PEREZ Lorette

BARAHONA Andrea

**Démarche de dépannage réseau ou troubleshooting.**

(équipements, interconnexion)

1. Éteindre et rallumer les composants à proximité : la machine en question, un routeur secondaire …
   1. Redémarrer l’équipement à proximité (qui ne met pas en enjeu le fonctionnement de l’infrastructure).
   2. Arrêter complètement l’équipement pendant quelques minutes, puis le rallumer. Si l’erreur est toujours présente, passer à la suite.
2. Vérifier le câblage : est-il défectueux ? Est-il bien branché ? Si besoin, vérifier la qualité des câbles et s’ils sont fonctionnels: brancher, débrancher. S’ils sont défectueux, les remplacer.

Dans le cadre d’une prestation, nous pouvons recourir à l’utilisation des **multimètres** afin de vérifier la connectivité physique. Ils se situent à l'extrémité inférieure de la gamme des outils de test de câbles. Ces appareils mesurent des paramètres tels que la tension AC et DC, le courant, la résistance, la capacité et la continuité du câble.

Les testeurs de câbles (scanners) permettent également de vérifier la connectivité physique. Ils sont disponibles pour les paires torsadées blindées (STP), paires torsadées non blindées (UTP), 10BaseT, câbles coaxiaux et les câbles twinax. Un testeur de câble donné peut être capable de remplir l'une des fonctions suivantes :

* Tester et faire un rapport sur les conditions du câble, y compris la diaphonie proche (NEXT), l'atténuation et le bruit.
* Effectuer des fonctions TDR, de surveillance du trafic et de cartographie des câbles.
* Afficher les informations de la couche MAC (Media Access Control) sur le trafic du réseau local, fournir des statistiques telles que l'utilisation du réseau et le taux d'erreur des paquets, ainsi que d’effectuer des tests de protocole limités (par exemple, des tests TCP/IP tels que le ping).

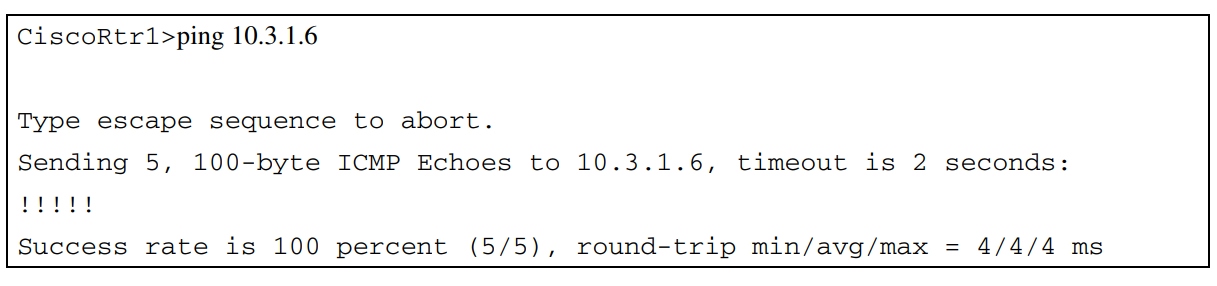
Des équipements de test similaires sont disponibles pour les câbles à fibres optiques. En raison du coût relativement élevé de ce câble et de son installation, le personnel chargé d’installer un câble à fibre optique doit le tester à la fois avant l'installation (test sur la bobine) et après l'installation. Le test de continuité de la fibre nécessite une source de lumière visible et tester l'atténuation et la perte de retour dans la fibre.

1. Troubleshooting des ports :
   1. **Le statut du port ou de l'interface est désactivé ou arrêté :** le statut du port ou de l'interface est désactivé ou arrêté. Une cause évidente, mais parfois négligée, de l'échec de la connectivité d'un port est une configuration incorrecte du commutateur. Si un port a un voyant orange fixe, cela signifie que le logiciel du commutateur a désactivé le port, soit par l'intermédiaire de l'interface utilisateur, soit par des processus internes**.** Il faut utiliser la commande “**show run interface**” et vérifiez si l'interface est en état d'arrêt.
   2. **L'état du port ou de l'interface est errDisable** :par défaut, les processus logiciels à l'intérieur du commutateur peuvent arrêter un port ou une interface si certaines erreurs sont détectées. Utilisez la commande “**show interface card-type {slot/port} status”** pour vérifier l’état du port.

**AU NIVEAU DES ORDINATEURS/SERVEURS :**

* 1. Les ordinateurs peuvent-ils se “ping” mutuellement ?

Pour le protocole IP, la commande ping envoie des messages d'écho ICMP (Internet Control Message Protocol). ICMP est le protocole Internet qui signale les erreurs et fournit des informations relatives à l'adressage des paquets IP. Dans le cas où deux ordinateurs n’arrivent pas à se pinger, il faudrait effectuer la commande “**tracert**” pour suivre le chemin emprunté par le paquet IP pour arriver à sa destination. Ensuite, il faudrait identifier où le paquet se perd, et pousser les analyses à ce niveau.



Codes de retour suite à un ping ping:

| Code | Signification | Causes possibles |
| --- | --- | --- |
| ! | Chaque point d'exclamation indique la réception d’un ICMP “echo reply”. | Le ping s'est terminé avec succès. |
| . | Chaque point indique que le serveur du réseau a dépassé le temps d'attente d'une réponse. | Ce message peut indiquer plusieurs  problèmes :  - Le ping a été bloqué par une liste d'accès ou un pare-feu.  - Un routeur le long du chemin n'a pas  n'avait pas de route vers la destination et n'a pas envoyé  un message ICMP  de “destination unreachable”.  - Un problème de connectivité physique  s'est produit quelque part le long du chemin. |
| U | Un message ICMP “unreachable” a été  reçu. | Un routeur le long du chemin n'avait pas la route définie vers l'adresse de destination. |
| C | Un message “source quence” ICMP a été reçu. | Un dispositif le long du  chemin - peut-être la  destination - reçoit peut-être trop de trafic ; vérifiez les files d'attente d'entrée. |
| & | Un message ICMP de “time exceeded” a été reçu. | Une boucle de routage peut s'être produite. |

* 1. Vérifier que chaque composant a bien son ip attribuée et que les interfaces sont bien “up” : on peut entrer la commande “show interfaces” ou “**show interfaces status**” pour vérifier ceci, mais également “**show running-config**” pour avoir un petit rapport descriptif pour chaque interface.

**AU NIVEAU DU ROUTEUR :**

* 1. Entrer la commande “**show version**” et vérifier que le composant est à jour.
  2. La commande “**show ip interface brief**” est utile au niveau de tous les composants pour vérifier la configuration des interfaces, s’il s’agit des bonnes adresses IP, masques de sous réseau et gateway.
  3. Entrer la commande “**show running-config**”
     1. PROTOCOLE OSPF : vérifier dans la configuration et via la commande “**show ip protocols**” si le protocole est activé. S’il l’est, on peut d’ores et déjà entrer la commande “**show ip route**” pour voir si des routes dynamiques ont été créées par OSPF. Si besoin, on peut rentrer la commande “**show ip ospf neighbor**” pour vérifier que les routeurs se reconnaissent entre eux.
     2. S’agit-il d’un souci de configuration au niveau des access-lists ? Le vérifier en tapant “**show access-lists**”.
     3. Vérifier si la configuration relative à la redondance des interfaces peut poser souci : on peut entrer la commande “**show standby**” ou “**show standby brief**”.
  4. Entrer la commande “**show interfaces**” : les interfaces sont-elles bien configurées ?

**AU NIVEAU DU SWITCH**

* 1. Vérification au niveau du VLAN : entrer les commandes “**show interfaces vlan**” pour être sûrs que celle-ci est bien configurée, si une IP et un masque de sous-réseau est bien attribuée. Si plusieurs VLAN sont connectés via un port trunk, on peut vérifier leur connectivité avec la commande “**show interfaces trunk**”.
  2. Pour voir la liste des adresses mac apprises par le switch, il faut entrer la commande “**show mac-address table**” et voir s’il s’agit d’un souci à ce niveau.
  3. Vérifier la configuration du “**port security**” sur chaque interface.

**TROUBLESHOOTING DU SERVEUR DHCP :**

* 1. Dans le cas où les IP sont mal attribuées, entrer la commande “**show ip dhcp pool**” pour vérifier tous les pools d’adresse IP configurés, et ainsi voir s’il s’agit d’un souci de DHCP.

**Commandes supplémentaires à rentrer pour le troubleshooting réseau :**

* 1. Est-ce un souci relatif au protocole ipv6 ? On peut entrer la commande “**show ipv6 route**” pour vérifier la connectivité via ce protocole.
  2. Pour voir tous les fichiers stockés dans la NVRAM, on peut rentrer la commande “**show flash**:”