# Fiche savoirs : Incidents réseau

## Principes généraux

Lors de la remontée d’un incident réseau, on fait une première analyse :

* nombre d'utilisateurs impactés ? Si plusieurs, il peut s'agir d'un incident d'infrastructure réseau (switch, routeur, serveur, accès internet…) ;
* incident persistant ou intermittent ? Si intermittent, plus difficile à diagnostiquer ;
* déconnecter un ordinateur problématique règle-t-il le problème pour les autres ?

En général, on suit le modèle OSI des couches basses vers les couches hautes pour trouver l'origine du problème :

|  |  |
| --- | --- |
| 1 Couche physique |  |
| 2 Couche liaison de données |  |
| 3 Couche réseau |  |
| 4 Couche transport |  |
| 5,6,7 Couche des protocoles applicatifs |  |

## Etapes de résolution

### Vérifier les connexions physiques

Valider les branchements et le brassage en contrôlant les voyants (leds) du côté de la carte réseau et des switchs :



Valider les câbles avec un testeur de câble. Par exemple, avec un testeur de câble basique :

Des outils plus sophistiqués existent :


### Vérifier le bon fonctionnement du (des) pilote(s) de carte réseau

Il s'agit de vérifier que le pilote fonctionne correctement, éventuellement retrouver la version afin de voir chez le constructeur s'il n'y a pas une mise à jour : utiliser le « gestionnaire de périphériques ».

**Vérifier la configuration IP locale**

En ligne de commandes :

c:\>

c:\> … pour conserver les paramètres dans un fichier texte

c:\> netsh …

L'objectif est de retrouver :

— adresse MAC :

— configuration IP en DHCP ou statique :

— adresse IP :

— masque réseau :

— nom d'hôte :

— configuration DNS (serveurs, suffixes) :

— passerelle :

Comparez avec la configuration d'une machine, située dans le même VLAN, qui fonctionne correctement et surveillez que :

— le début de l'adresse IP est similaire ;

— le masque réseau est similaire (penser aux sous-réseaux IP) ;

— la passerelle par défaut (début de l'adresse IP est similaire avec la machine) sinon communication impossible avec les autres sous-réseaux IP et internet ;

— le serveur DNS car si absent ou incorrect, la résolution de nom ne fonctionne pas et la communication échoue dans la plupart des cas.

Si DHCP : en tant qu'administrateur, utiliser les commandes pour renouveler la configuration IP :

ipconfig …

ipconfig …

**Attention**

**Si l'hôte possède une IP 169.254.x.x il y a un problème de ?**

### Vérifier la connectivité réseau

Les divers pare-feu peuvent être à la source de différents problèmes. À surveiller !

Ping à réaliser :

— ping avec … ;

— ping avec … ;

— ping avec … ;

— ping avec … ;

— ping avec … ;

— ping avec ...

Points à retenir :

— de chaque machine vers l'autre. Si blocage sur une seule des deux machines : ? ;

— ping sur l'IP fonctionne mais pas sur le nom : ? ;

— réponse "request timed out" : ? ;

— réponse "destination host unreachable" : ?

### Identifier la route

Utiliser les commandes pathping et tracert (pathping est plus précis sur les statistiques) pour déterminer à quel niveau la connectivité est rompue.

Accéder à la documentation de pathping pour déterminer les paramètres permettant :

* de ne pas tenter de résoudre les adresses IP des routeurs en leurs noms (afficher uniquement les IP)
* utiliser uniquement IPv4

### Vérifier la configuration DNS

— Contrôler le fichier hosts (c:\windows\system32\drivers\etc\hosts) ;

— Utiliser nslookup ;

— Purger le cache DNS avec ipconfig /flushdns.

### Vérifier l'accessibilité des ports TCP/uDP

#### En local

Sur la machine accueillant le service réseau en question, la commande netstat -n peut indiquer si le service est en écoute, sur quel port et sur quel protocole (TCP, UDP) :

C:\> netstat -n

Connexions actives

Proto Adresse locale Adresse distante État

TCP 127.0.0.1:1048 127.0.0.1:1049 ESTABLISHED

TCP 127.0.0.1:1049 127.0.0.1:1048 ESTABLISHED

TCP 127.0.0.1:3286 127.0.0.1:3287 ESTABLISHED

TCP 127.0.0.1:3287 127.0.0.1:3286 ESTABLISHED

TCP 127.0.0.1:3290 127.0.0.1:3291 ESTABLISHED

TCP 127.0.0.1:3291 127.0.0.1:3290 ESTABLISHED

TCP 192.168.1.101:3679 192.168.1.115:80 SYN\_SENT

TCP 192.168.1.101:3680 192.168.1.115:80 SYN\_SENT

#### À distance

Activez le client telnet si nécessaire :

* Dans Programmes et fonctionnalités, Activez la fonctionnalité Windows Client Telnet

Telnet : un usage « détourné » de cette commande permet de vérifier la connectivité avec un port TCP (ne fonctionne pas avec UDP). Si cela fonctionne correctement, en général le service distant (en fonction du protocole) affiche un message rapidement. Par exemple :

|  |
| --- |
| C:\> telnet smtp.orange.fr 25Trying 193.252.22.64… Connected to smtp.orange.fr.Escape character is '^]'.220 mwinf5d29 ME ESMTP server ready |

Sinon, on n'obtient aucune réponse (firewall intermédiaire) ou :

C:\> telnet 192.168.1.1 654

Trying 192.168.1.1…

telnet: Unable to connect to remote host: Connection refused

Portqry (à télécharger chez Microsoft, équivalent de nmap sur Linux) : vérifie à distance les ports UDP/ TCP ouverts sur une machine. Pour chaque port :

— "listening" : le port est ouvert et accessible ;

— "not listening" : aucun processus n'est à l'écoute sur ce port du système cible ;

— "filtered" : aucune réponse de l'hôte mais portqry.exe a reçu un message ICMP "Destination inaccessible - Port inaccessible" si le port est UDP, sinon il a reçu une réponse TCP "reset".

|  |  |
| --- | --- |
|  |  **EXEMPLE**C:\> portqry -n 172.30.254.2 -p tcp -e 80La réponse pourrait être :TCP port 80 (http service): LISTENING |
|  |

Installez PortQry et vérifiez les ports ouverts sur un serveur.

### Wi-Fi

Si le réseau est disponible dans les "réseaux sans fil", vérifier les méthodes de chiffrement et d'authentification. Contrôler le SSID ainsi que les paramètres suivants :

|  |  |  |
| --- | --- | --- |
| **Type de sécurité** | **Authentification** | **Chiffrement** |
| Open | Aucune | Aucune |
| Shared (WEP pas recommandé) | Aucune | Clé partagée |
| WPA-Personal | Aucune | Clé partagée (passphrase)TKIP (Temporal Key Integrity Protocol) |
| WPA-Enterprise | 802.1x | TKIP |
| WPA2-Personal | Aucune | Clé partagée (passphrase)CCMP (AES) |
| WPA2-Enterprise | 802.1x | CCMP (AES) |

**Attention il est possible d’empêcher la diffusion du SSID sur le point d’accès.**