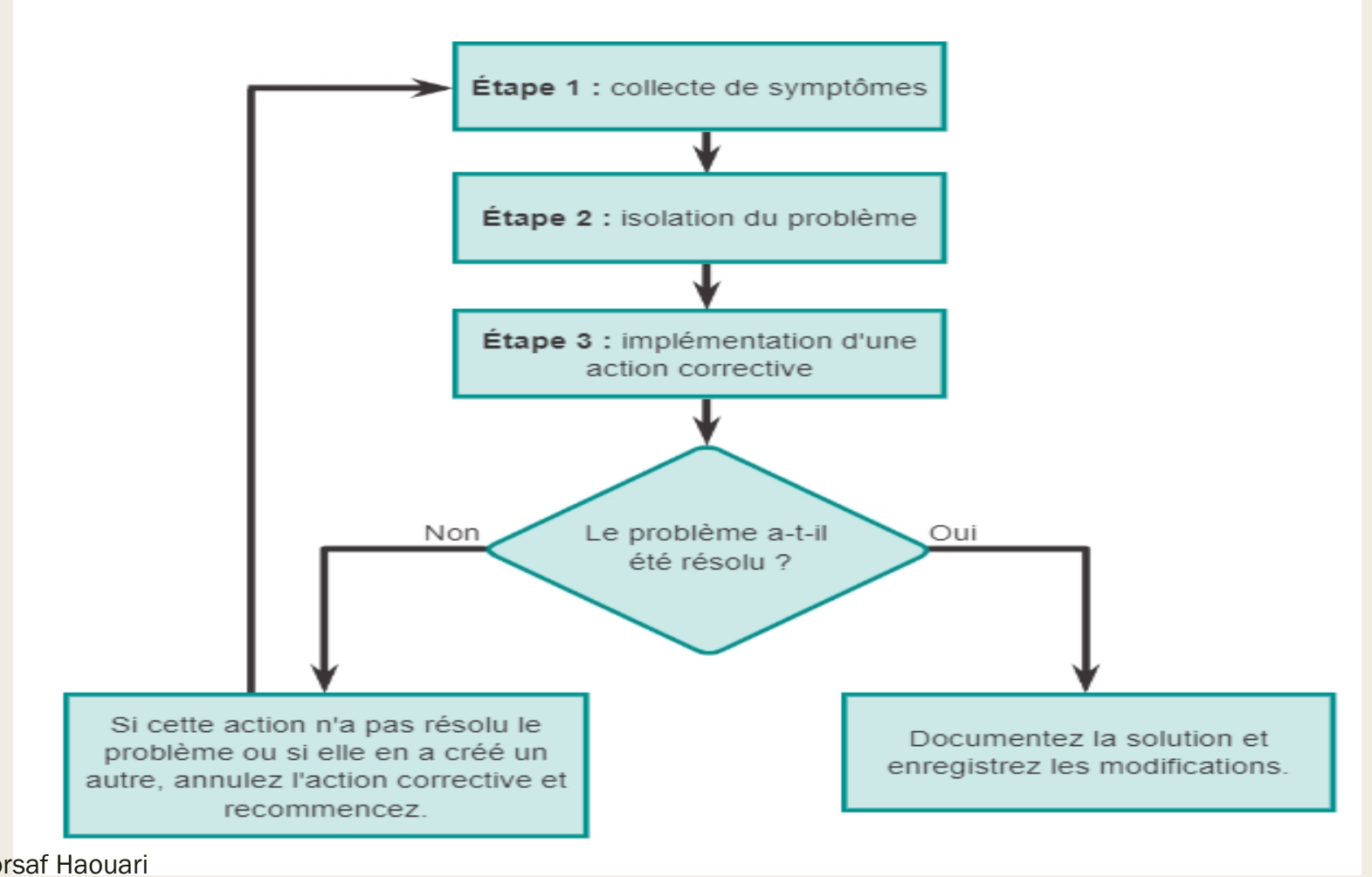
DÉPANNAGE D'UNE STATION DE TRAVAIL EN RÉSEAU

Résoudre les problème du réseau

- Tous les réseaux nécessiteront un dépannage.
- Si vous ne savez pas par où commencer ou si vous n’avez pas développé de méthodologie, vous perdrez du temps et des ressources.
- Sans une méthodologie de dépannage, les niveaux de frustration - des techniciens et de ceux qu'ils supportent - vont augmenter.
- Une méthodologie de dépannage systématique peut réduire considérablement le temps nécessaire pour résoudre un problème et fermer un ticket d'incident réseau, ce qui permet de gagner du temps ainsi que d'autres ressources.

Procédure générale de dépannage systématique

- Le processus de dépannage systématique se compose de trois étapes principales :



Étape 1. Collecte de symptômes :

- Il est essentiel d'obtenir une image complète du problème. Examiner attentivement comment le problème se manifeste
- Pour cela, le dépannage commence par la collecte et la documentation des symptômes du réseau et des utilisateurs.
- Lors de la collecte de symptômes, il est important que le technicien collecte des faits et des preuves afin d'éliminer progressivement des causes possibles et d'identifier finalement la véritable origine du problème.
- Le technicien pose des questions et analyse le problème afin de diminuer le nombre de possibilités.

  - *Exemples:*
    - Le problème se limite-t-il à un seul périphérique, à un groupe de périphériques ou à un sous-ensemble complet du réseau ?
    - Le problème s'applique-t-il au trafic entrant, au trafic sortant ou aux deux?
    - Essayez de déterminer quand le problème a commencé et de considérer sa fréquence. Est-ce un problème constant ou intermittent?
    - La cause peut être un effet secondaire imprévu de la maintenance. Quelqu'un a-t-il apporté des modifications au pare-feu ou à l'équipement de réseau auquel il est connecté?

Étape 2. Isolation du problème :

- Le technicien doit dresser une liste de toutes les causes possibles du problème.
- Pour élaborer cette liste de causes possibles, le technicien analyse les caractéristiques des problèmes au niveau des couches logiques du réseau afin de pouvoir sélectionner la cause la plus probable.
- Les techniciens doivent penser à remettre en question l'évidence.
  - *Exemple: Si l'imprimante réseau ne fonctionne pas, commencez par vous assurer qu'elle est allumée.*
- La liste des causes possibles doit ensuite être divisée en trois sections. Ils devraient être "peu probable", "probable" et "le plus probable".
- De cette façon, le technicien arrive à éliminer des variables jusqu'à ce qu'un problème unique ou un ensemble de problèmes apparentés ait été identifié en tant que cause.

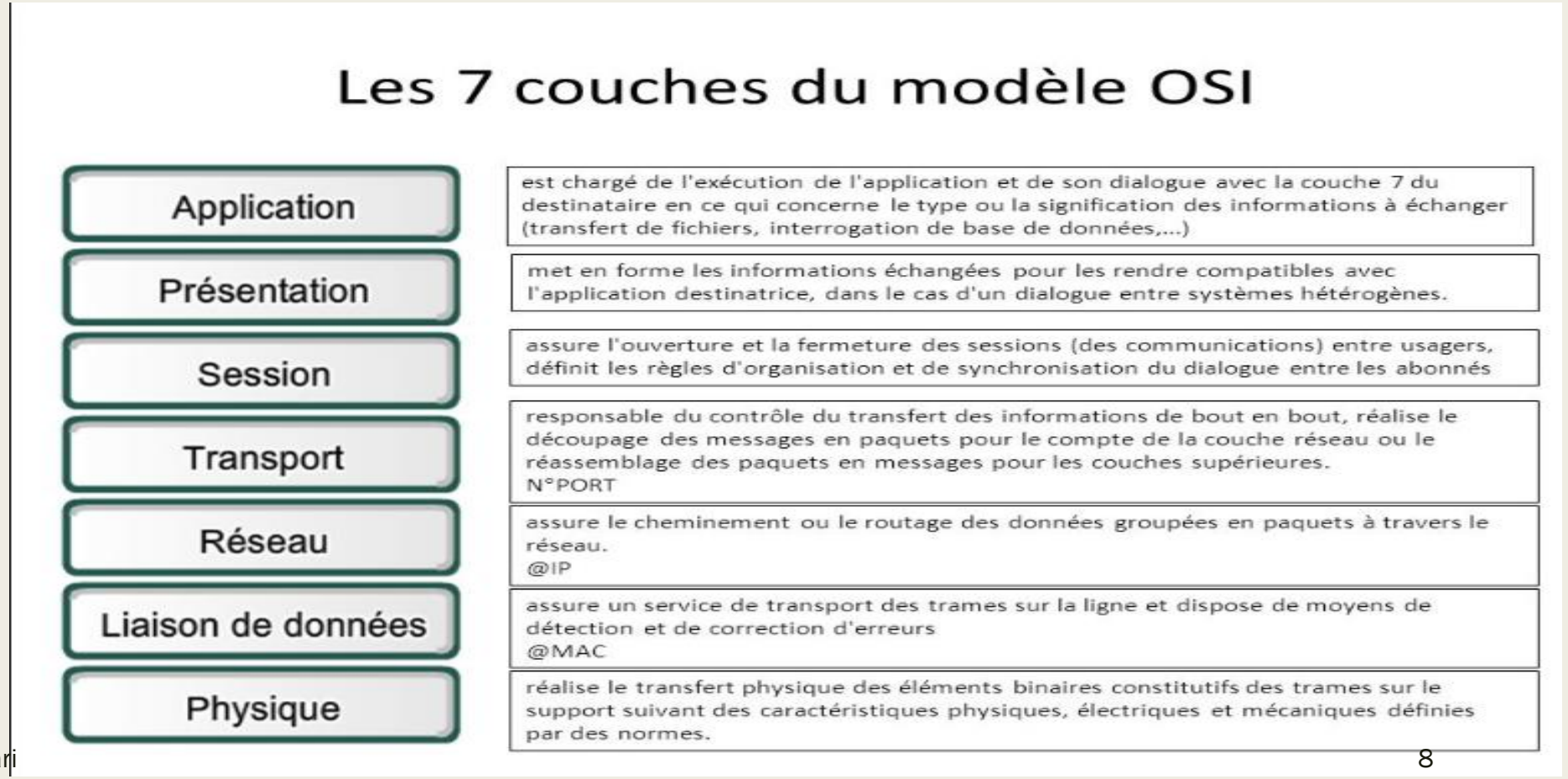
Étape 3. Implémentation d'une action corrective :

- Une fois le problème identifié et une solution trouvée, le technicien peut décider si cette solution peut être implémentée immédiatement ou reportée à plus tard.
- Cela dépend en effet de l'impact des modifications nécessaires sur les utilisateurs et le réseau.
  - *La gravité du problème doit être mise en rapport avec l'impact de sa solution.*
- Par exemple, si un serveur ou un routeur critique doit être mis hors connexion pendant un laps de temps relativement long, il peut être préférable d'attendre la fin de la journée de travail avant d'implémenter la résolution du problème.
- Parfois, une solution provisoire peut être mise en œuvre en attendant la résolution réelle du problème.
- Si l'action corrective crée un autre problème ou ne permet pas de résoudre le problème initial, la solution tentée est documentée, les modifications sont supprimées et le technicien recommence à collecter des symptômes et à essayer d'isoler le problème.

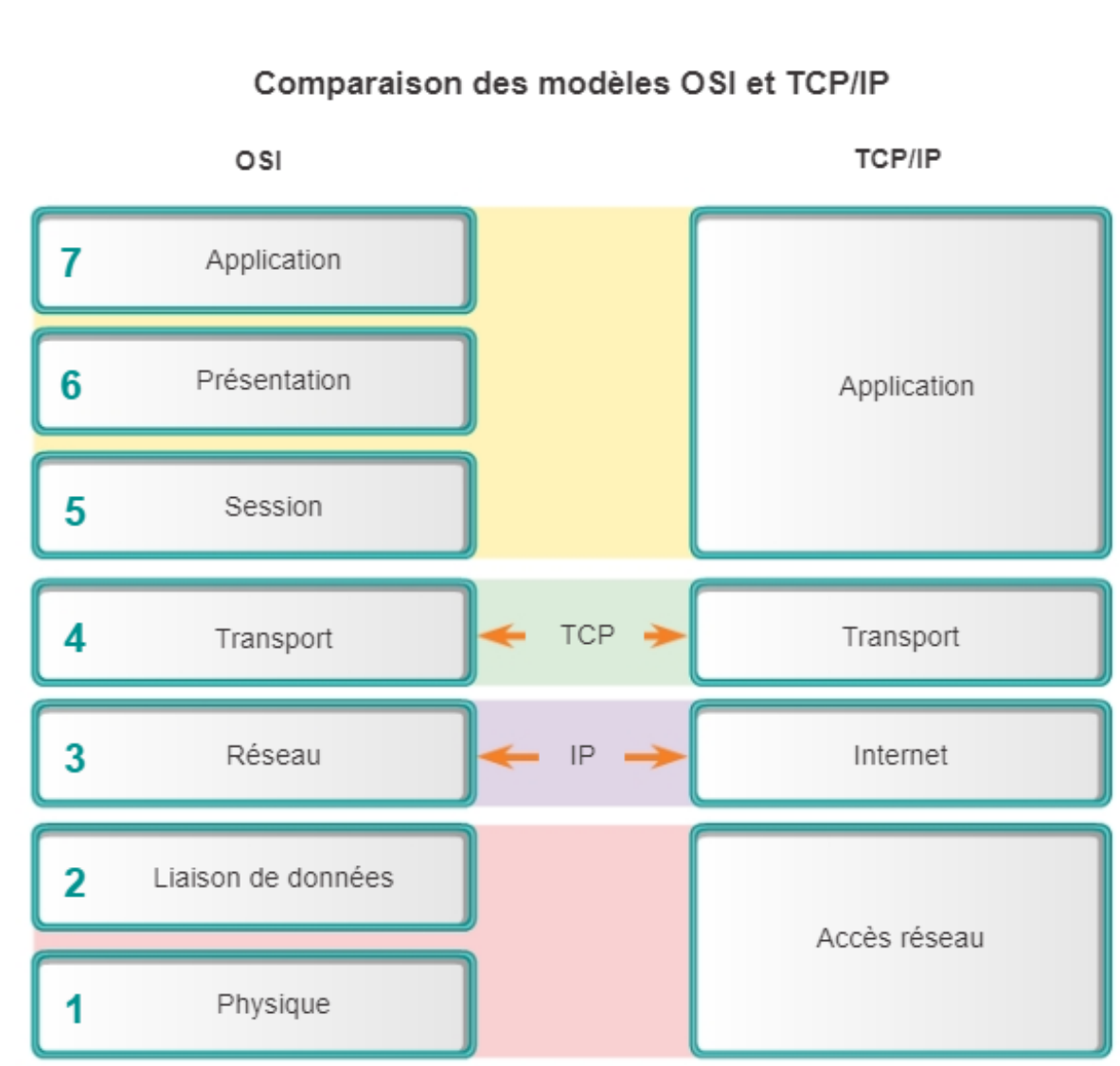
- Ces différentes étapes ne s'excluent pas mutuellement.
- En effet, le technicien peut à tout moment être amené à revenir à l’une des étapes précédentes.
- Par exemple, il se peut que le technicien doive collecter un plus grand nombre de symptômes lors de l'isolation d'un problème.
- De plus, un autre problème pourrait être créé lors de la tentative de correction d'un problème. Dans ce cas, supprimez les modifications et recommencez le dépannage.

Isolation du problème à l'aide des modèles en couches

- Afin d'isoler le problème, le technicien compare les caractéristiques du problème avec les couches logiques du réseau



Isolation du problème à l'aide des modèles en couches (suite)

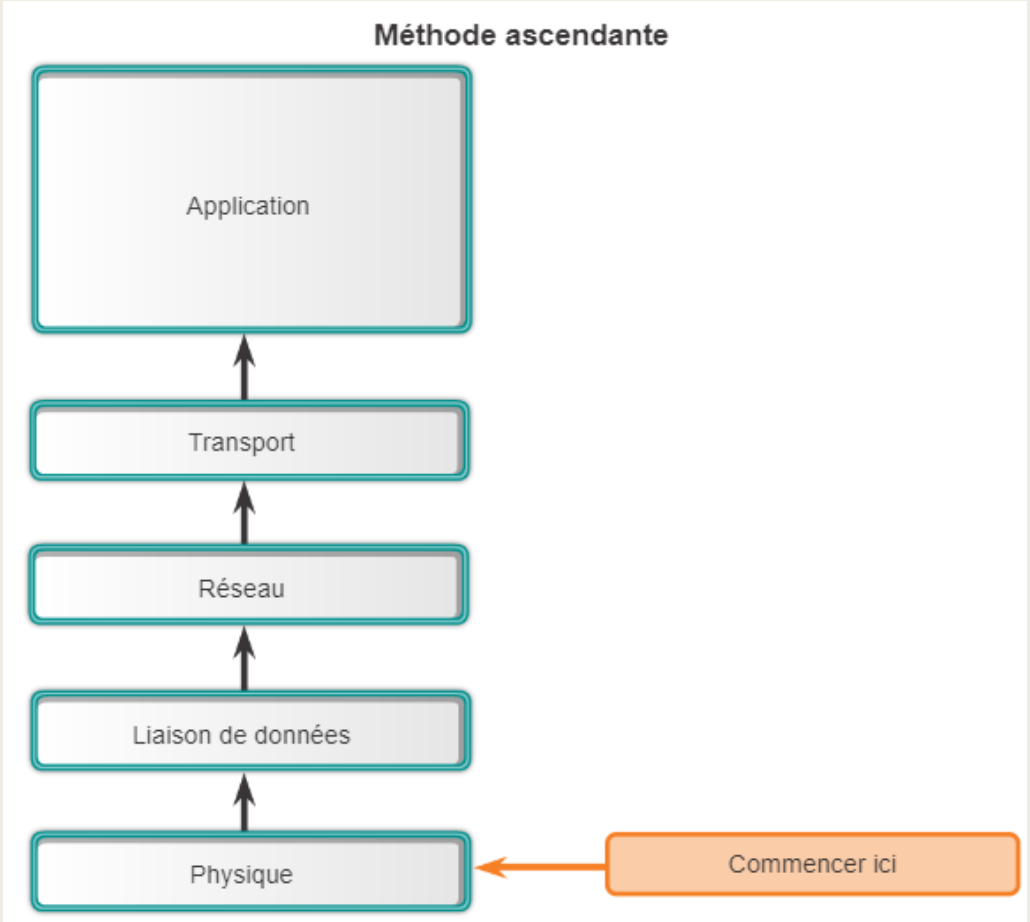


Isolation du problème à l'aide des modèles en couches (suite)

- Ces modèles en couches possèdent trois méthodes principales en matière de dépannage des réseaux :
  - *méthode ascendante*
  - *méthode descendante*
  - *diviser et conquérir*
- Chacune de ces approches présente ses avantages et ses inconvénients.

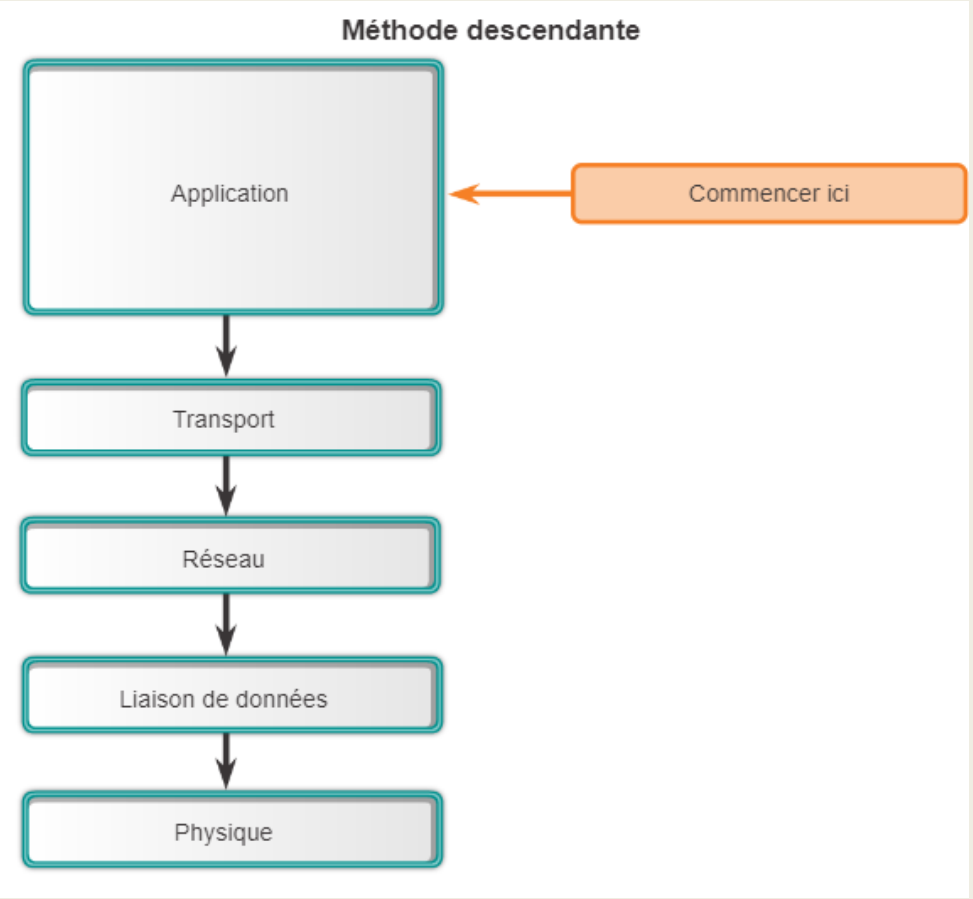
Méthode de dépannage ascendante

- Vous commencez par examiner les composants physiques du réseau, puis vous remontez une à une les différentes couches du modèle OSI jusqu'à ce que la cause du problème ait été identifiée
- Cette approche est conseillée lorsque vous pensez que le problème est physique.
- La plupart des problèmes réseau se situent au niveau des couches inférieures, ce qui signifie que la mise en œuvre de l'approche ascendante est souvent efficace.
- L'inconvénient de cette approche est qu'elle nécessite la vérification de chacun des périphériques jusqu'à ce que la cause possible du problème ait été trouvée.
  - *N'oubliez pas que chaque conclusion et possibilité doit être documentée ; cela peut donc représenter un travail administratif important.*
- Un autre défi consiste à déterminer quels périphériques examiner en premier lieu.



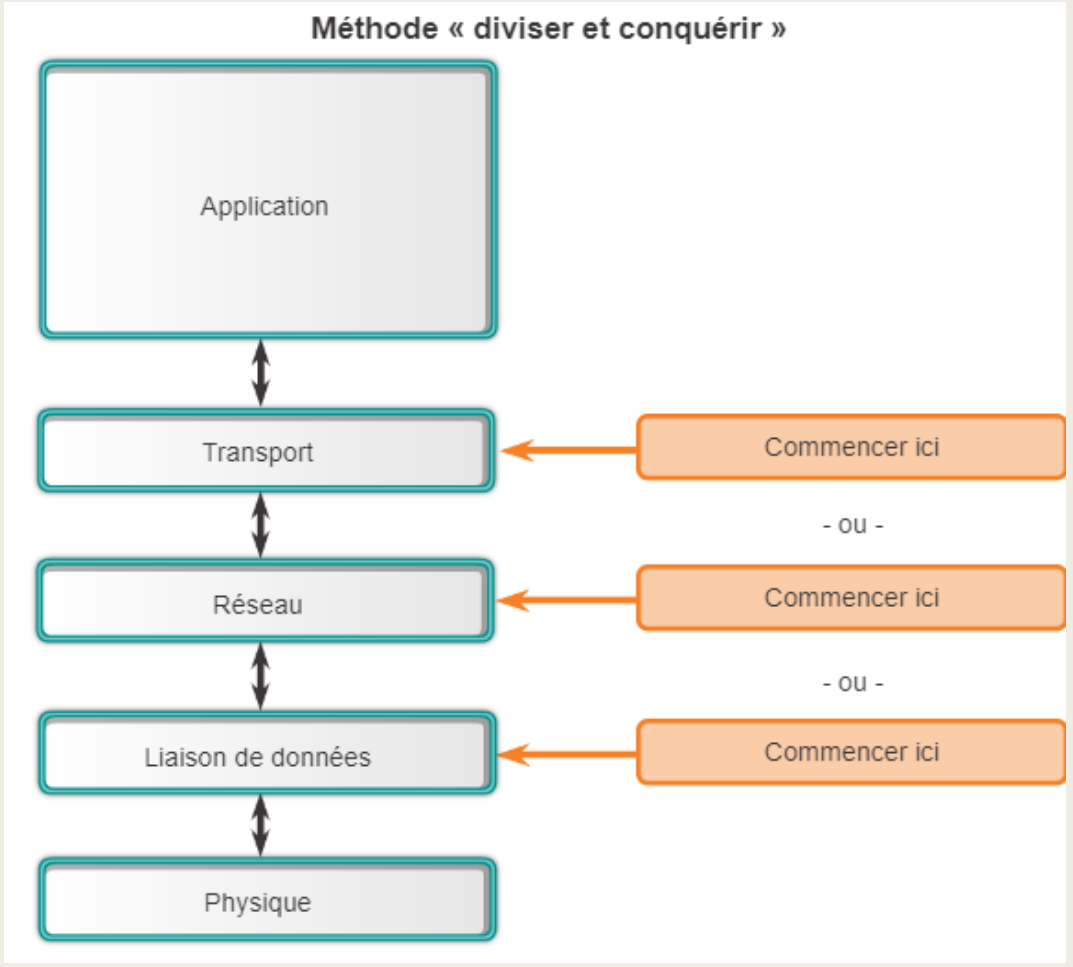
Méthode de dépannage descendante

- Le dépannage descendant commence par les applications destinées aux utilisateurs finaux, puis parcourt vers le bas une à une les différentes couches du modèle OSI jusqu'à ce que la cause du problème ait été identifiée.
- Utilisez cette approche lorsque vous pensez que le problème concerne un élément logiciel.
- L'inconvénient de l'approche descendante est qu'elle nécessite la vérification de chaque application réseau jusqu'à ce que la cause possible du problème ait été trouvée.
  - *Chaque conclusion et chaque possibilité doivent être documentées.*
- Le défi consiste à déterminer quelle application examiner en premier lieu.



Méthode de dépannage « diviser et conquérir »

- Le technicien sélectionne une couche et effectue des tests dans les deux sens à partir de cette couche.
- Vous commencez par collecter les expériences utilisateur du problème, vous documentez les symptômes, puis, à l'aide de ces informations, vous essayez de deviner par quelle couche entreprendre vos recherches.
- Lorsqu'il a été vérifié qu'une couche donnée fonctionne correctement, on peut supposer que les couches inférieures fonctionnent également de manière appropriée. Le technicien peut alors examiner les couches supérieures.
- Si une couche ne fonctionne pas correctement, le technicien peut commencer à examiner les couches inférieures du modèle.
- Par exemple, des utilisateurs ne peuvent pas accéder au serveur Web.
  - *Si une analyse a révélé la présence de connectivité, cela signifie que le problème se situe au-dessus de la couche 3.*
  - *Par contre, si le test de connectivité au serveur échoue, cela signifie que le problème se situe vraisemblablement au niveau d'une couche inférieure.*



Approches de dépannage moins structurées

- Outre l'approche systématique du dépannage, il existe également des approches de dépannage moins structurées.
- L'une de ces approches de dépannage se base sur une estimation réfléchie effectuée par le technicien, réalisée en fonction des symptômes du problème.
  - *Cette méthode doit de préférence être mise en œuvre avec des administrateurs réseau expérimentés, car ces derniers peuvent se baser sur leurs larges connaissances et leur grande expérience pour isoler et résoudre des problèmes réseau.*
  - *Avec un administrateur réseau moins expérimenté, cette méthode de dépannage s'apparente plutôt à un dépannage aléatoire.*
- Une autre approche consiste à comparer une situation de fonctionnement avec une situation de non-fonctionnement, puis à identifier les différences significatives, notamment :
  - Configurations
  - Versions des logiciels
  - Propriétés du matériel et des autres périphériques
  - *L'utilisation de cette méthode peut conduire à une solution fonctionnelle, mais sans clairement révéler la cause du problème.*
  - *Cette méthode peut être utile lorsque le technicien manque d'expertise ou lorsque le problème a besoin d'une résolution rapide.*
  - *Une fois la solution implémentée, le technicien peut mener des recherches supplémentaires sur la cause réelle du problème.*

Approches de dépannage moins structurées (suite)

- La substitution est une autre méthode de dépannage rapide.
- Elle implique le remplacement du périphérique problématique par un autre que l'on sait fonctionner parfaitement.
- Si cela permet de résoudre le problème, le technicien sait alors que le problème est dû au périphérique remplacé.
- Si le problème subsiste, cela signifie que la cause se situe ailleurs.
- Dans certaines situations, il peut s'agir d'une méthode idéale pour une résolution rapide d'un problème,
  - *Exemple en cas de panne d'un point de routage unique, tel qu'un routeur*
  - *Il est parfois plus utile de simplement remplacer le périphérique et de rétablir le service, plutôt que de dépanner le problème.*

Exemples de problèmes de la couche physique

- Dans la couche physique, les problèmes impliquent généralement une rupture de la connectivité physique qui constitue le réseau.
- Des connexions réseau rompues, des problèmes de câblage et de connecteurs et des problèmes matériels empêchant le mouvement de l'électricité d'un périphérique à l'autre indiquent généralement un problème au niveau de cette couche.

Exemples de problèmes de la couche liaison de données

- Les problèmes de liaison de données sont souvent liés aux problèmes du protocole ARP (Address Resolution Protocol) lorsqu'il associe des adresses IP à des adresses MAC (Media Access Control).

Exemples de problèmes de la couche réseau

- À la couche réseau, nous commençons à rencontrer des problèmes de traversée du réseau.
- Les problèmes de couche réseau surviennent généralement lorsque les paquets réseau ne peuvent pas se déplacer de la source à la destination.
- Cela peut être dû à un adressage IP incorrect ou à des adresses IP en double sur le réseau.

Exemples de problèmes de la couche transport

- Au niveau de la couche Transport, nous isolons les problèmes qui surviennent généralement avec les paquets TCP ou UDP dans les réseaux Ethernet.
- Cela peut être dû à des erreurs de retransmission excessives ou à une fragmentation des paquets.
- Les problèmes de cette couche peuvent être difficiles à localiser car, contrairement aux couches inférieures, ils n'entraînent souvent pas une perte totale de connectivité.

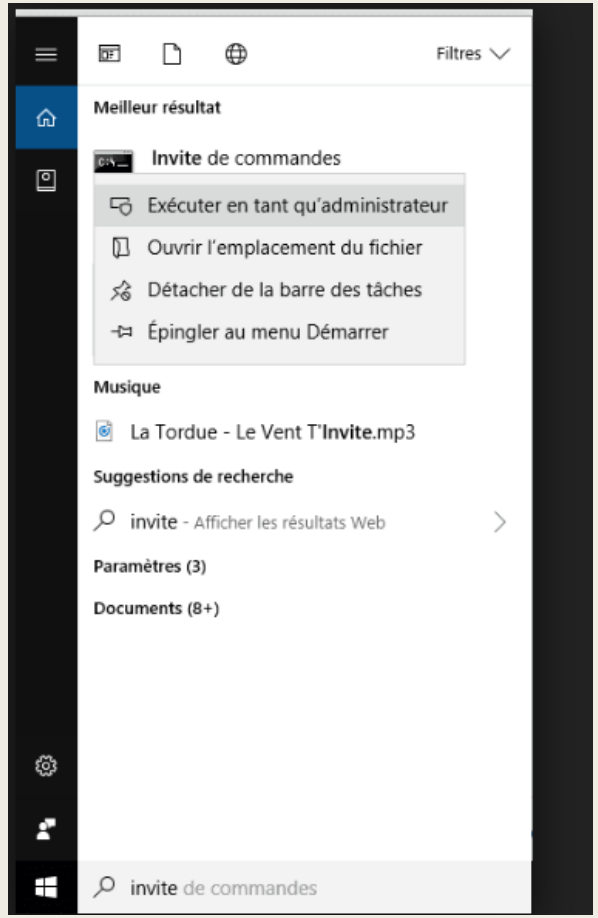
Exemples de problèmes de la couche Application

- Le processus de dépannage de cette couche implique des problèmes liés aux applications qui reposent sur le réseau.
- Ces applications peuvent impliquer une résolution DNS, ou autre, des problèmes d'application sur des systèmes d'exploitation résidents, des échecs de protocole de haut niveau.
- HTTP, SMTP, FTP et d'autres protocoles qui «utilisent généralement le réseau» plutôt que «exécutent le réseau» sont des exemples de ces protocoles de haut niveau.

Commandes réseau utiles de Windows

- Dans la suite, on verra les principales commandes réseaux utiles qui peuvent vous aider à diagnostiquer des problèmes réseaux sur Windows.
- Toutes les commandes fonctionnement avec l'invite de commandes.
- Invite de commande:
  - une interface qui permet d'envoyer des commandes directement à Windows
  - Pour ouvrir l'invite de commande sous Windows 10 en tant qu'administrateur:
    1. Chercher l'invite de commande à partir de l'icône de recherche
    2. Clic droit sur le résultat invite de commande
    3. Choisir l'option « Exécuter en tant qu'administrateur »
- Pour avoir de l'aide sur les options d'une commande, tapez:

  nomCommande \?



Commandes réseau: arp

- Affiche et modifie les tables de traduction d'adresses IP en adresses physiques utilisées par le protocole de résolution d'adresses ARP
  - *Permet de détecter les erreurs de mappage d'adresse*

```
Z:\>arp -a

Interface : 192.168.116.1 --- 0x6
  Adresse Internet      Adresse physique      Type
  192.168.116.254       00-50-56-ee-27-04     dynamique
  192.168.116.255       ff-ff-ff-ff-ff-ff     statique
  224.0.0.2             01-00-5e-00-00-02     statique
  224.0.0.22            01-00-5e-00-00-16     statique
  224.0.0.251           01-00-5e-00-00-fb     statique
  224.0.0.252           01-00-5e-00-00-fc     statique
  239.255.255.250       01-00-5e-7f-ff-fa     statique
  239.255.255.253       01-00-5e-7f-ff-fd     statique
  255.255.255.255       ff-ff-ff-ff-ff-ff     statique
```

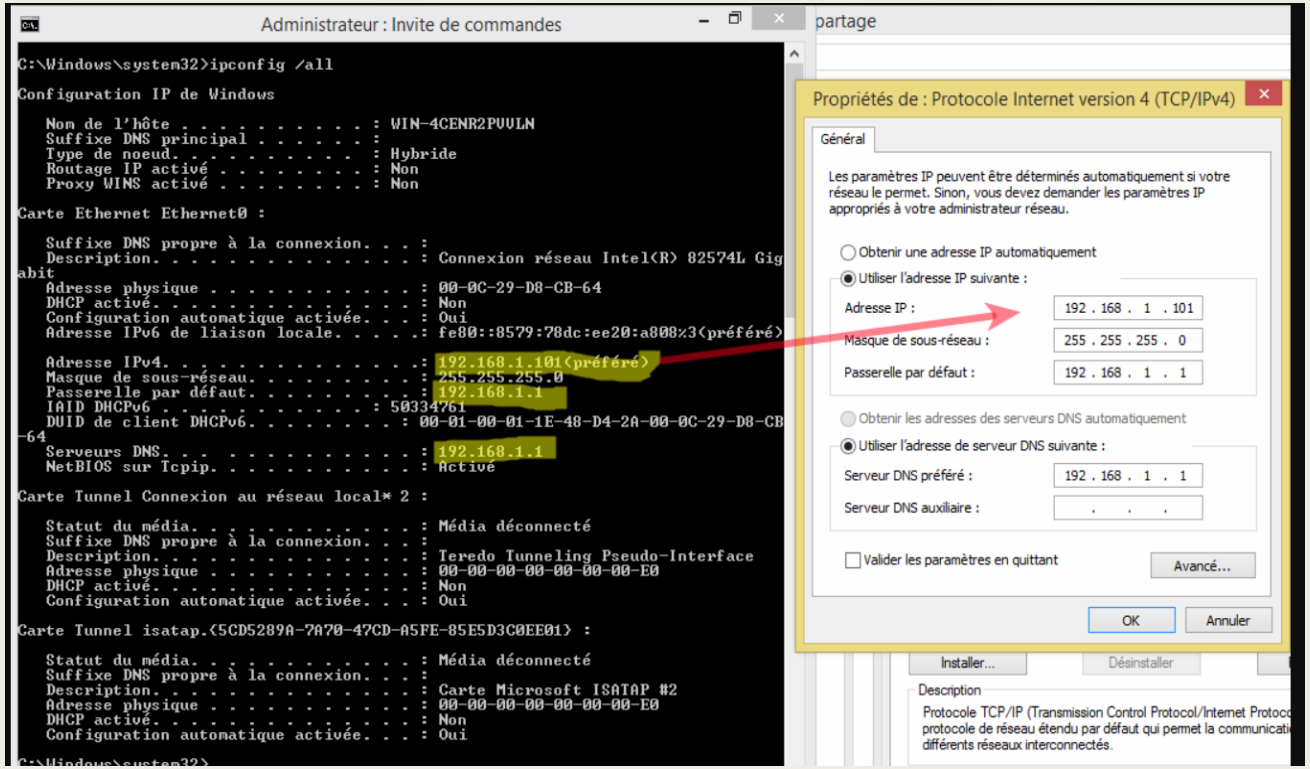
Commandes réseau: ipconfig

- Ipconfig est une commande qui permet d'obtenir la configuration IP de chaque interface réseaux.
- Cette commande fournit des informations telles que l'adresse IP, le masque de sous-réseau, l'adresse physique de la machine et la passerelle par défaut de la machine locale.
- Pour lister la configuration IP de toutes les interfaces :

  ipconfig /all

- Ipconfig permet aussi de vider le cache DNS, renouveler un bail DHCP.

- on retrouve bien la configuration TCP/IP IPv4 de notre interface Ethernet0



Commandes réseau: ipconfig (suite)

- *Cette commande ne vous dit pas ce que devraient être votre adresse IP et votre masque de sous-réseau ; elle dit seulement quelle adresse IP et quel masque de sous-réseau votre machine utilise.*
- *C'est à vous de vérifier que les paramètres d'adressage sont cohérents avec le schéma d'adressage IP de votre réseau*
  - *Exemple: on peut découvrir que la machine n'a pas du tout d'adresse IP, ce qui indiquerait un problème de connexion avec le serveur DHCP*
- ipconfig /flushdns Efface le contenu du cache de résolution du client DNS
  - *Cette commande pourrait être utile en cas de problèmes de résolution de noms*

Commandes réseau: Ping

- La commande ping permet d'envoyer des messages à un serveur qui peut en retour répondre.
- Cela permet de tester la connectivité à ce serveur.
  - *Il est cependant possible que le serveur n'accepte pas ces messages, via des règles de pare-feu/firewall et ne répondent pas alors que la connexion vers ce dernier est possible.*
- La syntaxe est: ping adresseDuServeur
- Si vous indiquez une adresse littérale, la commande ping va résoudre l'adresse, ce qui permet de tester les résolutions DNS :

```
C:\Users\dhaouari>ping www.google.ca

Envoi d'une requête 'ping' sur www.google.ca [216.58.219.227] avec 32 octets de données :
```

Commandes réseau: Ping (suite)

- Par défaut, la commande ping envoie 4 paquets, vous avez à chaque fois la réponse avec le délai.
  Puis un récapitulatif des statistiques avec les paquets réussies ou perdus s'affichent.
  Lorsque la connexion ne se fait pas, à cause d'un problème réseau ou parce que le serveur en face refuse ces demandes, ping retourne le message :

  Le délai d'attente est dépassé

- Si tous les paquets sont rejetées ou perdus, vous obtenez 100% de pertes.

```
C:\Users\dhaouari>ping www.malekal.com

Envoi d'une requête 'ping' sur ns206195.ovh.net [94.23.44.69] avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.

Statistiques Ping pour 94.23.44.69:
    Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),
```

Commandes réseau: tracert

- tracert permet de suivre les chemins qu'un paquet IP va prendre pour aller de la machine locale à une autre machine connectée au réseau IP.
- Les paquets IP sont acheminés vers la destination en passant d'un routeur à un autre. Chaque routeur examine sa table de routage pour déterminer le routeur suivant.
- tracert va permettre d'identifier les routeurs empruntés, indiquer le délai entre chacun des routeurs et les éventuelles pertes de paquets.
- La commande à saisir est :

  tracert adresseDuServeur

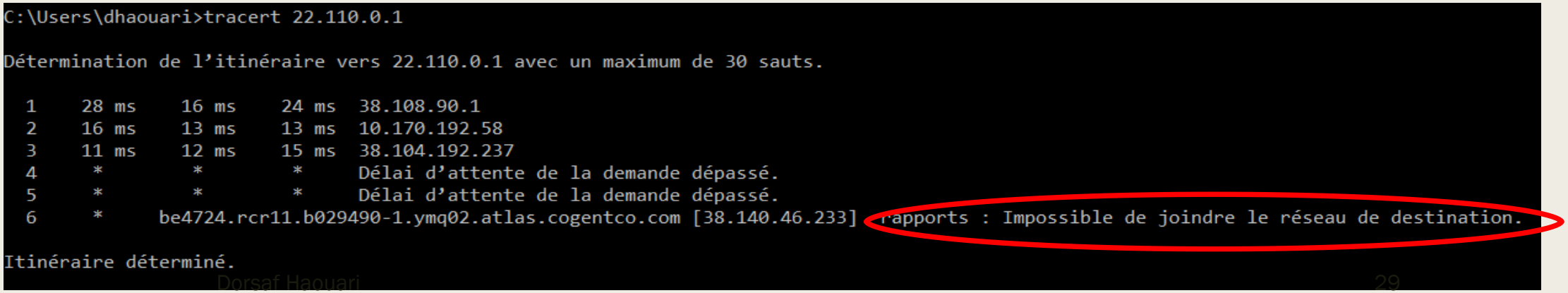
Commandes réseau: tracert (suite)

- Exemple d'une route empruntée pour atteindre www.google.com

```
C:\Users\dhaouari>tracert www.google.com

Détermination de l'itinéraire vers www.google.com [172.217.6.228]
avec un maximum de 30 sauts :

  1    13 ms    14 ms    13 ms  38.108.90.1
  2    13 ms    14 ms    14 ms  10.170.192.58
  3    15 ms    11 ms    14 ms  38.74.23.193
  4    15 ms    13 ms    11 ms  be4724.rcr11.b029490-1.ymq02.atlas.cogentco.com [38.140.46.233]
  5    16 ms    16 ms    12 ms  be3501.rcr21.ymq02.atlas.cogentco.com [154.54.1.85]
  6    20 ms    23 ms    12 ms  tata.ymq02.atlas.cogentco.com [154.54.10.206]
  7    22 ms    23 ms    20 ms  209.85.149.230
  8    27 ms    22 ms    21 ms  108.170.251.21
  9    27 ms    25 ms    27 ms  108.170.235.210
 10    22 ms    23 ms    21 ms  216.239.54.206
 11    27 ms    23 ms    25 ms  108.170.248.1
 12    24 ms    36 ms    25 ms  108.170.237.209
 13    26 ms    24 ms    26 ms  lga25s55-in-f4.1e100.net [172.217.6.228]

Itinéraire déterminé.
```

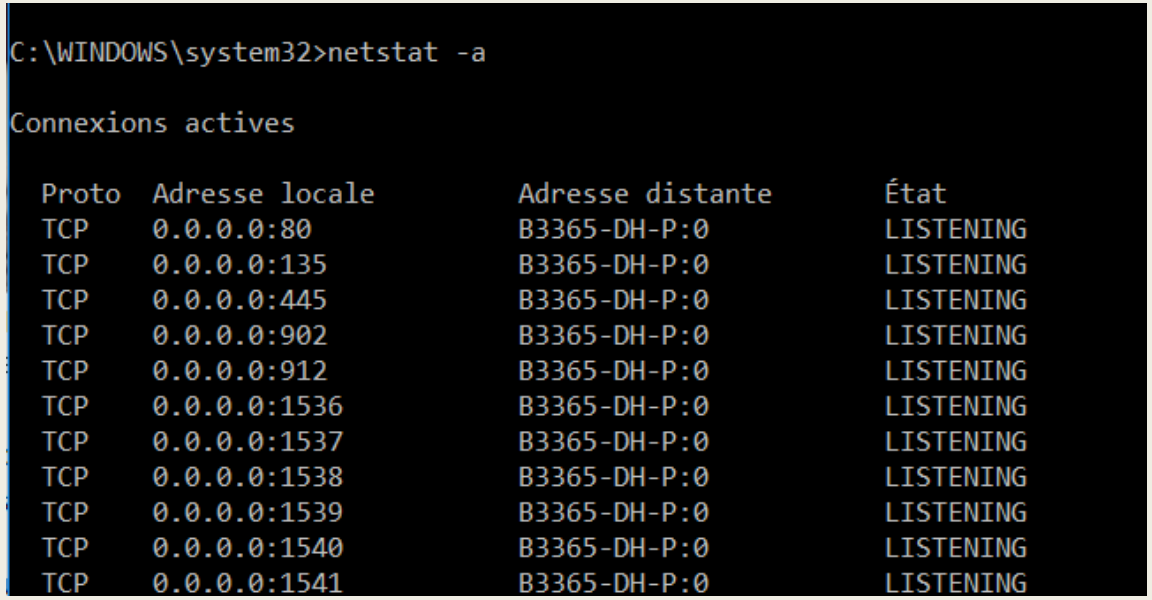
Commandes réseau: tracert (suite)

- Les informations de tracert seront utiles pour diagnostiquer les problèmes sur un des liens vers la destination.
- Exemple:
  - *Vous pouvez utiliser TRACERT pour déterminer où un paquet s'est arrêté sur le réseau.*
  - *Dans l'exemple suivant, le routeur de cogent a déterminé qu'il n'existe pas de chemin valide pour l'hôte sur 22.110.0.1.*
  - *On peut supposer qu'il existe un problème de configuration du routeur ou que le réseau 22.110.0.0 n'existe pas (adresse IP incorrecte).*



Commandes réseau: netstat

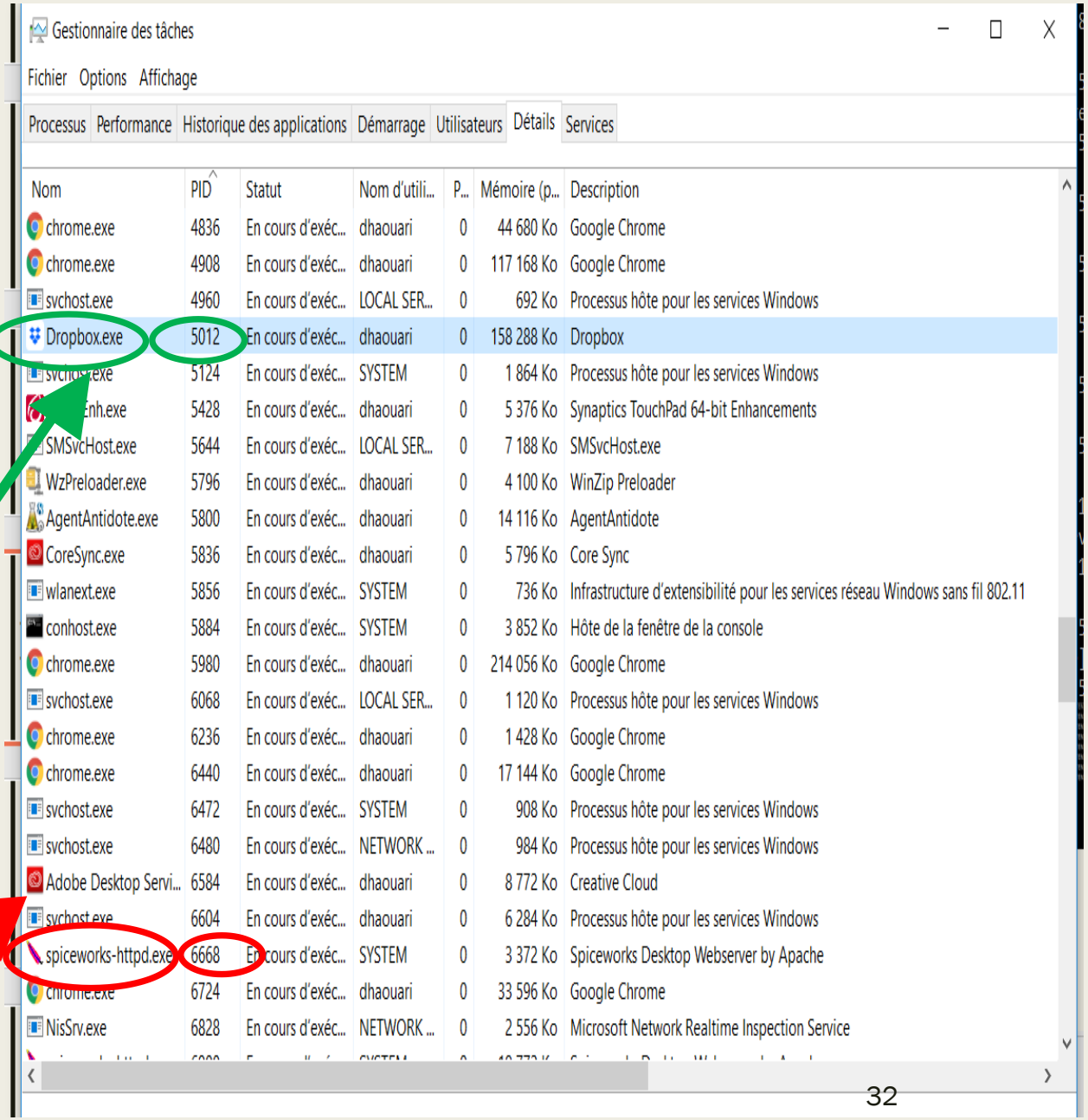
- Netstat peut donner les statistiques par interfaces réseaux et par protocole.
- Netstat –a permet de lister les connexions actives ainsi que les ports en écoute
- Le nombre après les deux points, indique le nombre du port utilisé par la connexion



Commandes réseau: netstat (suite)

- Netstat –ab permet d'afficher l'exécutable impliqué dans la création de chaque connexion ou port d'écoute
- L'option -o permet d'ajouter une colonne PID.
  - *Ainsi vous pouvez savoir à quel processus est lié la connexion depuis le gestionnaire de tâches de Windows.*
- Exemple:
  - *Voire diapositive suivante*

```
 TCP    0.0.0.0:3389           B3365-DH-P:0           LISTENING       1312
 TermService
[svchost.exe]
 TCP    0.0.0.0:5040           B3365-DH-P:0           LISTENING       11576
 CDPSvc
[svchost.exe]
 TCP    0.0.0.0:9675           B3365-DH-P:0           LISTENING       6668
[spiceworks-httpd.exe]
 TCP    0.0.0.0:9676           B3365-DH-P:0           LISTENING       6668
[spiceworks-httpd.exe]
 TCP    0.0.0.0:17500          B3365-DH-P:0           LISTENING       5012
[Dropbox.exe]
 TCP    0.0.0.0:62354          B3365-DH-P:0           LISTENING       3892
[perl.exe]
```



Commandes réseau: netstat (suite)

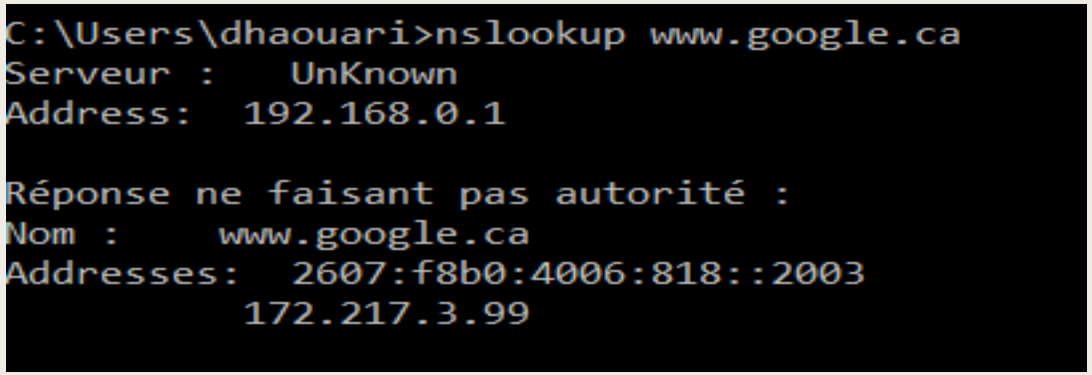
- netstat –e affiche des statistiques Ethernet
  - Les lignes Erreurs et Rejets sont intéressantes, car elles indiquent, si l'interface rencontre des problèmes.
  - Leur valeur doit être à 0 ou proche de 0. Sinon, cela est anormale,
  - Un nombre élevé d'erreurs dans la colonne Émis indique:
    - Réseau local surchargé
    - Problème au niveau de la connexion physique entre le hôte local et le réseau
  - Un nombre élevé d'erreurs dans la colonne Reçus indique:
    - Réseau local surchargé
    - Problème au niveau de la connexion physique entre le hôte local et le réseau
    - Hôte local surchargé

```
C:\WINDOWS\system32>netstat -e
Statistiques de l'interface

                           Reçus            Émis

Octets                  803336765        87336808
Paquets monodiffusion      533911          338732
Paquets non monodiffusion  2339078          12891
Rejets                          0               0
Erreurs                         0               0
Protocoles inconnus             0
```

Commandes réseau: nslookup

- nslookup est une commande qui permet de tester les résolutions DNS.

- Pour effectuer une résolution DNS, il suffit de saisir une adresse littérale :



- Les deux premières lignes affichent les informations du serveur DNS configuré localement