





# Cahier de débogage en réseaux

Tout comme la programmation, la configuration des réseaux informatique demande certaines capacités de débogage, pour comprendre les problèmes possibles qui se sont présentés et améliorer la situation.

Dans ce cahier le but sera d'apprendre comment déboguer des situations particulières : les démarches à faire pour diagnostiquer le problème, l'interprétation des résultats, ainsi que des démarches d'amélioration possibles.

Tout au long des ressources R2.04 et R2.05, vous allez remplir ce cahier en trouvant :

- des symptômes 
- des outils de débogage 
- des erreurs fréquentes 
- des améliorations à apporter 

## Problème de configuration d'adresse IP

Une des compétences de base à acquérir en réseaux est la configuration d'une adresse IP.

### Symptômes

Nous avons configuré une adresse IP sur une machine.

Mais, un ping de la part d'une machine du même réseau ne semble pas aboutir.

Que faire ?

### Outils de diagnostic

Si le ping qui n'aboutit pas alors qu'il provient d'une machine dans le même réseau, alors le problème ne peut jamais être le routage (on n'a pas besoin d'un routeur pour échanger des messages au sein d'un même réseau. Le problème doit être au niveau de la configuration des adresses IP des deux machines (la source ou la destination du ping).

Comment peut-on trouver le problème

1. Visualiser la configuration IP de toutes les interfaces des deux machines. Commande :

2. Visualiser les configurations des interfaces actives sur les deux machines. Commande :


3. Si une configuration pérenne a été mise en place, visualiser la configuration. Elle est dans quel fichier ?

4. [Problème Kathará] Visualiser si les deux machines sont dans un même réseau sur Kathará. Quel fichier faut-il vérifier et quelle doit être la configuration dans ce cas-ci ?

5. [Problème Kathará] Visualiser si la configuration IP des deux machines a été réalisée correctement dans les fichiers de startup. Quels fichiers faut-il regarder ?

## Trouver le problème

Voici quelques erreurs très fréquentes (et comment vous pouvez confirmer qu'elles sont à la base de votre problème de connectivité), ainsi que des solutions possibles :

 1. L'interface a été configurée mais n'est pas active.

Comment puis-je confirmer ce diagnostic en utilisant les outils ci-dessus ?

✿ Solution : comment remédier la situation (Commande) :

- ⚠ 2. Oubli de CIDR lors de la configuration IP. Vous avez tapé :
- ```
ip address add <adresse> dev <interface>
```

Comment puis-je confirmer ce diagnostic en utilisant les outils ci-dessus ?

✿ Solution : comment remédier la situation (Commande) :


- ⚠ 3. Vous avez bien configuré des adresses avec des CIDR mais les deux machines ne se trouvent pas dans le même réseau.


Comment confirmer ce diagnostic avec les outils ci-dessus ?


✿ Solution : comment remédier la situation (Commande) :

- ⚠ 4. Configuration pérenne incorrecte. Si l'adresse ou le masque sont incorrectes, la configuration échouera.


Comment confirmer ce diagnostic avec les outils ci-dessus ?


 5. Configuration pérenne correcte, mais non-activée.

 Solution : comment remédier la situation :

 6. Problème de configuration Kathará : vous avez mis les machines dans deux domaines de collision différents.

Comment confirmer ce diagnostic avec les outils ci-dessus ?

 Solution : comment remédier la situation :

 7. Problème de configuration Kathará : la configuration réalisée dans le fichiers de startup est incorrecte.

Comment confirmer ce diagnostic avec les outils ci-dessus ?

## Problème de connectivité entre sous-réseaux configurées

Une fois la connectivité intra-réseau acquise, le prochain défi est de pouvoir faire communiquer entre elles deux machines appartenant à des réseaux différents.

Plusieurs types de symptômes peuvent se présenter, mais en général les outils de débogage pour des problèmes de connectivité sont les suivantes :

### Outils de diagnostic

Un problème de connectivité inter-réseau relève en général de deux types de problèmes : un problème de configuration de la machine, ou un problème de routage.

Les outils déjà discutés dans la section précédente peuvent bien-sûr être utilisés pour diagnostiquer un problème de configuration d'adresse IP, soit d'un côté soit de l'autre.


Ici, nous allons rajouter quelques outils à utiliser :

1. Visualiser les routes configurées sur chaque machine. Commande :
2. Utilisation d'un logiciel comme Wireshark pour diagnostiquer le problème. Quel filtre faut-il utiliser pour une capture Wireshark ?
3. Utilisation de pings entre des machines. Une tentative de ping peut avoir plusieurs résultats. Le ping peut ne pas partir, peut partir sans retourner, ou partir et revenir.  
Commande à utiliser :


### Le ping ne part pas

Deux machines sont configurées, dans deux réseaux différents.

Quand je fais un ping de l'une vers l'autre, j'ai un message d'erreur disant Network Unreachable.

 Dans ce cas, sauf erreur de configuration IP, le problème est toujours le manque d'une route sur la machine à partir de laquelle on a envoyé le ping. Le ping ne part pas car il n'y a pas de route configurée.


Comment confirmer ce diagnostic avec les outils ci-dessus ?

 Solution : comment remédier la situation :


 [RTNETLINK : Network unreachable](#)

Une machine est configurée avec une adresse IP. Je veux lui rajouter une route par défaut. Lorsque je tape la commande correcte pour ajouter la route, j'ai le message d'erreur suivant :

```
RTNETLINK answers : Network is unreachable
```

 Dans ce cas, le problème provient de l'incompatibilité entre l'adresse IP de la machine et celle du routeur par défaut. Si les deux adresses n'appartiennent pas au même réseau, alors il y aura cette erreur.


Comment confirmer ce diagnostic avec les outils ci-dessus ?

 Solution : comment remédier la situation :

## Ping part, ne revient pas

Deux machines sont configurées, dans deux réseaux différents.

Quand je fais un ping de l'une vers l'autre, je vois le ping partir mais il ne revient pas. Pour l'instant on va supposer que la machine cible du ping n'est pas sur Internet : les deux machines se trouvent dans des sous-réseaux sous notre contrôle.


 Si le ping part, alors une passerelle a été configurée pour la machine source. Le ping se perd quelque part dans son aller-retour, et donc le premier pas est d'identifier le point d'arrêt.

Pour identifier le problème, il est indispensable de comprendre la route que le ping doit emprunter : il est donc judicieux de lister les étapes de transmission et d'examiner chaque segment de la route.

**Comment trouver le point d'arrêt avec les outils ci-dessus ?**

En fonction du point d'arrêt, la cause du manque de connectivité diffère, ainsi que la solution potentielle. Une première cause peut être la mauvaise configuration d'une machine sur la route par rapport à son/ses adresses(s) IP (première partie de ce cahier). Mais quelles autres causes peut-on trouver ?

Voici quelques possibilités :

 1. Route mal-configurée ou non-configurée à l'aller.

**Quels résultats de l'utilisation des outils de dépannage ci-dessus peuvent nous faire penser à ce type de problème ?**

✿ Solution : comment remédier la situation :

⚠ 2. Route mal configurée ou non-configurée au retour.

Quels résultats de l'utilisation des outils de dépannage ci-dessus peuvent nous faire penser à ce type de problème ?

✿ Solution : comment remédier la situation :

⚠ 3. Manque de ip\_forward

Quels résultats de l'utilisation des outils de dépannage ci-dessus peuvent nous faire penser à ce type de problème ?


✿ Solution : comment remédier la situation (commande) :



## Message ICMP : TTL expired (dépassement TTL)

Deux machines sont configurées, dans deux réseaux différents.

Quand je fais un ping de l'une vers l'autre, je vois le ping partir mais il ne revient pas. Je regarde sur Wireshark pour me rendre compte qu'est-ce qui se passe et je note la présence d'un message ICMP déclarant un dépassement de TTL.

 Une message de TTL dépassé signifie le fait que le routage actuel n'a pas pu mener le ping à sa destination dans le TTL permis (souvent 64 sauts). Cela peut indiquer l'isolement du réseau de destination du ping, mais également un routage cyclique quelque part entre les deux machines.

## Problème de connectivité Internet


Une fois les machines de nos sous-réseaux configurées, nous pouvons vouloir les connecter à Internet. Cette démarche peut engendrer ses propres problèmes.


Nous allons supposer que toutes les machines et les routes nécessaires sont bien configurées.

Plusieurs types de symptômes peuvent apparaître.

## Route OK, ping KO


Un ping 8.8.8.8 sur une machine que nous avons configurée n'aboutit pas. Un ping entre notre machine et la passerelle qui fait la connexion Internet aboutit bien. Le ping entre la passerelle qui fait la connexion Internet aboutit bien aussi. Le ip\_forward est correctement réalisé sur chaque passerelle.

 En général cela indique un manque de masquerade à la sortie d'un réseau privé.


 **Solution : comment remédier la situation (commande) :**

 Accès par IP OK, accès par nom KO

Une machine arrive à faire un ping 8.8.8.8, mais elle n'arrive pas à faire ping [www.google.fr](http://www.google.fr).


 Clairement le problème se situe au niveau de la résolution de nom de domaine. Plusieurs situations sont possibles : par exemple, un manque de route ou un manque de configuration sur notre machine pour la résolution de nom

Comment peut-on savoir si le souci provient d'un problème de routage ?

 Si le problème est un manque de configuration de résolution de nom comment peut-on remédier la situation ?

 Problèmes sur apt-update

Sur une machine, nous voulons utiliser apt-update pour une (re-)mise à jour. Toutefois, la commande apt-update aboutit dans une erreur qui semble indiquer une impossibilité de joindre le site de mises à jour.

 Celle-ci est une manifestation alternative du même problème discuté ci-dessus sur la résolution de nom. Les mêmes diagnostics et solutions s'imposent

## Problème d'installation/utilisation d'un service

Une dernière compétence à acquérir dans le cadre des ressources R2.04 et R2.05 est l'installation de base de certains services, notamment DHCP mais également des services de type HTTP ou FTP.

Pour la mise en place des services, en plus des problèmes qui peuvent apparaître à cause de la mauvaise configuration des machines et/ou du routage, on sera confrontés à des difficultés supplémentaires, qui demanderont des outils spécifiques de diagnostic

## Outils de diagnostic

L'installation et la mise à disposition d'un service sur une machine arrive en plusieurs étapes. À chaque pas, des vérifications doivent être mises en place pour pouvoir repérer, déboguer et corriger des éventuels problèmes.

Voici quelques outils qui peuvent s'avérer utiles pour ce débogage :

1. DHCP : vérification de la configuration sans démarrage du service. Commande :

2. Vérification d'un démarrage correct pour un service. Commande avec différenciation de paramètres par type de protocole de couche 4 :

3. Trouver l'adresse MAC sur une machine. Commande :

4. Le service DHCP a démarré. Comment essayer d'avoir une adresse dynamiquement ? Et si on veut renouveler l'adresse ?


5. Utilisation de Wireshark : Quels filtres utiliser pour les messages pertinents à la navigation Web ? Et l'adressage dynamique ?

 Service configuré et démarré, ne fonctionne pas

Un service est configuré et on a démarré le serveur. Mais, lorsqu'on essaie de l'utiliser il ne fonctionne pas. Qu'est-ce qui se passe ?


Le diagnostic dans ce cas n'est pas évident, et le but de cette partie du cahier est de confirmer un diagnostic plutôt que de trouver des solutions immédiates (la solution se trouve en général dans le débogage et la modification de la configuration du service).

Voici quelques causes potentielles.


 Le serveur n'est pas à l'écoute.

Comment peut-on savoir si le serveur est à l'écoute ?

Quelle différence entre l'utilisation du paramètre -a plutôt que -n en termes d'affichage du service pour la commande ss (et quelle conséquence pour le diagnostic en question) ?

 Le serveur est à l'écoute, mais sur un autre port que celui habituel.

Comment peut-on confirmer l'état d'écoute et trouver le port ?

 Pour le service DHCP, notre machine ne réussit pas à se connecter, car la configuration pérenne ne figure que des adresses et routes statiques.

Comment peut-on confirmer ce diagnostic ?


 Comment peut-on assurer une configuration pérenne qui permet l'adressage dynamique ?

## Problèmes d'adressage ou de routage en DHCP


Un serveur DHCP est mis en place. Il a démarré correctement.


Une machine dans ce réseau est configurée pour recevoir des adresses dynamiquement. Mais, lorsqu'on fait un ping 8.8.8.8 le ping ne marche pas.

Clairement, plusieurs problèmes peuvent causer ce comportement. Voyons quelques possibilités.


 La durée du bail de l'adresse est trop courte ou la plage d'adresses est trop petite pour accueillir notre machine.


Comment peut-on confirmer ce diagnostic ?

 Quel(s) fichier(s) faut-il modifier pour améliorer la situation ? Quel est le fichier à modifier et dans quelles lignes faut-il faire la modification ?

 La configuration DHCP permet à la machine de recevoir une adresse correctement mais aucun routeur n'est indiqué dans la configuration.

Comment peut-on confirmer ce diagnostic à partir de la machine client DHCP ?

 Comment peut-on améliorer la configuration ? Donnez le fichier à modifier et les modifications à apporter !

 La configuration DHCP permet à la machine de recevoir une adresse correctement et un routeur fonctionnel est indiqué. Sauf que le routeur prend son adresse en DHCP et son adresse change ponctuellement.

Comment peut-on confirmer ce diagnostic ?



Comment peut-on améliorer la configuration ? Donnez le fichier à modifier et les modifications à apporter !



La configuration DHCP est correcte, l'adressage et le routage est correct. Le problème provient du routage, qui n'est pas réalisé correctement.

Comment peut-on confirmer ce diagnostic ?