**ROYAUME DU MAROC**

مكتب التكوين المهني وإنعاش الشغل

**Office de la Formation Professionnelle et de la Promotion du Travail**

# Diagnostique des 7 Couches réseau
www.ofppt.info

OFPPT

**D**IRECTION **R**ECHERCHE ET **I**NGENIERIE DE **F**ORMATION

**SECTEUR NTIC**

# Sommaire

# 2. Rappel sur les sept couches OSI

Les constructeurs informatiques ont proposé des architectures réseaux propres à leurs équipements. Par exemple, IBM a proposé SNA, DEC a proposé DNA... Ces architectures ont toutes le même défaut : du fait de leur caractère propriétaire, il n'est pas facile des les interconnecter, à moins d'un accord entre constructeurs. Aussi, pour éviter la multiplication des solutions d'interconnexion d'architectures hétérogènes, l'ISO (International Standards Organisation), organisme dépendant de l'ONU et composé de 140 organismes nationaux de normalisation, a développé un modèle de référence appelé modèle OSI (Open Systems Interconnection). Ce modèle décrit les concepts utilisés et la démarche suivie pour normaliser l'interconnexion de systèmes ouverts (un réseau est composé de systèmes ouverts lorsque la modification, l'adjonction ou la suppression d'un de ces systèmes ne modifie pas le comportement global du réseau).

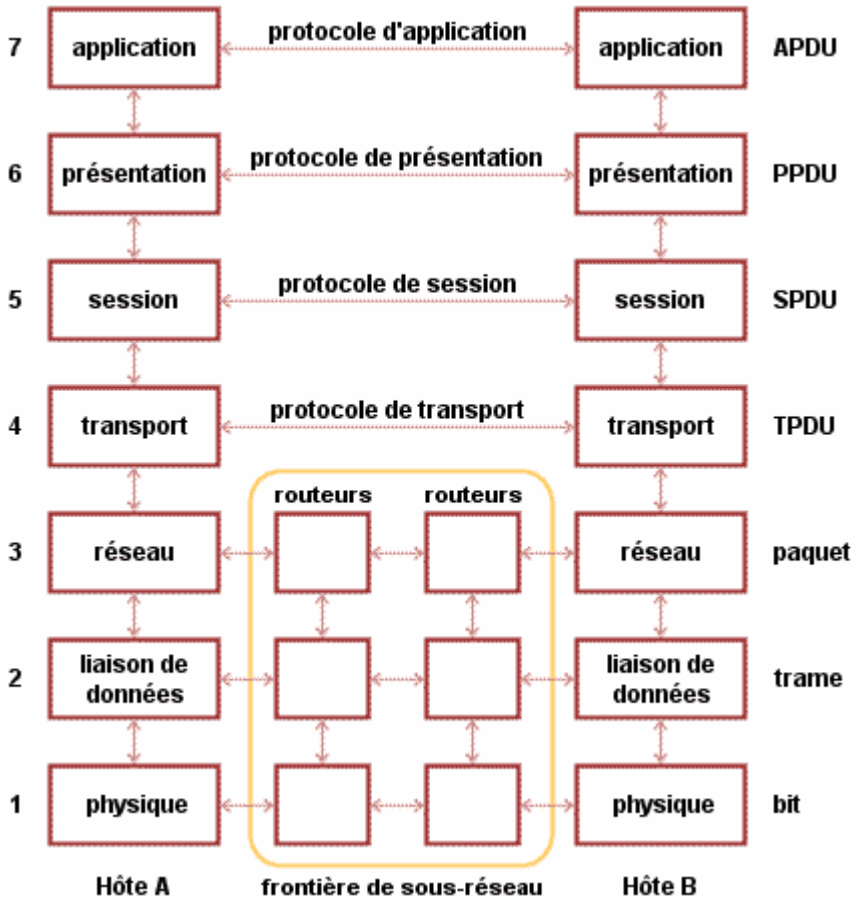
Au moment de la conception de ce modèle, la prise en compte de l'hétérogénéité des équipements était fondamentale. En effet, ce modèle devait permettre l'interconnexion avec des systèmes hétérogènes pour des raisons historiques et économiques. Il ne devait en outre pas favoriser un fournisseur particulier. Enfin, il devait permettre de s'adapter à l'évolution des flux d'informations à traiter sans remettre en cause les investissements antérieurs. Cette prise en compte de l'hétérogénéité nécessite donc l'adoption de règles communes de communication et de coopération entre les équipements, c'est à dire que ce modèle devait logiquement mener à une normalisation internationale des protocoles.

Le modèle OSI n'est pas une véritable architecture de réseau, car il ne précise pas réellement les services et les protocoles à utiliser pour chaque couche. Il décrit plutôt ce que doivent faire les couches. Néanmoins, l'ISO a écrit ses propres normes pour chaque couche, et ceci de manière indépendante au modèle, i.e. comme le fait tout constructeur.

Les premiers travaux portant sur le modèle OSI datent de 1977. Ils ont été basés sur l'expérience acquise en matière de grands réseaux et de réseaux privés plus petits ; le modèle devait en effet être valable pour tous les types de réseaux. En 1978, l'ISO propose ce modèle sous la norme ISO IS7498. En 1984, 12 constructeurs européens, rejoints en 1985 par les grands constructeurs américains, adoptent le standard.

## 2.1. 2 - Les différentes couches du modèle

### 2.1.1. 2.1 - Les 7 couches




Les principes qui ont conduit à ces 7 couches sont les suivants :

- une couche doit être créée lorsqu'un nouveau niveau d'abstraction est nécessaire, - chaque couche a des fonctions bien définies,

- les fonctions de chaque couche doivent être choisies dans l'objectif de la normalisation internationale des protocoles,

- les frontières entre couches doivent être choisies de manière à minimiser le flux d'information aux interfaces,

- le nombre de couches doit être tel qu'il n'y ait pas cohabitation de fonctions très différentes au sein d'une même couche et que l'architecture ne soit pas trop difficile à maîtriser.

Les couches basses (1, 2, 3 et 4) sont nécessaires à l'acheminement des

informations entre les extrémités concernées et dépendent du support physique. Les couches hautes (5, 6 et 7) sont responsables du traitement de l'information relative à la gestion des échanges entre systèmes informatiques. Par ailleurs, les couches 1 à 3 interviennent entre machines voisines, et non entre les machines d'extrémité qui peuvent être séparées par plusieurs routeurs. Les couches 4 à 7 sont au contraire des couches qui n'interviennent qu'entre hôtes distants.

### 2.1.2. La couche physique

La couche physique s'occupe de la transmission des bits de façon brute sur un canal de communication. Cette couche doit garantir la parfaite transmission des données (un bit 1 envoyé doit bien être reçu comme bit valant 1). Concrètement, cette couche doit normaliser les caractéristiques électriques (un bit 1 doit être représenté par une tension de 5 V, par exemple), les caractéristiques mécaniques (forme des connecteurs, de la topologie...), les caractéristiques fonctionnelles des circuits de données et les procédures d'établissement, de maintien et de libération du circuit de données.

L'unité d'information typique de cette couche est le bit, représenté par une certaine différence de potentiel.

### 2.1.3. La couche liaison de données

Son rôle est un rôle de "liant" : elle va transformer la couche physique en une liaison a priori exempte d'erreurs de transmission pour la couche réseau. Elle fractionne les données d'entrée de l'émetteur en trames, transmet ces trames en séquence et gère les trames d'acquittement renvoyées par le récepteur. Rappelons que pour la couche physique, les données n'ont aucune signification particulière. La couche liaison de données doit donc être capable de reconnaître les frontières des trames. Cela peut poser quelques problèmes, puisque les séquences de bits utilisées pour cette reconnaissance peuvent apparaître dans les données.

La couche liaison de données doit être capable de renvoyer une trame lorsqu'il y a eu un problème sur la ligne de transmission. De manière générale, un rôle important de cette couche est la détection et la correction d'erreurs intervenues sur la couche physique. Cette couche intègre également une fonction de contrôle de flux pour éviter l'engorgement du récepteur.

L'unité d'information de la couche liaison de données est la trame qui est composées de quelques centaines à quelques milliers d'octets maximum.

### 2.1.4. La couche réseau

C'est la couche qui permet de gérer le sous-réseau, i.e. le routage des paquets sur ce sous-réseau et l'interconnexion des différents sous-réseaux entre eux. Au moment de sa conception, il faut bien déterminer

le mécanisme de routage et de calcul des tables de routage (tables statiques ou dynamiques...).

La couche réseau contrôle également l'engorgement du sous-réseau. On peut également y intégrer des fonctions de comptabilité pour la facturation au volume, mais cela peut être délicat.

### 2.1.5. Couche transport

Cette couche est responsable du bon acheminement des messages complets au destinataire. Le rôle principal de la couche transport est de prendre les messages de la couche session, de les découper s'il le faut en unités plus petites et de les passer à la couche réseau, tout en s'assurant que les morceaux arrivent correctement de l'autre côté. Cette couche effectue donc aussi le réassemblage du message à la réception des morceaux.

Cette couche est également responsable de l'optimisation des ressources du réseau : en toute rigueur, la couche transport crée une connexion réseau par connexion de transport requise par la couche session, mais cette couche est capable de créer plusieurs connexions réseau par processus de la couche session pour répartir les données, par exemple pour améliorer le débit. A l'inverse, cette couche est capable d'utiliser une seule connexion réseau pour transporter plusieurs messages à la fois grâce au multiplexage. Dans tous les cas, tout ceci doit être transparent pour la couche session.

Cette couche est également responsable du type de service à fournir à la couche session, et finalement aux utilisateurs du réseau : service en mode connecté ou non, avec ou sans garantie d'ordre de délivrance, diffusion du message à plusieurs destinataires à la fois... Cette couche est donc également responsable de l'établissement et du relâchement des connexions sur le réseau.

Un des tous derniers rôles à évoquer est le contrôle de flux.

C'est l'une des couches les plus importantes, car c'est elle qui fournit le service de base à l'utilisateur, et c'est par ailleurs elle qui gère l'ensemble du processus de connexion, avec toutes les contraintes qui y sont liées.

L'unité d'information de la couche réseau est le message.

### 2.1.6. La couche session

Cette couche organise et synchronise les échanges entre tâches distantes. Elle réalise le lien entre les adresses logiques et les adresses physiques des tâches réparties. Elle établit également une liaison entre deux programmes d'application devant coopérer et commande leur dialogue (qui doit parler, qui parle...). Dans ce dernier cas, ce service

d'organisation s'appelle la gestion du jeton. La couche session permet aussi d'insérer des points de reprise dans le flot de données de manière à pouvoir reprendre le dialogue après une panne.

### 2.1.7. La couche présentation

Cette couche s'intéresse à la syntaxe et à la sémantique des données transmises : c'est elle qui traite l'information de manière à la rendre compatible entre tâches communicantes. Elle va assurer l'indépendance entre l'utilisateur et le transport de l'information.

Typiquement, cette couche peut convertir les données, les reformater, les crypter et les compresser.

### 2.1.8. La couche application

Cette couche est le point de contact entre l'utilisateur et le réseau. C'est donc elle qui va apporter à l'utilisateur les services de base offerts par le réseau, comme par exemple le transfert de fichier, la messagerie...

# 3. Les utilitaires de connectivité

Ces utilitaires permettant de "déboguer" et de configurer TCP/IP. Vous les trouverez indispensables pour identifier des problèmes de connectivité, tester les communications entre nœuds de réseau et les paramètres TCP/IP des machines de votre réseau.

Les quatre problèmes de connectivité les plus fréquents sont :

- **Dysfonctionnement ou mauvaise configuration du protocole TCP/IP** : Le logiciel protocolaire ne fonctionne pas ou n'est pas configuré pour fonctionner correctement sur le réseau.
- **Problèmes de média :** Un câble n'est pas connecté ou est défectueux. Un Hub, un Switch ou le routeur ne fonctionne pas.
- **Résolution de noms incorrecte :** Les noms DNS et NetBIOS ne peuvent être résolus. Les ressources sont accessibles par adresse IP, mais pas par le nom de machine ou par le nom DNS.
- **Trafic excessif** : Le réseau semble fonctionner, mais il est très lent.

## *3.1. 1. Le dysfonctionnement ou la mauvaise configuration du protocole TCP/IP*

Comme tout logiciel, le protocole TCP/IP peut ne pas avoir été installé correctement. Même après avoir été installé, il peut s'arrêter à cause d'un fichier défectueux ou d'une modification de la configuration du système.
Par exemple, même si le logiciel fonctionne, la machine peut être incapable de se connecter aux autres machines parce que son adresse IP et son masque de sous-réseau sont incorrects.

Le protocole TCP/IP fournit des utilitaires qui vous aident à déterminer si TCP/IP fonctionne et s'il est correctement configuré, tels que :

- **Ping**

Est un outil de diagnostic très utile qui initie un test de connectivité réseau très simple et Indique si l'autre machine répond.

- **Utilitaires de configuration**

Permettent d'afficher les informations de configuration de TCP/IP et permettent de vérifier que l'adresse IP, le masque de sous-réseau, le serveur DNS et d'autres paramètres sont
configurés correctement.

- **ARP (Protocole de Résolution d'Adresse)**

Permet de voir et de configurer le contenu du cache ARP qui associe les adresses IP aux adresses physiques.

### 3.1.1. Ping (un acronyme de Packet internet groper)

L'utilitaire **Ping** envoie un message à la machine destinatrice, en utilisant la requête écho d'ICMP (ICMP est le Protocole de Contrôle de Messages d' Internet).
Si la machine destinatrice est présente et opérationnelle, elle répond en utilisant le message écho de ICMP.
Lorsque la machine émettrice reçoit la réponse, elle affiche un message indiquant que le **ping** est fructueux.
La réussite de la commande **ping** atteste que la machine émettrice et les machines destinatrices sont bien sur le réseau et en état de communiquer. Cependant, **ping** est une application minimaliste.
Si le **ping** fonctionne correctement, vous pouvez éliminer les problèmes liés à la couche d'accès au réseau, à l'interface réseau, au câblage et au routeur.
**Ping** présente un certain nombre d'options qui le rendent utile pour "déboguer" les problèmes de réseau.

**Sous DOS**

Saisir C:\>ping <option>

Dans un scénario de "débogage" classique, un administrateur de réseau exécute, dans l'ordre, les commandes ping suivantes sur :

• l'adresse de bouclage (127.0.0.1) afin de vérifier que TCP/IP fonctionne correctement sur la machine locale.
• l'adresse IP locale (192.168.x.yyy) afin de vérifier que l'interface réseau fonctionne correctement et que l'adresse IP locale est bien configurée.
• la passerelle par défaut (routeur ou serveur proxy) afin de vérifier que la machine peut communiquer avec le sous-réseau local et que la passerelle par défaut est présente.

• une adresse située au-delà de la passerelle par défaut, afin de vérifier que celle-ci retransmet bien les paquets au-delà du segment de réseau local.
• la machine locale et les machines distantes avec leurs noms de machine afin de vérifier que les résolutions de noms fonctionnent.
Ces étapes constituent une bonne approche de résolution d'un problème réseau. Vous n'aurez toujours pas la réponse, mais au moins vous saurez où chercher.

### 3.1.2. La commande IPCONFIG

Tous les systèmes d'exploitation récents disposent d'un utilitaire affichant la configuration TCP/IP.
Ces utilitaires fournissent 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.
Vous pouvez employer ces utilitaires pour vérifier que l'adresse IP de la machine est celle que vous attendez.

*Cas particulier de **DHCP** (**Dynamic Host Configuration Protocol**)*
*Vous ne pouvez pas toujours trouver l'adresse IP à partir des utilitaires de configuration : ils vous indiquent quelle adresse IP est en cours d'utilisation.*
*Si votre machine est configurée pour DHCP, vous pouvez même découvrir qu'elle n'a pas du tout d'adresse IP, ce qui indique un problème de connexion avec le serveur DHCP.*
*Ces utilitaires ne vous disent pas ce que devraient être votre adresse IP et votre masque de sous-réseau ; ils disent 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.*

Les systèmes DOS, Unix et Linux utilisent la commande **ipconfig** pour afficher les informations d'adressage.
L'adresse IP est plus associée à une carte réseau qu'à une machine elle-même.
Si une machine dispose de 2 cartes réseau (une pour l'Internet, l'autre pour l'Intranet), elle aura 2 adresses IP.
La commande ipconfig affiche les informations d'adressage de chaque carte réseau.

**Sous DOS**

- **C:\>ipconfig /all**

### 3.1.3. Le Protocole de Résolution d'Adresse (ARP)

**ARP** est un protocole clé de TCP/IP utilisé pour déterminer l'adresse physique correspondant à une adresse IP.
Chaque machine située sur un réseau TCP/IP maintient un cache ARP :
Une table de correspondance entre les adresses IP et les adresses physiques.
La commande **arp** permet de visualiser le contenu de la machine locale ou d'une autre machine.

**Sous DOS**

Saisir : **C:\>arp** pour visualiser toutes les options.

Les entrées dans le cache ARP sont, par défaut, dynamiques.
Les entrées du cache commencent à expirer dès lors qu'elles sont entrées. Ne soyez pas surpris qu'il n'y ait pas ou peu d'entrées dans le cache ARP.

## *3.2. Les problèmes de média*

Un problème de Hub, de Switch, de câble n'est pas réellement un problème TCP/IP. Cependant, vous pouvez encore utiliser des utilitaires de diagnostic TCP/IP pour détecter des problèmes de média.

En général, si le réseau s'arrête brusquement, un problème de média en est sûrement la cause.

- Assurez-vous que tous les câbles réseau sont correctement enfichés.
- Les cartes réseau, les Hubs, les switches, les routeurs disposent de LED indiquant que l'équipement est en service et prêt à recevoir des données.
- Tester le câblage réseau avec un contrôleur ou un testeur de câble tel que **FlukNetwork** ou autres
- Utiliser l'utilitaire **ping** pour isoler les problèmes de média.

Si une machine peut "lancer un **Ping** sur sa propre adresse, mais pas d'autres adresses du réseau, le défaut se situe dans le segment de câble connectant la machine au sous-réseau local.

## *3.3. Les problèmes de résolution de noms*

Un problème de résolution de noms se produit lorsqu'un nom de machine à laquelle un message est adressé ne peut pas être résolu sur le réseau.
Un problème de résolution de noms n'est pas forcément un problème de connectivité, parce que cela ne signifie pas nécessairement que la machine source ne peut pas se connecter à la machine cible.
Le symptôme le plus courant d'un problème de résolution de noms est que la machine source peut atteindre la machine de destination avec son adresse IP, mais pas son nom de machine.

### 3.3.1. La résolution de noms et le fichier <hosts>

La configuration de la résolution de noms sur un petit réseau est souvent très simple. Les systèmes d'exploitation supportant TCP/IP reconnaissent le fichier **hosts** et l'utilisent pour la résolution des noms.

1. Assigner une adresse IP et un nom de machine à chaque poste.
2. Créer un fichier hosts.txt (sous Windows avec Bloc-notes) faisant correspondre l'adresse IP au nom de machine de chaque poste.
3. Placer le fichier **hosts** dans le répertoire Windows.

Exemple de fichier **hosts :**

```
127.0.0.1       localhost              # cette machine
192.168.1.11    poste01                # poste 1 du Comptable
```

**#** est u signe désignant un commentaire optionnel
Le fichier contient une entrée pour l'adresse de bouclage 127.0.0.1

## *3.4. Les problèmes de performance de réseau*

Les problèmes de performance du réseau sont des problèmes qui ralentissent votre réseau.

Puisque le protocole TCP/IP utilise des paramètres TTL (**T**ime **T**o **L**ive) limitant la durée de vie d'un paquet sur le réseau, des problèmes de ralentissement peuvent occasionner des pertes de paquets et, par conséquent, des pertes de connectivité.

Même si vous ne perdez pas la connexion, un réseau lent peut être source d'énervement et de baisse de productivité.

Un trafic excessif est la cause essentielle de ralentissement (trop de machines, un matériel actif défectueux provoquant un goulet d'étranglement quelque part sur le réseau).

TCP/IP dispose de certains utilitaires vous permettant de voir où vont les paquets et d'afficher des statistiques relatives aux performances du réseau.

### 3.4.1. La commande Tracert

L'utilitaire **tracert** trace le chemin emprunté par les paquets lorsqu'ils cheminent de votre machine vers leurs destinations, en traversant plusieurs passerelles. Le chemin tracé est simplement un chemin entre la source et la destination.
**Tracert** est une commande lente : il faut compter entre 10 à 15 secondes par routeur.

En plus de localiser chaque routeur ou passerelle traversés par les paquets, **tracert** enregistre également le temps d'aller et retour RTT (**R**ound **T**rip **T**ime) pour atteindre chaque routeur.

La syntaxe de la commande est :

**C:\>tracert <adresse IP>** ou **<nom DNS>** ou **<adresse URL>**

### 3.4.2. La commande Netstat

L'utilitaire **netstat** affiche des statistiques relatives aux protocoles TCP/IP et ICMP. Ces statistiques affichent de nombreux compteurs pour des items tels que les paquets émis, les paquets reçus et les erreurs qui auraient pu se produire.

Vous ne devez pas être surpris si votre machine reçoit de temps en temps des paquets provoquant des erreurs, des rejets ou des dysfonctionnements.

TCP/IP tolère ces types d'erreurs et il ré-émet automatiquement le paquet.

Pour connaître les options de la commande **netstat** :

**C:\>netstat ?**

### 3.4.3. La commande Nbtstat

L'utilitaire **nbtstat** fournit des statistiques concernant NetBIOS sur TCP/IP.
**Nbtstat** vous permet de visualiser la table des noms NetBIOS de la machine locale ou d'une machine distante.

Pour connaître les options de la commande **nbtstat** :

**C:\>nebstat ?**

## 3.5. Résumé des commandes

| | |
|---|---|
| **Netsh** | Outil de configuration utilisé par de nombreux services réseau. À chaque service réseau correspond un contexte précis contenant des commandes spécifiques à ce service. Dans le cas des contextes des commandes **netsh interface ip** et **netsh interface ipv6**, affiche et administre les paramètres du protocole TCP/IP sur l'ordinateur local ou sur un ordinateur distant. |
| **Netstat** | Affiche des statistiques relatives au protocole et des informations sur les connexions TCP actuelles. |
| **Nslookup** | Exécute des requêtes DNS et en affiche les résultats. |
| **Ping** | Envoie des messages ICMP (Internet Control Message Protocol) Echo ou ICMPv6 (Internet Control Message Protocol for IPv6) de demande d'écho afin de tester l'accessibilité. |
| **Route** | Permet d'afficher les tables de routage IPv4 et IPv6 et de modifier la table de routage IPv4. |
| **Tracert** | Envoie des messages ICMP Echo ou ICMPv6 de demande d'écho afin de déterminer l'itinéraire réseau emprunté par les paquets IPv4 ou IPv6 pour parvenir à une destination précise. |
| **Pathping** | Envoie des messages ICMP Echo ou ICMPv6 de demande d'écho afin de déterminer l'itinéraire suivi par un paquet IPv4 ou IPv6 pour parvenir à une destination et affiche des informations sur les pertes de paquets de chaque routeur et de chaque liaison du chemin. |
| **Service SNMP** | Fournit des informations de statut ainsi que des statistiques aux systèmes de gestion SNMP (Simple Network Management System). |
| **Observateur d'événements** | Enregistre les erreurs et les événements. |
| **Journaux et alertes de performance** | Consignent les performances du protocole TCP/IP essentiel et envoient des alertes (le service SNMP doit être installé). |
| **Moniteur réseau** | Capture et affiche le contenu des paquets TCP/IP envoyés depuis, ou vers, des |

| | |
|---|---|
| | ordinateurs exécutant Windows Server 2003. |
| **Netdiag** | Exécute une batterie de tests de diagnostic sur les composants réseau. Netdiag fait partie des outils de support de Windows XP et de Windows Server 2003 qui figurent dans le dossier Support\Outils du CD-ROM du produit Windows XP ou Windows Server 2003. |
| **Telnet** | Teste l'établissement de la connexion TCP entre deux nœuds. |
| **Ttcp** | Écoute ou envoie des données des segments TCP et des messages UDP entre deux nœuds. Ttcp.exe accompagne Windows Server 2003 ; il se trouve dans le dossier Valueadd\Msft\Net\Tools du CD-ROM du produit Windows Server 2003. |

# 4. Diagnostiquer et tester les couches OSI

Les tests de base d'un réseau doivent être effectués séquentiellement, selon l'ordre des couches du modèle de référence OSI. Il est préférable de commencer par la couche 1, jusqu'à la couche 7 si nécessaire. Au niveau de la couche 1, cherchez à identifier des problèmes simples, tels que des cordons d'alimentation déconnectés d'une prise murale. Les problèmes les plus fréquents sur les réseaux IP proviennent d'erreurs dans le système d'adressage. Il est important de vérifier la configuration des adresses avant de passer aux autres étapes de configuration.
Chaque test décrit dans cette section est axé sur le fonctionnement d'un réseau au niveau d'une couche donnée du modèle OSI. Les commandes **telnet** et **ping** sont deux commandes importantes utilisées pour tester un réseau.

## *4.1. Utilisation d'une approche structurée du dépannage*

Le dépannage est un processus qui permet à un utilisateur de localiser les problèmes sur un réseau. Ce processus de dépannage devrait être basé sur des normes de gestion de réseau mises en place par un administrateur réseau. La création d'une documentation est très importante pour le processus de dépannage.

Les étapes de ce modèle sont les suivantes:

**Étape 1:** Collecte de toutes les données disponibles et analyse

des causes d'échec

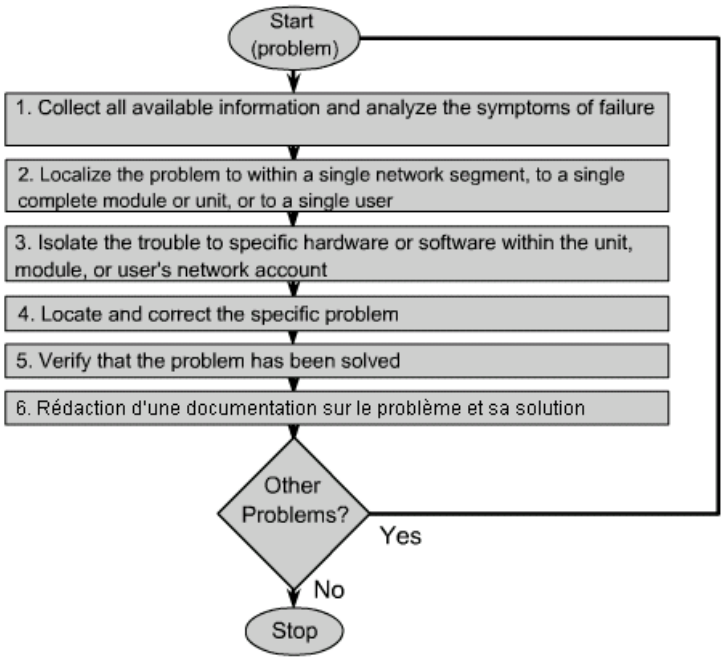
**Étape 2:** Localisation du problème au sein d'un segment de réseau, d'une unité ou d'un module, ou au niveau utilisateur

**Étape 3:** Imputation du problème à un matériel ou à un logiciel spécifique au sein de l'unité, du module ou du compte réseau d'un utilisateur

**Étape 4:** Recherche et correction du problème

**Étape 5:** Confirmation de la résolution du problème

**Étape 6:** Rédaction d'une documentation sur le problème et sa solution




La figure illustre une autre approche du dépannage. Le dépannage ne se limite pas à ces deux méthodes. Toutefois, le recours à un processus structuré est d'une importance capitale pour le fonctionnement efficace et sans coupure d'un réseau.
Par le biais d'une approche structurée du dépannage, chaque membre d'une équipe de support de réseau peut connaître les opérations que chacun a réalisées pour résoudre un problème. Si diverses solutions de dépannage sont testées sans aucune organisation ni documentation, la résolution des problèmes n'est pas efficace. Même si un problème est résolu dans le cadre d'une approche non structurée, il sera probablement impossible de reproduire la solution lorsque des problèmes similaires surviendront ultérieurement

## *4.2. Test sur la base des couches OSI*

La phase de test doit commencer au niveau de la couche 1 du modèle OSI, jusqu'à la couche 7 si nécessaire.
Les erreurs identifiées au niveau de la couche 1 peuvent être les suivantes:

- Câbles rompus
- Câbles déconnectés
- Câbles raccordés à des ports inappropriés
- Connexions instables
- Câbles inappropriés pour la tâche à accomplir (les câbles console, les câbles croisés et les câbles droits doivent être employés à bon escient)
- Problèmes d'émetteur-récepteur
- Problèmes de câblage ETCD
- Problèmes de câblage ETTD
- Unités hors tension

Les erreurs identifiées au niveau de la couche 2 peuvent être les suivantes:

- Interfaces série configurées de façon incorrecte
- Interfaces Ethernet configurées de façon incorrecte
- Ensemble d'encapsulation inapproprié (HDLC est utilisé par défaut pour les interfaces série)
- Fréquence d'horloge inappropriée pour les interfaces série
- Problèmes de carte réseau (NIC)

Les erreurs identifiées au niveau de la couche 3 peuvent être les suivantes:

- Protocole de routage non activé
- Protocole de routage incorrect activé
- Adresses IP incorrectes
- Masques de sous-réseau incorrects

Si des erreurs apparaissent sur le réseau, le processus de test basé sur les couches OSI doit être déclenché. La commande **ping** est utilisée pour tester la connectivité au niveau de la couche 3. La commande **telnet** peut être utilisée au niveau de la couche 7 pour vérifier le logiciel de la couche application entre des stations source et de destination. Ces deux commandes sont décrites plus loin dans une autre section de ce document

### 4.2.1. Dépannage de la couche 1 à l'aide des témoins lumineux

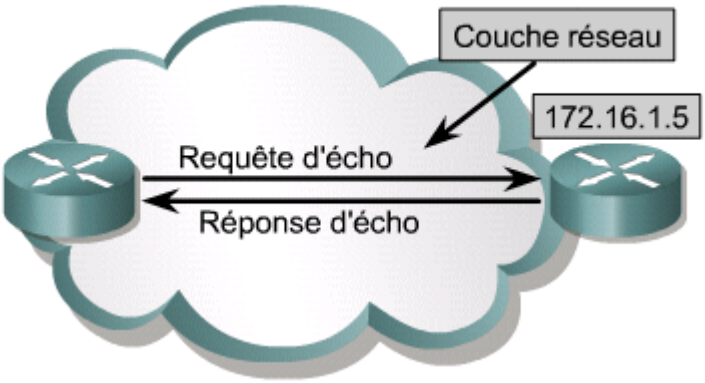
Les témoins lumineux sont utiles au dépannage. La plupart des interfaces ou des cartes réseau comportent des témoins lumineux qui indiquent si la connexion est valide. Ces témoins lumineux sont souvent appelés voyants de liaison. L'interface peut également disposer de témoins lumineux pour indiquer si le trafic est en cours de transmission (TX) ou reçu (RX). Si l'interface comporte des témoins lumineux indiquant que la connexion n'est pas valide, mettez l'unité hors tension et replacez la carte d'interface. Un voyant de liaison peut également indiquer une mauvaise connexion ou l'absence de liaison à cause d'un câble inapproprié ou défectueux.
Vérifiez que tous les câbles sont connectés aux ports appropriés. Vérifiez que toutes les interconnexions sont raccordées au bon emplacement à l'aide du câble et de la méthode appropriés. Vérifiez que tous les ports de concentrateur et de commutateur sont associés au réseau VLAN ou au domaine de collision approprié, et que les options de Spanning Tree correspondantes, entre autres, sont définies correctement.
Vérifiez que le câble approprié est utilisé. Un câble croisé peut être requis pour des connexions directes entre deux commutateurs ou concentrateurs, ou entre deux hôtes, tels que des PC ou des routeurs. Vérifiez que le câble de l'interface source est correctement connecté et en bon état. En cas de doute sur la connexion, replacez le câble et vérifiez la sécurité de la connexion. Essayez de remplacer le câble par un câble de travail connu. Si ce câble est connecté à une prise murale, utilisez un testeur de câble pour vérifier que la prise est correctement raccordée.
Vérifiez également le type, la connexion et la configuration de tout émetteur-récepteur utilisé. Si le remplacement du câble ne résout pas le problème, essayez de remplacer l'émetteur-récepteur si vous en utilisez un.
Assurez-vous également que l'unité est bien sous tension. Contrôlez toujours les composants de base avant d'exécuter des diagnostics ou de tenter un dépannage plus complexe

### 4.2.2. Dépannage de la couche 3 à l'aide de la commande ping

La commande **ping** utilise le protocole ICMP (Internet Control Message Protocol) pour vérifier la connexion matérielle et l'adresse logique au niveau de la couche réseau.

| Message | Usage |
|---|---|
| Destination inaccessible | Indique à l'hôte source qu'un paquet ne peut pas être livré. |
| Dépassement du délai | Le délai de livraison d'un paquet a expiré ; le paquet a été éliminé. |
| Épuisement de la source | La source envoie les données plus rapidement qu'elles ne peuvent être transmises. Ce message invite l'émetteur à ralentir. |
| Redirection | Le routeur qui envoie ce message a reçu un paquet pour lequel une autre route aurait pu être privilégiée. Ce message invite l'émetteur à utiliser la route la plus optimale. |
| Écho | Ce message est utilisé par la commande ping pour vérifier la connectivité. |
| Problème de paramètre | Ce message est utilisé pour identifier un paramètre qui est incorrect. |
| Horodatage | Ce message est utilisé pour mesurer le délai entre deux hôtes. |
| Demande de masque d'adresse/réponse à la demande | Ce message est utilisé pour demander et connaître le masque de sous-réseau à utiliser. |
| Annonce et sélection de routeur | Ce message permet aux hôtes de connaître de manière dynamique les adresses IP des routeurs connectés au sous-réseau. |

Le tableau de la figure indique les différents types de message ICMP. Il s'agit d'un mécanisme de test des plus élémentaires pour la connectivité du réseau.




```
Router>ping 172.16.1.5
Type escape sequence to abort.
Sending 5, 100 byte ICMP Echos to 172.16.1.5,
timeout is 2 seconds:
!!!!!
Success rate is 100 percent,
round-trip min/avg/max = 1/3/4 ms
Router>
```

Dans la figure, la cible 172.16.1.5 de la commande **ping** a répondu correctement aux cinq datagrammes envoyés. Les points d'exclamation (**!**) indiquent chaque écho réussi. Si votre écran affiche un ou plusieurs points (.) au lieu de points d'exclamation, cela signifie que le délai d'attente de l'application du routeur a expiré (ou encore, a été dépassé) pendant qu'elle attendait un écho de paquet de la cible précisée dans la commande **ping**.

La commande suivante active un outil de diagnostic qui est utilisé pour vérifier la connectivité:

Router#**ping** [protocole] {hôte | adresse}

La commande **ping** teste les connexions du réseau en envoyant des requêtes d'écho ICMP à un hôte cible et en écoutant les réponses. La commande **ping** vérifie le nombre de paquets envoyés, le nombre de réponses reçues et le pourcentage de paquets perdus. Elle vérifie également le temps nécessaire pour que les paquets atteignent leur destination et pour que les réponses soient reçues. Ces informations permettent de contrôler la communication entre une station de travail et d'autres hôtes, et si des données ont été perdues.

La commande **ping** peut être appelée à la fois en mode privilégié et en mode utilisateur. La commande **ping** peut être utilisée pour confirmer la connectivité de base sur les réseaux AppleTalk, ISO CLNS (service réseau non orienté connexion), IP, Novell, Apollo, VINES, DECnet ou XNS.

L'utilisation d'une commande **ping** étendue indique au routeur d'exécuter une gamme plus étendue d'options de test. Pour utiliser la commande **ping** étendue, entrez **ping** sur la ligne de commande, puis appuyez sur la touche **Entrée** sans saisir d'adresse IP. Des invites de commande vont apparaître chaque fois que vous appuyerez sur la touche **Entrée**. Ces nombreux invites permettent de spécifier davantage d'options que le **ping** standard.

Il est intéressant d'utiliser la commande **ping** lorsque le réseau fonctionne correctement pour voir comment s'exécute cette commande dans des conditions normales et disposer d'un modèle de comparaison lors du dépannage.

### 4.2.3. Dépannage de la couche 7 à l'aide de la commande Telnet

L'utilitaire Telnet est un protocole de terminal virtuel qui fait partie de la pile de protocoles TCP/IP. Il permet de vérifier le logiciel de la couche application entre les stations d'origine et de destination. Il s'agit du mécanisme de test le plus complet qui soit. L'utilitaire Telnet est normalement utilisé pour connecter des unités distantes, collecter des informations et exécuter des programmes.
L'application Telnet fournit un terminal virtuel pour la connexion aux routeurs exécutant TCP/IP. Dans le cadre du dépannage, il est utile de vérifier qu'une connexion peut être établie à l'aide de Telnet. Cela prouve qu'au moins une application TCP/IP est capable d'établir une connexion de bout en bout. Une connexion Telnet réussie indique que l'application de couche supérieure, ainsi que les services des couches inférieures, fonctionnent correctement.
Si un administrateur peut envoyer une commande Telnet à un routeur mais pas à un autre, vérifiez la connectivité au niveau des couches inférieures. Si la connectivité a été vérifiée, l'échec de Telnet est vraisemblablement dû à des problèmes spécifiques d'adressage, d'attribution de noms ou d'autorisation d'accès. Ces problèmes peuvent exister sur le routeur de l'administrateur ou sur celui que vous avez tenté d'atteindre via Telnet.
Si une commande Telnet vers un serveur donné échoue à partir d'un hôte, essayez de vous connecter à partir d'un routeur et de plusieurs autres unités. Lors des tentatives de connexion via Telnet, si aucune invite de connexion n'apparaît, vérifiez ce qui suit:

- Une recherche DNS inverse sur l'adresse du client peut-elle être trouvée ? De nombreux serveurs Telnet n'autorisent pas les connexions à partir d'adresses IP qui ne disposent pas d'entrées DNS. Il s'agit d'un problème fréquent pour les adresses DHCP dans lesquelles l'administrateur n'a pas ajouté d'entrées DNS pour les groupes DHCP.

- Il est possible qu'une application Telnet ne puisse pas négocier les options appropriées et ne se connecte donc pas. Sur un routeur

Cisco, ce processus de négociation peut être visualisé à l'aide de la commande **debugtelnet**.

- Il est possible que l'utilitaire Telnet soit désactivé ou ait été déplacé vers un port autre que 23 sur le serveur de destination.

# 5. Rappel sur les commandes de dépannage des routeurs Cisco

## *5.1. Commande show ip route*

La commande **`show ip route`** affiche le contenu de la table de routage IP. Cette table contient des entrées pour tous les réseaux et les sous-réseaux connus, ainsi qu'un code indiquant comment ces informations ont été apprises. Voici des exemples de commandes supplémentaires à utiliser avec la commande **`show ip route`**:

- **`show ip route connected`**
- **`show ip route`** *`address`*
- **`show ip route rip`**
- **`show ip route igrp`**
- **`show ip route static`**

## *5.2. Les commandes debug*

Les commandes **debug** permettent d'identifier précisément les problèmes de protocole et de configuration. La commande **debug** est utilisée pour afficher des événements et des données dynamiques. Étant donné que les commandes **show** n'affichent que des informations statiques, elles fournissent une représentation historique du fonctionnement du routeur. L'utilisation des informations affichées par la commande **debug** procure des informations sur les événements en cours sur le routeur. Ces événements peuvent concerner le trafic sur une interface, les messages d'erreur générés par des nœuds sur le réseau, les paquets de diagnostic propres à un protocole et d'autres données utiles pour le dépannage. Le résultat dynamique de la commande **debug** peut nuire aux performances, car il crée des surcharges sur le processeur susceptibles d'interrompre le fonctionnement normal du routeur. C'est pourquoi la commande **debug** doit être utilisée avec parcimonie. Utilisez les commandes **debug** pour examiner certains types de trafic ou des problèmes spécifiques après avoir envisagé plusieurs causes possibles.

Les commandes **debug** doivent être utilisées pour localiser des problèmes et non pour surveiller le fonctionnement normal du réseau.

## 5.3. Commande show Controller

La commande show controllers sert à déterminer le type de câble connecté sans avoir à inspecter les câbles.

Exemple : resulta de la commande **`show controllers serial 0/0`**

```
QUICC Serial unit 0
idb at 0x20A31A3A8, driver data structure at 0x20A4C60
SCC Registers:
General [GSMR]= 0x2: 0x00000030, Protocol-specific
[PSMR]=0x0
Events [SCCE]=0x0000, Mask [SCCM]=0x001F, Status
[SCCS]=0x0006
Transmit on Demand [T0DR]=0x0, Data Sync [DSR]=0x7E7E
Interrupt Registers:
----output omitted----
DTE V.35 serial cable attached.

SCC GENERAL PARAMETER RAM (at 0xFF00F00)
Rx BD Base [RBASE]=0x540, Fn Code [RFCR]=0x18
Tx BD Base [TBASE]=0x580, Fn Code [TFCR]=0x18
```

La commande **show controllers serial 0/0** interroge le circuit intégré, ou puce de contrôleur, qui contrôle les interfaces série et affiche des informations sur l'interface physique série 0/0. Le résultat varie d'une puce de contrôleur à une autre. Le résultat varie d'une puce de contrôleur à une autre. Même au sein d'un même type de routeur, différentes puces de contrôleur peuvent être utilisées.

## 5.4. Les commandes show ip protocols et show ip route

Les commandes **show ip protocols** et **show ip route** affichent des informations sur les protocoles de routage et sur la table de routage. Les informations affichées par ces commandes peuvent être utilisées pour vérifier la configuration du protocole de routage.

## 5.5. La commande traceroute

La commande **traceroute** est utilisée pour découvrir les routes que les paquets empruntent lors du déplacement vers leur destination. L'utilitaire Traceroute peut également être utilisé pour aider à tester la couche

réseau (couche 3) saut par saut et pour fournir des références pour les performances.

La commande **traceroute** est souvent référée comme étant la commande **trace** dans le matériel de référence. Cependant, la syntaxe exacte de la commande est **traceroute**.

## 5.6. La commande show cdp

Le protocole CDP (Cisco Discovery Protocol) annonce des informations sur les unités à ses voisins directs, notamment les adresses MAC et IP, ainsi que les interfaces de sortie.
Les informations affichées par la commande **show cdp neighbors** contiennent des informations sur les unités voisines Cisco directement connectées.
Resultat de la commande **show cdp neighbors :**

```
Capability Codes: R - Router, T - Bridge, B - Sourse, Route Bridge,
                  S - Switch, H- Host, I - IGMP, r- Repeater

Device ID     LocalInterface   Holdtime   Capability   Platform    Port ID
3350-srvs     Fas 0/0          153        R S I        WS-C3550-2  Fas 0/1
Cyberspace    ser 0/1          171        R            3640        Ser 1/1
004096581e28 Fas 0/0           150                     AIR-AP350   fec0
0040965716a5 Fas 0/0           152                     AIR-AP350   fec
BHM           Ser 0/0          137        R            2601        Ser 0/0
accessl       Fas 0/2          162        R            2511        Eth 0
```

Ces informations sont utiles pour le débogage des problèmes de connectivité. Si un problème de câblage est suspecté, activez les interfaces avec la commande **no shutdown**, puis exécutez la commande **show cdp neighbors detail** avant toute autre configuration. La commande affiche les détails relatifs à une unité spécifique, tels que les interfaces actives, l'ID de port et l'équipement. La version de la plate-forme logicielle Cisco IOS exécutée sur les unités distantes apparaît également.
Si la couche physique fonctionne correctement, toutes les autres unités Cisco directement connectées doivent être affichées. L'absence d'unité connue reflète probablement un problème au niveau de la couche 1.
Le protocole CDP présente un problème de sécurité. La quantité d'informations fournies par CDP est tellement vaste que ce protocole peut être à l'origine d'une défaillance au niveau de la sécurité. 2Pour des raisons de sécurité, CDP doit être configuré uniquement sur des liaisons entre des unités Cisco, et désactivé sur les ports ou les liaisons utilisateur qui ne sont pas gérés localement.

## 5.7. La commande show interfaces

La commande **`show interfaces`** est peut-être l'outil le plus important pour découvrir les problèmes de couche 1 et 2 avec le routeur. Le premier paramètre (ligne) fait référence à la couche physique. Le deuxième

paramètre (protocole) indique si les processus de l'IOS qui contrôlent le protocole de ligne considèrent l'interface comme utilisable. Cela dépend de la réception ou non des messages de test d'activité. Les messages de test d'activité sont des messages envoyés par une unité du réseau à une autre pour lui indiquer que le circuit virtuel existant entre les deux est toujours actif. Si l'interface manque trois messages de test d'activité consécutifs, le protocole de ligne est considéré comme inactif.
Lorsque la ligne est inactive, le protocole est toujours inactif, car il n'existe aucun média utilisable pour le protocole de couche 2. Cela est particulièrement vrai lorsque l'interface est en panne à cause d'un problème matériel et lorsqu'elle a été désactivée par un administrateur.
Si l'interface est active et que le protocole de ligne est désactivé, un problème de couche 2 existe. Les causes possibles sont les suivantes:

- Aucun message de test d'activité (keepalives)
- Aucune fréquence d'horloge (clock rate)
- Aucune correspondance au niveau du type d'encapsulation

La commande **show interfaces serial** doit être utilisée après configuration d'une interface série pour vérifier les modifications et s'assurer que l'interface est opérationnelle.

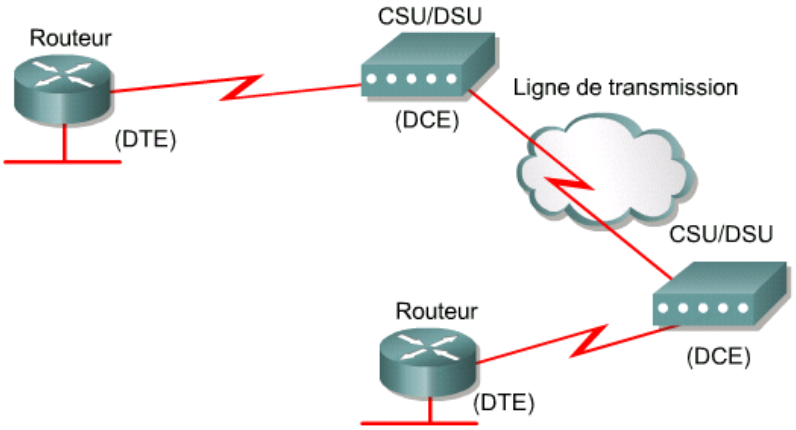
# 6. Dépannage de la liaison série

### 6.1.1. Présentation des communications série

Les technologies des réseaux WAN s'appuient sur une transmission série au niveau de la couche physique. Cela signifie que les bits d'une trame sont transmis un par un sur le support physique.
Parmi les nombreuses normes de communication série, on trouve les suivantes:

- RS-232-E
- V.35
- HSSI (High Speed Serial Interface

### 6.1.2. ETCD/ETTD




Une connexion série comporte un équipement terminal de traitement de données (ETTD) à une extrémité de la connexion et un équipement de communication de données (ETCD) à l'autre extrémité. La connexion entre les deux ETCD est le réseau de transmission du fournisseur du réseau WAN. Le CPE, généralement un routeur, constitue l'ETTD. Il peut également s'agir d'un terminal, d'un ordinateur, d'une imprimante ou d'un télécopieur. L'ETCD, généralement un modem ou une unité CSU/DSU, est l'équipement servant à convertir les données utilisateur de l'ETTD en une forme compatible avec la liaison de transmission du fournisseur d'accès au WAN. Le signal est reçu par l'ETCD distant, qui le décode en une séquence de bits. Cette séquence est ensuite signalée à l'ETTD.
Le port série synchrone d'un routeur est configuré comme ETTD ou ETCD en fonction du câble qui y est relié, commandé comme ETTD ou ETCD pour correspondre à la configuration du routeur. Si le port est configuré en ETTD, le réglage par défaut, une horloge externe est requise au niveau de l'unité CSU/DSU ou d'un autre équipement ETCD

### 6.1.3. Protocole HDLC

Cisco HDLC est la méthode d'encapsulation par défaut utilisée par les équipements Cisco sur des lignes série synchrones. Si l'interface série est configurée avec un autre protocole d'encapsulation et que l'encapsulation doit être replacée en HDLC, accédez au mode de configuration de l'interface série. Entrez ensuite la commande **encapsulation hdlc** pour spécifier le protocole d'encapsulation de l'interface.

Cisco HDLC est un protocole point-à-point pouvant être utilisé sur des lignes louées entre deux équipements Cisco. Pour communiquer avec un équipement d'une autre marque que Cisco, le PPP synchrone constitue une option plus viable.

### 6.1.4. Dépannage d'une interface série

Les résultats de la commande **show interfaces serial** présentent des informations spécifiques aux interfaces série.

Quand HDLC est configuré «**Encapsulation HDLC**» doit apparaître dans les résultats.
Quand PPP est configuré, «**Encapsulation PPP**» doit apparaître dans les résultats.

Cinq états de problème possibles peuvent être identifiés sur la ligne d'état de l'interface affichée par **show interfaces serial**:

1. L'interface série x est désactivée et le protocole de ligne est désactivé (Serial x is down, line protocol is down)
2. L'interface série x est activée et le protocole de ligne est désactivé
3. L'interface série x est activée et le protocole de ligne est activé (en boucle)
4. L'interface série x est activée et le protocole de ligne désactivé
5. L'interface série x est désactivée pour des raisons d'administration (administratively down) et le protocole de ligne est désactivé

La commande **show controllers** est un autre outil de diagnostic important pour le dépannage des lignes série. Les résultats renvoyés par **show controllers** indiquent l'état des canaux de l'interface et signalent la présence ou l'absence d'un câble

Des commandes de débogage, utiles pour résoudre les problèmes d''interface série et de WAN, sont présentées ci-dessous:

- **debug serial interface** – Vérifie si les paquets de veille HDLC s'incrémentent. S'ils ne s'incrémentent pas, il existe probablement un problème de synchronisation sur la carte d'interface ou le réseau.
- **debug arp** – Indique si le routeur envoie ou reçoit des informations relatives aux routeurs (avec des paquets ARP) de l'autre côté du nuage de réseau WAN. Utilisez cette commande quand certains nœuds d'un réseau TCP/IP répondent, mais d'autres non.
- **debug frame-relay lmi** – Récupère des informations sur l'interface LMI (Local Management Interface), afin de déterminer si un commutateur Frame Relay et un routeur envoient et reçoivent des paquets LMI.
- **debug frame-relay events** – Détermine si des échanges se produisent entre un routeur et un commutateur Frame Relay.
- **debug ppp negotiation** – Montre les paquets PPP (*Point-to-Point Protocol*) transmis au démarrage de PPP, au moment où les options PPP sont négociées.
- **debug ppp packet** – Montre les paquets PPP envoyés et reçus. Cette commande affiche les transferts de paquets à bas niveau.

- **debug ppp** – Montre les erreurs PPP, telles que les trames illégales ou déformées, associées à la négociation et à l'utilisation de la connexion PPP.
- **debug ppp authentication** – Montre les échanges de paquets PPP CHAP (*Challenge Handshake Authentication Protocol*) et PAP (*Password Authentication Protocol*).

### 6.1.5. Le protocole PPP

Les aspects configurables de PPP incluent les méthodes d'authentification, la compression, la détection d'erreurs et la prise en charge ou non de la multiliaison. La section ci-après décrit les différentes options de configuration de PPP.

**Configuration de PPP**

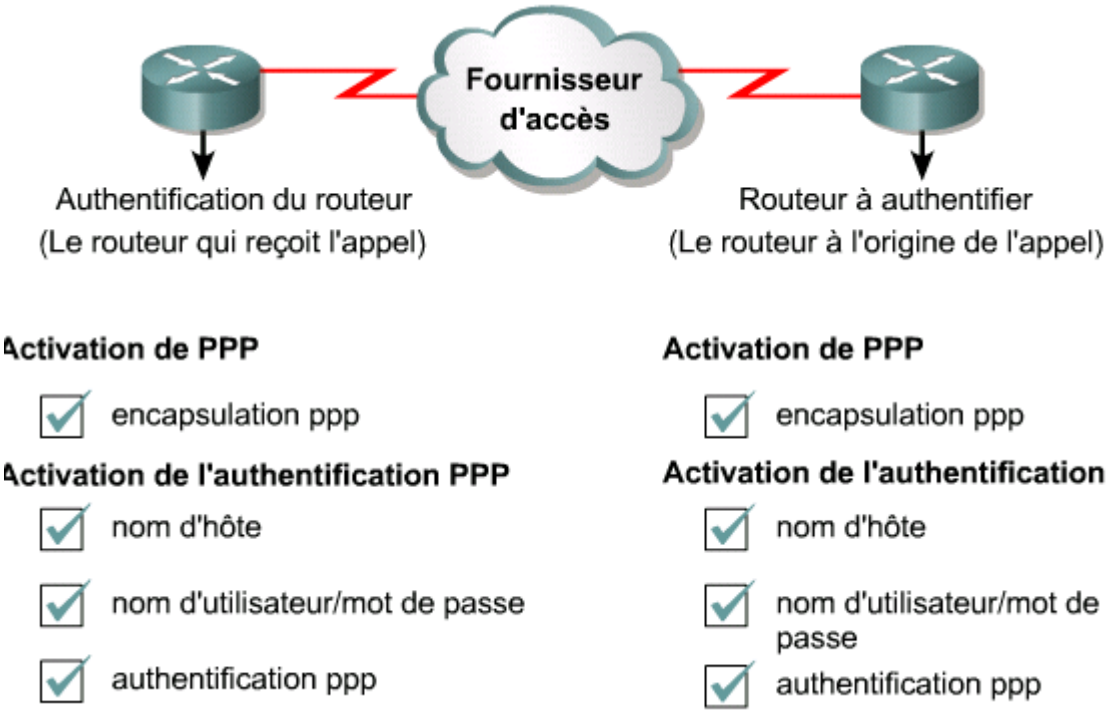
L'exemple suivant permet l'encapsulation de PPP sur l'interface série 0/0:

Router#**configure terminal**

Router(config)#**interface serial 0/0**

Router(config-if)#**encapsulation ppp**

**Configuration de l'authentification PPP**



### Les étapes pour configurer

| | |
|---|---|
| Étape 1 | Définissez sur chaque routeur le nom d'utilisateur et le mot de passe prévu pour le routeur distant :<br>`Router(config)#username name password secret`<br>Description des arguments :<br>• *name*-This is the host name of the remote router.<br>Remarque : Les majuscules et les minuscules sont différenciées pour le nom d'hôte.<br>• *secret*-Sur les routeurs Cisco, le mot de passe secret doit être identique sur les deux routeurs. |
| Étape 2 | Passez en mode de configuration d'interface pour l'interface voulue. |
| Étape 3 | Configurez l'interface pour l'encapsulation PPP :<br>`Router(config-if)#encapsulation ppp` |
| Étape 4 | Configurez l'authentification PPP :<br>`Router(config-if)#ppp authentication {chap \| chap pap \| pap chap \| pap}` |
| Étape 5 | Si les protocoles CHAP et PAP sont activés, la première méthode indiquée est demandée pendant la phase de négociation de la liaison. Si l'homologue refuse la première méthode ou suggère la deuxième, cette dernière est essayée. |
| Étape 6 | Dans Cisco IOS versions 11.1 ou ultérieures, PAP doit être activé sur l'interface, car il est désactivé par défaut.<br>`Router(config-if)#ppp pap sent-username username passwor password` |

### Dépannage de la configuration de l'encapsulation série

La commande **debug ppp authentication** affiche la séquence d'échange d'authentification.


```
4d20h: %LINK-3-UPDOWN: Interface Serial0/0, changed state to up
4d20h: Se0/0 PPP: Treating connection as a dedicated line
4d20h: Se0/0 PPP: Phase is AUTHENTICATING, by both
4d20h: Se0/0 CHAP: O CHALLENGE id 2 len 28 from "left"
4d20h: Se0/0 CHAP: I CHALLENGE id 3 len 28 from "right"
4d20h: Se0/0 CHAP: O RESPONSE id 3 len 28 from "left"
4d20h: Se0/0 CHAP: I RESPONSE id 2 len 28 from "right"
4d20h: Se0/0 CHAP: O SUCCESS id 2 len 4
4d20h: Se0/0 CHAP: I SUCCESS id 3 len 4
4d20h: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0,
changed state to up
```

La figure illustre les résultats renvoyés par le routeur de gauche au cours de l'authentification CHAP avec le routeur de droite, quand **debug ppp authentication** est activée. Lorsque l'authentification bidirectionnelle est configurée, chaque routeur authentifie l'autre. Des messages s'affichent pour le processus authentifiant et le processus authentifié. Utilisez la commande **debug ppp authentication** pour afficher la séquence d'échange au moment où elle se produit.

| Affichage | Description |
|---|---|
| Se0/0 PPP : Phase is AUTHENTICATING, by both | Authentification bidirectionnelle |
| Se0/0 PPP : O AUTH-REQ id 4 len 18 from "left" | Requête d'identification sortante |
| Se0/0 PPP : O AUTH-REQ id 1 len 18 from "right" | Requête d'authentification entrante |
| Se0/0 PPP : Authenticating peer right | Authentification entrante |
| Se0/0 PPP : O AUTH-ACK id 1 len 5 | Accusé de réception sortant |
| Se0/0 PPP : O AUTH-ACK id 4 len 5 | Accusé de réception entrant |

La figure présente les résultats renvoyés par le routeur pour une authentification PAP bidirectionnelle.
La commande **debug ppp** sert à afficher des informations sur le fonctionnement de PPP. La forme **no** de cette commande désactive l'affichage du message de débogage.

Router#**debug ppp** {**authentication** | **packet** | **negotiation** | **error** | **chap**}

Router#**no debug ppp** {**authentication** | **packet** | **negotiation** | **error** | **chap**

Mettre l'accent sur un point particulier

## Pour approfondir le sujet....

Proposition de références utiles permettant d'approfondir le thème abordé

## Sources de référence

Citer les auteurs et les sources de référence utilisées pour l'élaboration du support