

# Dépannage

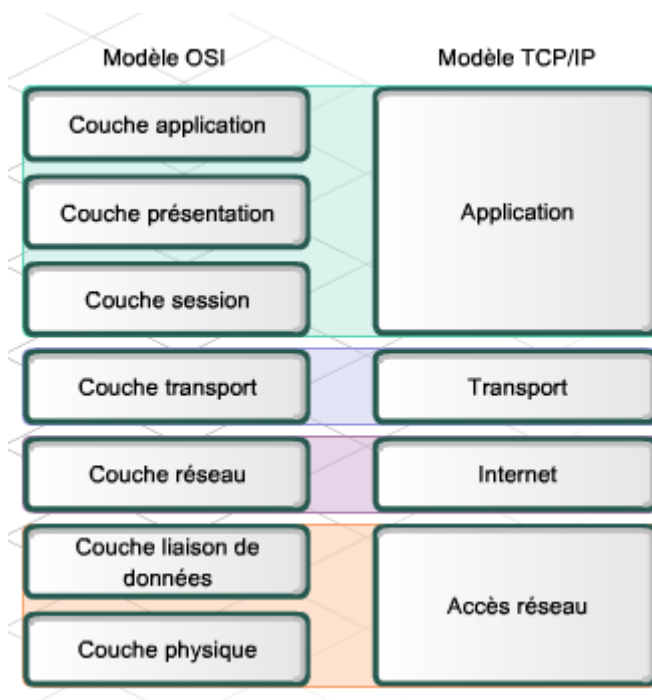
## 1 Méthodologies et outils de dépannage

### 1.1 Modèle OSI et dépannage

Une des qualités qu'un professionnel des réseaux doit apprendre à développer en priorité est la faculté de dépanner les problèmes réseau de façon efficace. En effet, les responsables de dépannage réseau sont très demandés. C'est pour cette raison que les examens de certification Cisco évaluent les compétences des candidats en matière d'identification et de correction des problèmes de réseaux.

Lors des processus de dépannage, un grand nombre de techniciens utilisent les modèles réseaux OSI et TCP/IP pour isoler la cause d'un problème. Les modèles de réseaux logiques séparent les fonctionnalités du réseau en couches modulaires. Chaque couche du modèle OSI ou TCP/IP présente des fonctions et des protocoles spécifiques. Une connaissance des capacités, fonctions et périphériques de chaque couche, ainsi que des relations de chaque couche avec les couches avoisinantes, permet à l'ingénieur réseau de procéder efficacement au dépannage.

Dans ce chapitre, la structure des activités de dépannage est présentée en fonction des modèles OSI et TCP/IP. Avant de commencer, révisez la section des cursus CCNA Discovery : Réseaux domestiques et pour petites entreprises et CCNA Discovery : Travailler dans une PME ou chez un fournisseur de services Internet consacrée aux modèles OSI et TCP/IP.



## **Utilisation du modèle de référence OSI comme outil de dépannage**

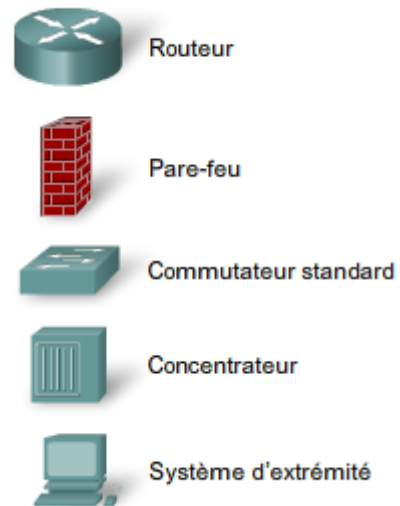
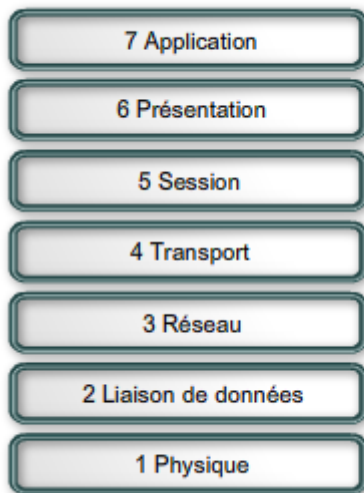
Le modèle OSI fournit aux ingénieurs réseau un langage commun. Il est important de comprendre les fonctions mises en œuvre, ainsi que les périphériques réseau qui opèrent au niveau de chaque couche du modèle OSI.

Les couches supérieures (de 5 à 7) du modèle OSI concernent les fonctions d'applications spécifiques et ne sont généralement mises en œuvre que dans les logiciels. Les problèmes isolés au niveau de ces couches sont généralement causés par des erreurs de configuration logicielle des systèmes d'extrémité sur les clients et les serveurs.

Les couches inférieures (de 1 à 4) du modèle OSI gèrent les problèmes de transport des données.

La couche réseau (couche 3) et la couche transport (couche 4) ne sont généralement mises en œuvre que dans les logiciels. Outre les erreurs logicielles au niveau des systèmes d'extrémité, les erreurs de configuration logicielles au niveau des routeurs et des pare-feu sont à l'origine d'un grand nombre des problèmes isolés sur ces couches. Les erreurs d'adressage IP et de routage surviennent au niveau de la couche 3.

La couche physique (couche 1) et la couche liaison de données (couche 2) sont mises en œuvre dans le matériel et les logiciels. La couche physique est la plus proche du support réseau physique, le câblage réseau par exemple, et est chargée de placer les informations sur le support. Les problèmes matériels et les incompatibilités engendrent des problèmes au niveau des couches 1 et 2.



**Exercice**

Identifiez la couche à laquelle appartient le protocole ou la technologie.

Pour chaque protocole ou technologie affiché, cliquez sur la couche appropriée.

| Couche physique | Couche liaison de données | Couche réseau | Couche transport | Couches supérieures |
|-----------------|---------------------------|---------------|------------------|---------------------|
|                 |                           |               |                  |                     |

Numéro de port, répéteur, commutateur, routage, SMTP, trame, concentrateur, paquet, signalisation électrique, RJ 45, http, Commutation réseau, Ethernet, Onde radio, UDP, TCP, adresse MAC, Telnet, Adresse IP, carte réseau , FTP, logiciel client

Corrigé

| Couche physique                                                                                    | Couche liaison de données                                                 | Couche réseau                     | Couche transport              | Couches supérieures                              |
|----------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|-----------------------------------|-------------------------------|--------------------------------------------------|
| Répéteurs<br>Concentrateurs<br>Signalisation électrique<br>Câble à paires torsadées<br>Ondes radio | Trames<br>Commutation réseau<br>Ethernet<br>Adresses MAC<br>Cartes réseau | Routage<br>Paquets<br>Adresses IP | Numéros de port<br>UDP<br>TCP | SMTP<br>HTTP<br>Telnet<br>FTP<br>Logiciel client |

**Travaux pratiques :** En vous servant de la fiche de travail qui vous a été distribuée, organisez les objectifs CCENT en fonction de la ou des couches auxquelles ils s’adressent.

## **1.2 Méthodologies de dépannage**

Il existe trois principales approches de dépannage basé sur les modèles réseau :

- Méthode descendante
- Méthode ascendante
- Méthode Diviser et conquérir

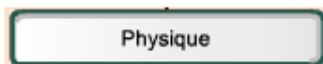
Chaque méthode s'applique à un réseau organisé en couches. À l'aide d'une de ces méthodes de dépannage, un dépanneur peut vérifier l'intégralité des fonctionnalités de chaque couche, jusqu'à ce que le problème soit localisé et isolé.

**Méthode descendante** : ce dépannage commence par la couche application et progresse vers le bas. Il recherche le problème du point de vue de l'utilisateur et de l'application. Une seule application est-elle en panne ou toutes les applications sont-elles défectueuses ? Par exemple, l'utilisateur peut-il accéder à diverses pages Web sur Internet, mais sans pouvoir envoyer de courriels ? D'autres stations de travail rencontrent-elles le même problème ?

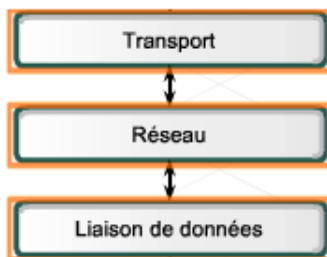
**Méthode ascendante** : ce dépannage commence par la couche physique et progresse vers le haut. La couche physique concerne le matériel et la connexion des câbles. Les câbles sont-ils raccordés de façon sécurisée ? Si l'équipement comporte des témoins lumineux, sont-ils allumés ou éteints ?

**Méthode Diviser et conquérir** : ce dépannage démarre généralement sur l'une des couches du milieu, puis progresse vers le haut ou vers le bas. Par exemple, le dépanneur peut commencer au niveau de la couche réseau, en vérifiant les informations de configuration IP.

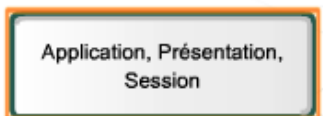
La structure de ces approches les rend parfaitement adaptées au dépanneur novice. Les personnes plus expérimentées ignorent souvent les approches structurées et se basent sur leur instinct et leur expérience.



| Approche de dépannage | Principe de fonctionnement                                                                         | Cas applicables                             | Avantages / Inconvénients                                                                                                                                    |
|-----------------------|----------------------------------------------------------------------------------------------------|---------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ascendante            | Commence toujours par la couche physique et remonte jusqu'à la détection d'une couche défectueuse. | Particulièrement adaptée aux cas complexes. | Cette approche est lente, mais très fiable. Lorsque le problème provient de l'application (couche supérieure), cette approche peut prendre un certain temps. |



| Approche de dépannage | Principe de fonctionnement                                                                                                                              | Cas applicables                                                                                                         | Avantages / Inconvénients                                                                                                                                       |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Diviser et conquérir  | Selon les circonstances (problèmes signalés) et votre expérience, vous pouvez commencer par une couche quelconque et remonter ou descendre la pile OSI. | Action la plus appropriée lorsque vous avez suffisamment d'expérience et que le problème présente des symptômes précis. | Cette approche permet d'atteindre la couche problématique plus rapidement que les autres approches. Cette approche n'est efficace que si vous êtes expérimenté. |



| Approche de dépannage | Principe de fonctionnement                                                                              | Cas applicables                                                                                                                                                        | Avantages / Inconvénients                                                                                                                        |
|-----------------------|---------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| Descendante           | Commence toujours par la couche application et redescend jusqu'à la détection d'une couche défectueuse. | Cette approche est particulièrement adaptée en présence de problèmes plus simples qui sont probablement liés à l'application/ l'utilisateur ou à la couche supérieure. | Si le problème est lié à des couches inférieures, vous avez perdu beaucoup de temps et d'efforts à explorer les couches application supérieures. |

**Exercice**

Des clients se plaignent de ne pouvoir accéder aux pages Web depuis un serveur Web du FAI.

Placez les actions entreprises par le technicien dans la catégorie de méthode de dépannage appropriée.

- Le technicien suspecte qu'un pare-feu soit à l'origine du problème et vérifie la configuration du pare-feu.
- Le technicien vérifie les connexions filaires entre le serveur Web et le commutateur connecté directement.
- Le technicien envoie une requête ping au serveur, puis au commutateur situé sur le site du client.
- Le technicien appelle le client pour déterminer si seules les applications Web sont affectées.
- Le technicien vérifie les témoins lumineux de la carte réseau sur le serveur Web.
- Le technicien vérifie si le serveur dispose de l'entrée DNS appropriée pour la résolution de noms.

Dépannage ascendant

Dépannage descendant

Diviser et conquérir

**Corrigé**

Dépannage ascendant

- Le technicien vérifie les témoins lumineux de la carte réseau sur le serveur Web.
- Le technicien vérifie les connexions filaires entre le serveur Web et le commutateur connecté directement.

Dépannage descendant

- Le technicien vérifie si le serveur dispose de l'entrée DNS appropriée pour la résolution de noms.
- Le technicien appelle le client pour déterminer si seules les applications Web sont affectées.

Diviser et conquérir

- Le technicien envoie une requête ping au serveur, puis au commutateur situé sur le site du client.
- Le technicien suspecte qu'un pare-feu soit à l'origine du problème et vérifie la configuration du pare-feu.

**1.3 Outils de dépannage**

Il est très difficile de dépanner un problème de connectivité réseau, quel qu'en soit le type, sans avoir recours au diagramme du réseau, qui indique notamment les adresses IP, les routes

IP et les périphériques tels que les pare-feu et les commutateurs. Les topologies logiques et physiques sont extrêmement utiles dans les processus de dépannage réseau.

### **Topologies réseau physiques**

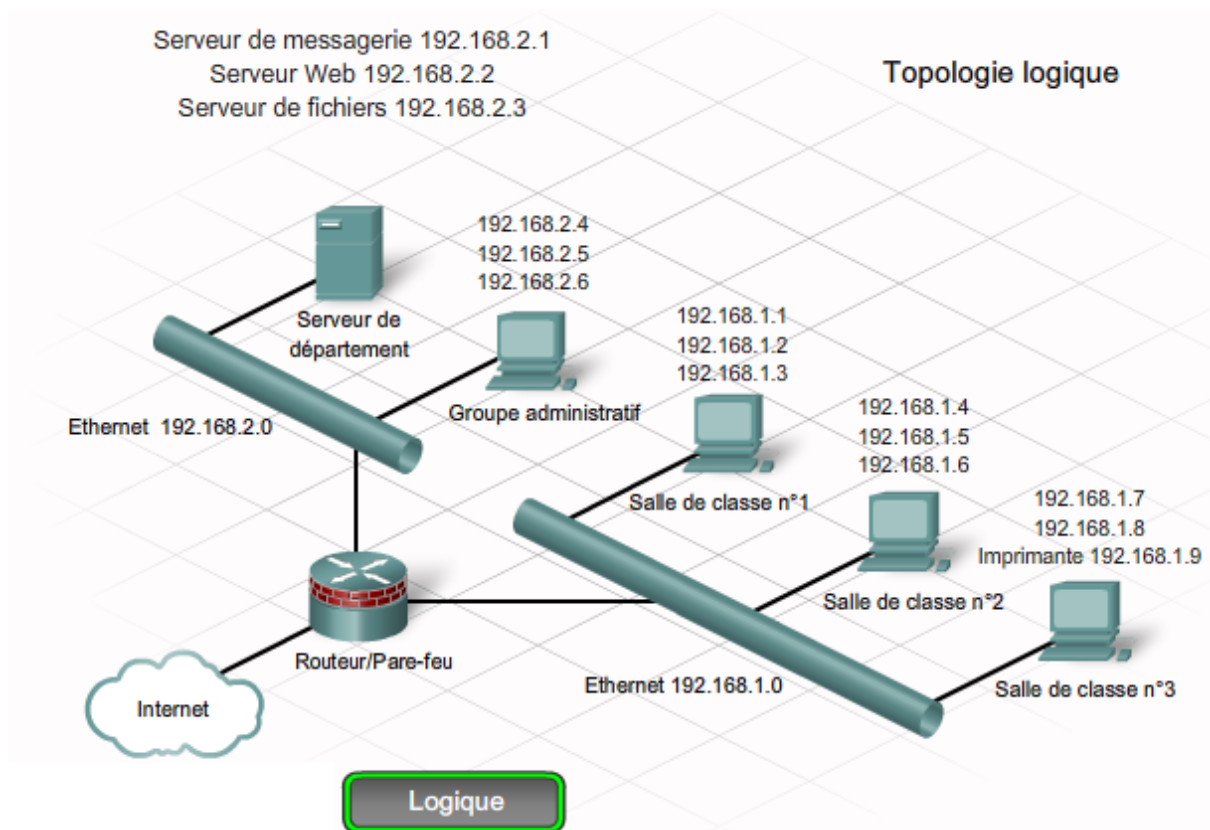
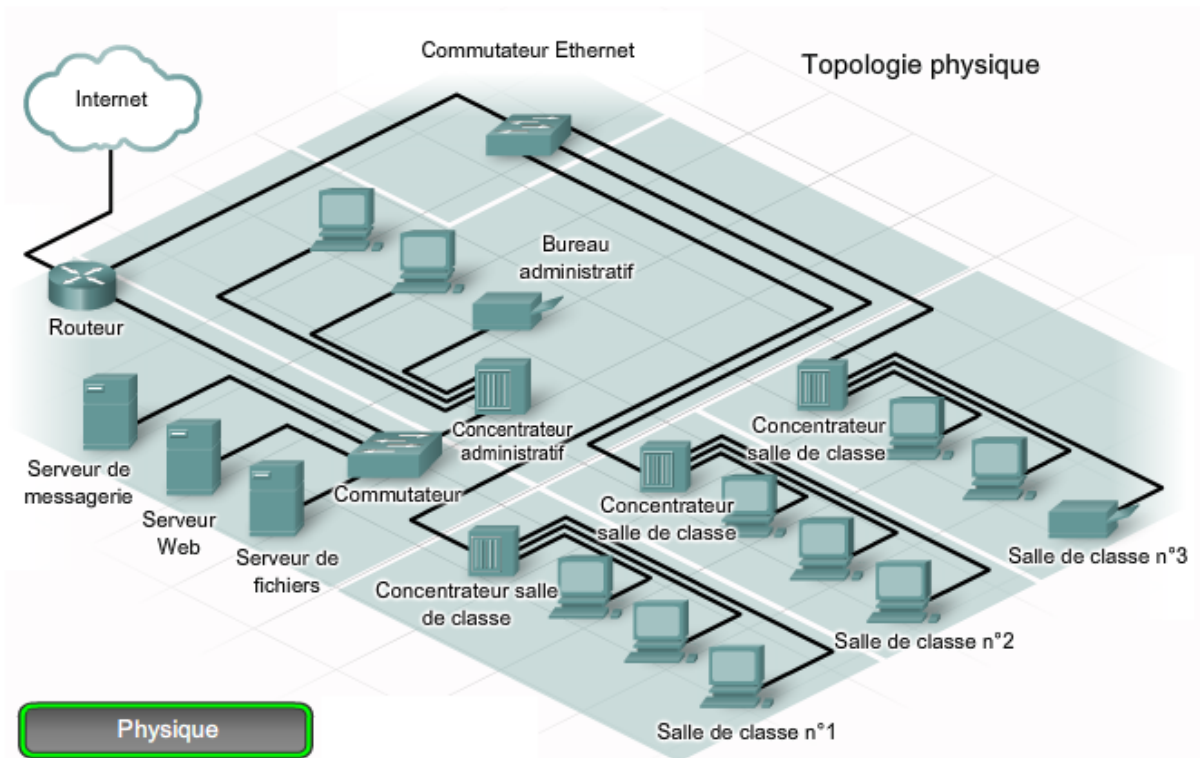
Un diagramme physique du réseau indique la disposition physique des périphériques connectés au réseau. Vous devez savoir comment les périphériques sont physiquement connectés pour pouvoir résoudre des problèmes au niveau de la couche physique, notamment les problèmes de câblage ou de matériel. Les topologies réseau physiques sont généralement constituées des éléments suivants :

- Types de périphériques
- Modèles et fabricants de périphériques
- Emplacements
- Versions du système d'exploitation
- Types et identificateurs de câbles
- Points d'extrémité de câblage

### **Topologies réseau logiques**

Un diagramme logique du réseau indique comment les données sont transférées sur le réseau. Les éléments tels que les routeurs, les serveurs, les concentrateurs, les hôtes et les périphériques de sécurité sont représentés par des symboles. Les topologies réseau logiques sont généralement constituées des éléments suivants :

- Identificateurs de périphériques
- Adresses IP et masques de sous-réseau
- Identificateurs d'interfaces
- Protocoles de routage
- Routes statiques et par défaut
- Protocoles de liaison de données
- Technologies de réseau étendu

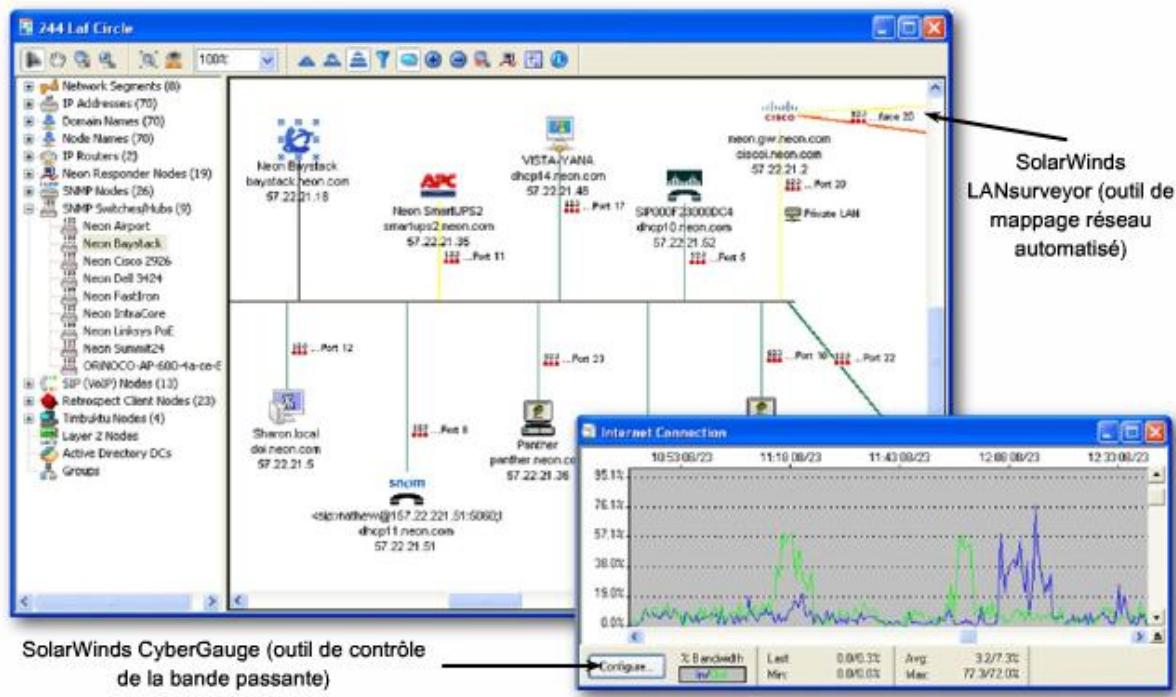


Outre les schémas de réseau, d'autres outils peuvent s'avérer utiles dans le dépannage efficace des problèmes et du manque de performances d'un réseau.



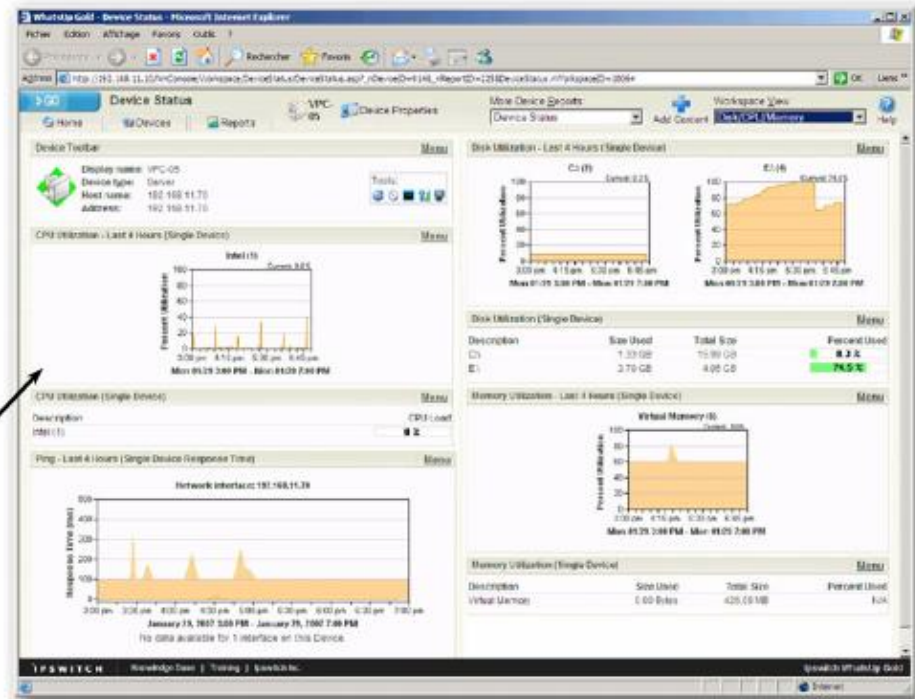
## Documentation du réseau et outils de création de ligne de base

La documentation du réseau et les outils de création de ligne de base sont disponibles pour les systèmes d'exploitation Windows, Linux et UNIX. CiscoWorks peut vous aider à dessiner le diagramme du réseau, à mettre à jour la documentation du matériel et des logiciels réseau et à mesurer de façon rentable l'utilisation de la bande passante sur le réseau. Ces outils logiciels sont souvent dotés de fonctions de contrôle et de rapport qui permettent d'établir la ligne de base du réseau.



## Outils de système d'administration de réseaux (NMS)

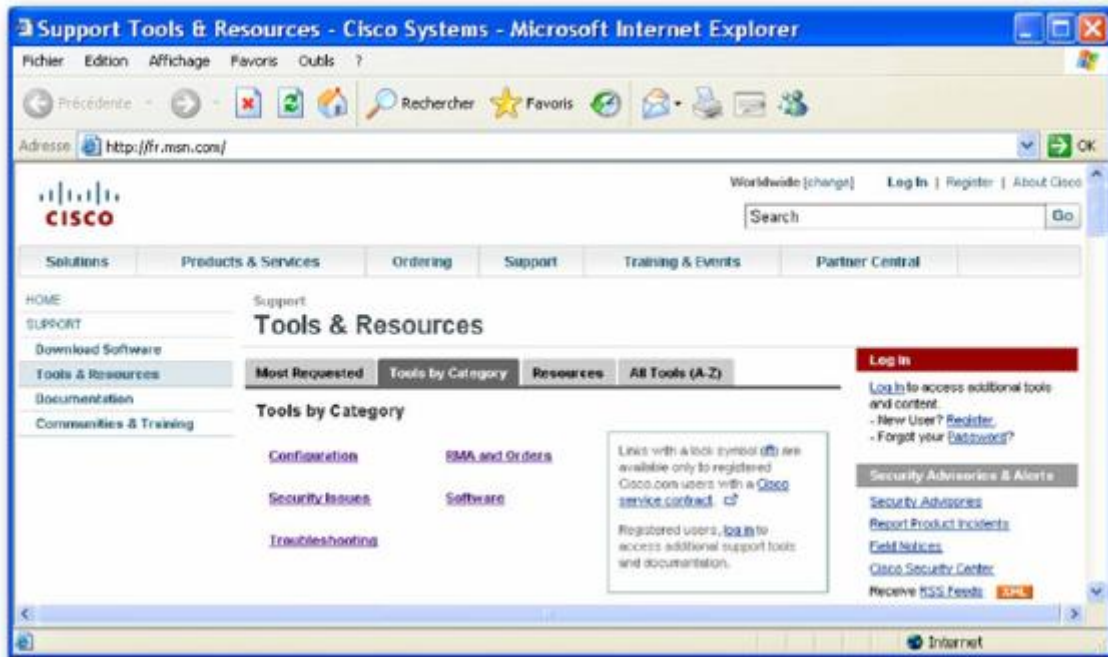
Les outils de système d'administration de réseaux permettent de surveiller les performances du réseau. Ils affichent une représentation graphique des périphériques réseau. Si une défaillance survient, l'outil peut en localiser la source et déterminer si elle a été provoquée par une activité ou un logiciel malveillants, ou par un périphérique défectueux. CiscoView, HP Openview, Solar Winds et WhatsUp Gold sont des exemples d'outils d'administration de réseaux couramment utilisés.



Écran d'état du périphérique NMS fourni par le logiciel WhatsUp Gold

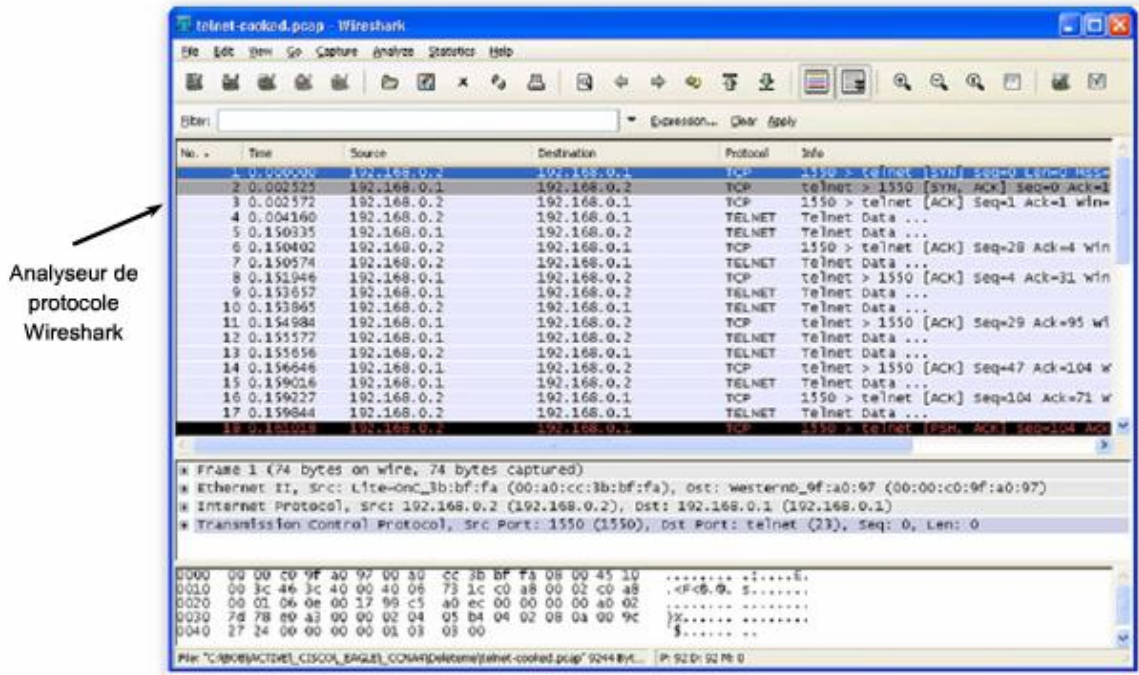
### Bases de connaissances

Les bases de connaissances des fabricants de périphériques réseau sont devenues une source d'informations indispensable. En associant les bases de connaissances en ligne aux moteurs de recherche sur Internet, un administrateur réseau a accès à de nombreuses informations basées sur l'expérience.



### Analyseurs de protocoles

Un analyseur de protocole décode les différentes couches de protocole dans une trame enregistrée et présente ces informations sous un format relativement facile à utiliser. Les analyseurs de protocoles peuvent capturer le trafic réseau afin de l'analyser. Le résultat capturé peut être filtré pour afficher un trafic spécifique ou certains types de trafic, sur base de critères définis. Vous pouvez par exemple afficher tout le trafic d'un périphérique particulier. Les analyseurs de protocoles, tels que Wireshark, fournissent des informations de dépannage détaillées sur les données communiquées sur le réseau. La configuration et l'arrêt d'une session TCP entre deux hôtes constitue un exemple des types d'informations affichables via un analyseur de protocoles.



**Travaux pratiques : Utiliser Wireshark pour observer la connexion TCP en trois étapes**

Certaines défaillances constatées au niveau des couches inférieures du modèle OSI ne sont pas facilement identifiables par les outils logiciels. Par conséquent, il est parfois nécessaire d'utiliser des outils matériels de dépannage tels que des testeurs de câble, des multimètres et des analyseurs réseau.

**Testeurs de câble**

Les testeurs de câble sont des appareils portables spécialisés qui permettent de tester différents types de câblage de communication de données. Les testeurs de câble peuvent être utilisés pour détecter des câbles rompus ou croisés et des connexions court-circuitées ou mal jumelées. Des testeurs plus sophistiqués, tels que les TDR (Time-Domain Reflectometer) permettent de mesurer la distance qui les sépare d'une coupure d'un câble. Les testeurs de câble permettent également de déterminer la longueur d'un câble.



Testeur LinkRunner Pro de Fluke Networks



Testeur de qualification CableIQ de Fluke Networks

## Multimètres numériques

Les multimètres numériques sont des instruments qui permettent de mesurer directement les valeurs électriques de la tension, du courant et de la résistance. Dans le cas d'un dépannage réseau, la majorité des tests du multimètre implique la vérification de la tension d'alimentation et la vérification que les périphériques réseau sont bien alimentés.



Multimètre numérique Fluke série 179

## Analyseurs réseau portables



En branchant un analyseur réseau à un commutateur sur le réseau, un ingénieur réseau peut déterminer les utilisations moyenne et maximale du segment. L'analyseur permet également d'identifier les périphériques à la base du trafic réseau le plus important, d'analyser le trafic réseau par protocole et d'afficher les détails de l'interface. Les analyseurs réseau s'avèrent très utiles pour la résolution de problèmes provenant de logiciels malveillants ou d'attaques de déni de service.



Analyseur réseau intégré OptiView™ Series III de Fluke Networks

#### 1.4 Guide de certification du participant

##### **Guide du participant CCENT**

**Cliquez sur l'icône des travaux pratiques pour télécharger la section 9.1 du Guide du participant CCENT.**

## 2 Dépannage de problèmes des couches 1 et 2

### 2.1 Problèmes au niveau des couches 1 et 2

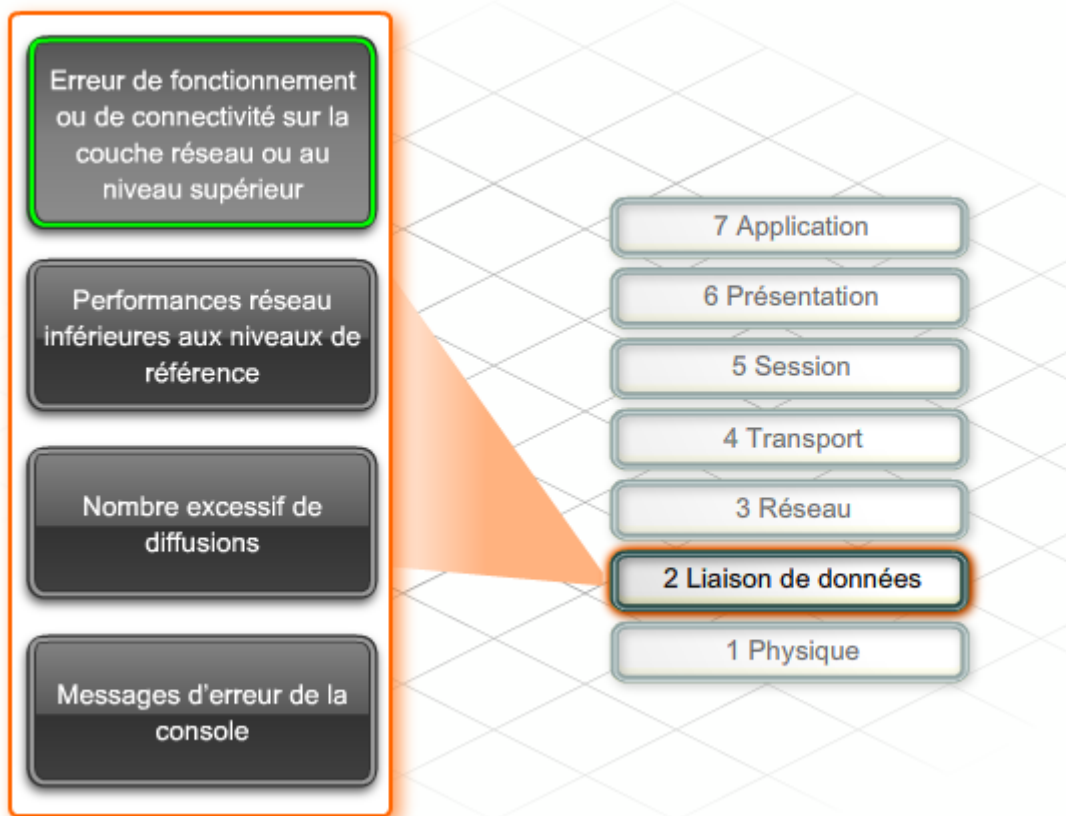
Les couches liaison de données et physique englobent les fonctions matérielles et logicielles. Le fonctionnement de toutes les communications réseau repose sur les technologies de ces couches. Un ingénieur réseau doit être capable d'isoler et de corriger rapidement les problèmes survenant au niveau de ces couches.

La couche physique, ou couche 1, est responsable des spécifications physiques et électriques de la transmission de bits d'un hôte à l'autre sur le support physique, qu'il soit filaire ou sans

fil. Les problèmes réseau survenant au niveau de la couche 1 peuvent provoquer une perte de connectivité du réseau, ou diminuer les performances réseau.

Les types de problèmes qui surviennent au niveau de la couche 1 sont directement liés au type de technologie utilisée. Par exemple, Ethernet est une technologie à accès multiple. Les protocoles Ethernet utilisent un algorithme pour détecter l'absence de signal dans le câblage pour initier une transmission. Toutefois, il est possible que deux périphériques initiant un envoi exactement en même temps provoquent une collision. En cas de collision, tous les périphériques interrompent la transmission pendant une durée aléatoire avant de poursuivre la transmission. Capable de détecter les collisions et de leur répondre, Ethernet est souvent appelé CSMA/CD (Carrier Sense Multiple Access with Collision Detection).

Notez toutefois que les collisions excessives peuvent provoquer la diminution des performances réseau. Les collisions peuvent devenir un problème plus important sur les supports partagés, tels qu'un réseau de concentrateurs, que sur les ports commutés.



La couche liaison de données, ou couche 2, spécifie le mode de formatage des données transmises sur le réseau. Elle régule également les autorisations d'accès au réseau. La couche 2 fournit le lien entre les fonctions logicielles de la couche réseau et les composants matériels de couche 1 pour les applications de réseau local et étendu. Pour résoudre efficacement les problèmes de couche 1 et 2, les ingénieurs doivent disposer des connaissances et compétences nécessaires en matière de normes de câblage, d'encapsulation et de verrouillage de trame.

Après que l'ingénieur a vérifié que la couche 1 est fonctionnelle, il doit pouvoir déterminer si le problème provient de la couche 2 ou d'une couche supérieure. Par exemple, si un hôte peut

envoyer une requête ping à l'adresse de bouclage local, 127.0.0.1, mais qu'il ne peut accéder aux autres services du réseau, le problème peut être lié au verrouillage de trame de la couche 2, ou provenir d'une carte d'interface incorrectement configurée. Les analyseurs de réseau et d'autres outils en ligne peuvent localiser la source d'un problème de couche 2. Dans certains cas, un périphérique reconnaît qu'un problème s'est produit au niveau de la couche 2 et envoie un message d'alerte sur la console.

Exercice

Faites correspondre le problème de couche 1 ou de couche 2 avec un symptôme possible.

Alimentation électrique ou alimentation de secours défectueuse

Conflit du mode bidirectionnel

Aucun message de test d'activité reçu

Trop grand nombre d'hôtes dans un segment de réseau partagé

Câble lâche

Conflit d'encapsulation

Perte intermittente de connectivité

Collisions excessives sur une interface

Message de console indiquant la désactivation d'un protocole

**Corrigé**

Perte intermittente de connectivité

Alimentation électrique ou alimentation de secours défectueuse

Câble lâche

Collisions excessives sur une interface

Conflit du mode bidirectionnel

Trop grand nombre d'hôtes dans un segment de réseau partagé

Message de console indiquant la désactivation d'un protocole

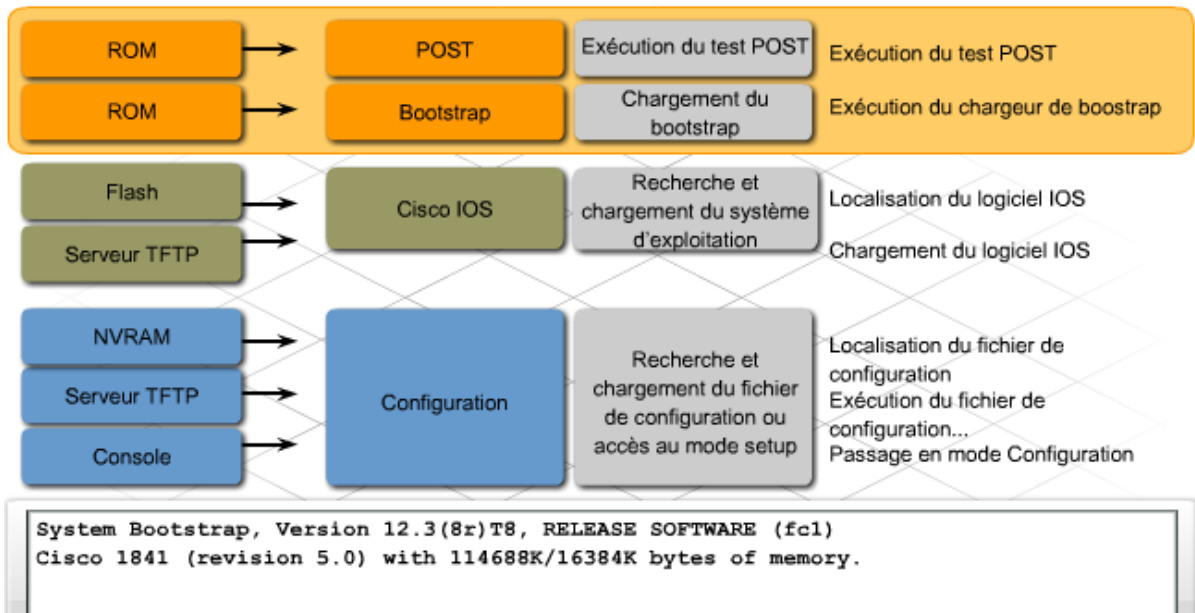
Aucun message de test d'activité reçu

Conflit d'encapsulation

## 2.2 Dépannage matériel des périphériques et des erreurs d'amorçage

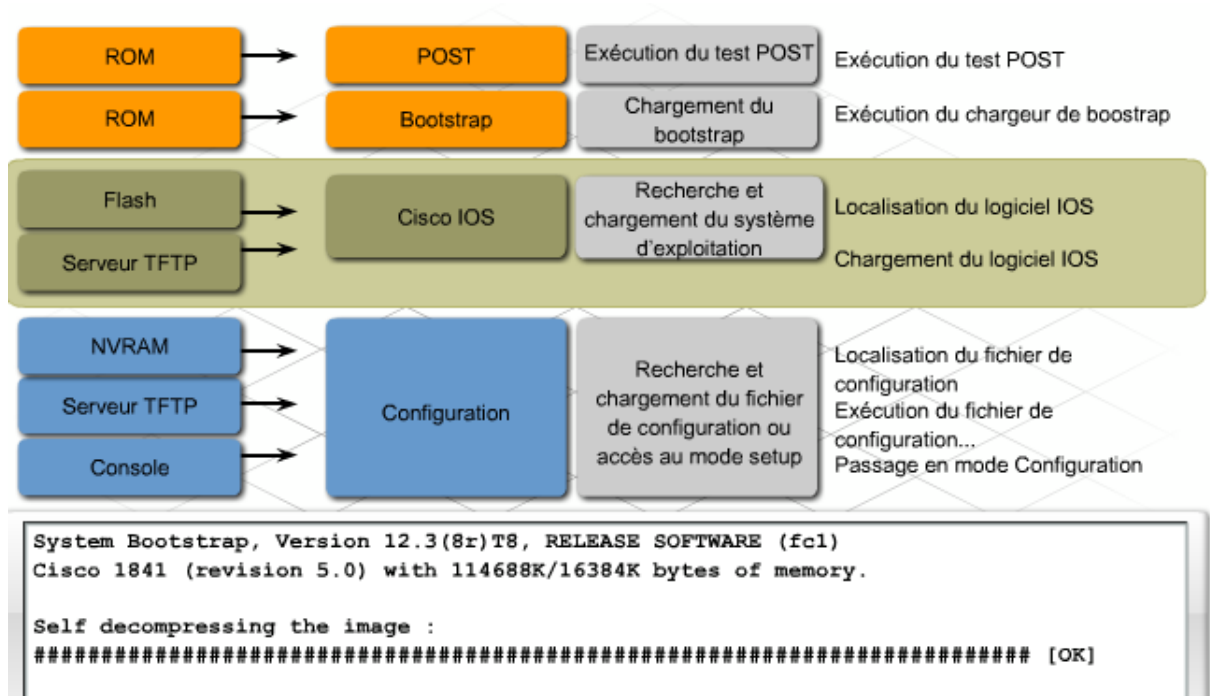
Des problèmes réseau surviennent souvent après le redémarrage d'un périphérique. Un redémarrage peut survenir de façon involontaire, après une mise à niveau, ou une coupure de courant. Pour résoudre les problèmes de défaillance matérielle et les erreurs d'amorçage, il convient tout d'abord d'examiner le processus utilisé par les périphériques Cisco IOS lors du démarrage. Le processus d'amorçage se compose de trois étapes :

### 1. Exécution du test POST et chargement du programme d'amorçage

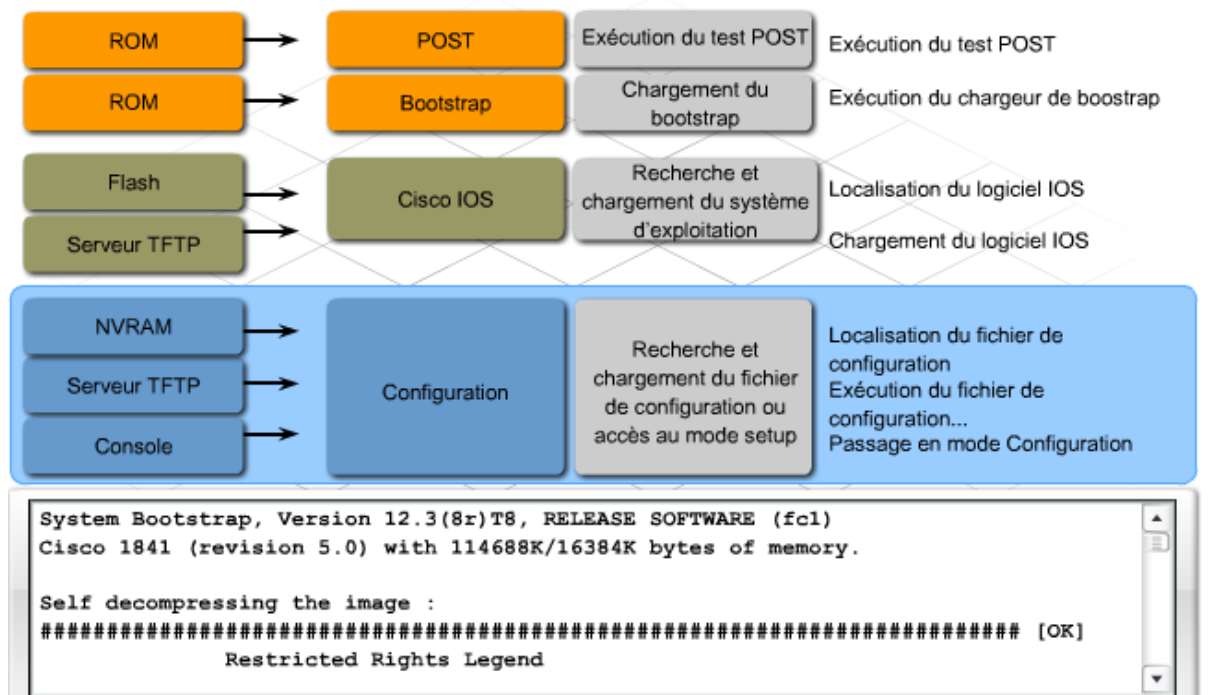


### 2. Localisation et chargement du logiciel Cisco IOS





### 3. Recherche et chargement du fichier de configuration initiale ou accès au mode Assistant de configuration



Lors de l'amorçage d'un périphérique réseau Cisco, il est conseillé d'observer les messages de la console affichés lors de la séquence d'amorçage. Une fois le logiciel Cisco IOS chargé, l'ingénieur peut utiliser les commandes permettant de vérifier si les composants matériels et logiciels sont parfaitement opérationnels.

La commande **show version** affiche la version du système d'exploitation et indique si tous les composants matériels des interfaces sont reconnus.

La commande **show flash** affiche le contenu de la mémoire Flash, y compris le fichier image de Cisco IOS. Il affiche également la quantité de mémoire Flash actuellement utilisée et le pourcentage de mémoire disponible.

La commande **show ip interfaces brief** affiche l'état opérationnel des interfaces du périphérique et les adresses IP attribuées.

Les commandes **show running-configuration** et **show startup-configuration** permettent de vérifier si toutes les commandes de configuration ont été reconnues lors du rechargement.

Lorsqu'un périphérique rencontre un problème d'amorçage et provoque une panne du réseau, remplacez le périphérique par un périphérique valide connu afin de restaurer les services des utilisateurs. Une fois les services restaurés, prenez le temps nécessaire pour dépanner et réparer le périphérique défectueux.

Après l'amorçage du routeur, le LED vert s'affiche. Si une erreur survient au cours du processus d'amorçage, les périphériques Cisco exécutent des actions par défaut, destinées au rétablissement après erreur, par exemple le passage en mode ROMmon. Il existe cinq erreurs d'amorçage fréquentes, auxquelles des stratégies de dépannage sont associées.

### **Échec du test POST du périphérique**

Lorsque le périphérique échoue au test POST, aucun résultat ne s'affiche sur l'écran de la console. De plus, les LED système changent de couleur ou clignotent, selon le type du périphérique. Pour obtenir l'explication du fonctionnement des LED, consultez la documentation du périphérique. En cas d'échec du test POST, éteignez le périphérique et débranchez-le, puis enlevez tous les modules d'interface. Réamorcez ensuite le périphérique. Si le test POST échoue à nouveau, contactez le service d'assistance du fabricant du périphérique. Si le test POST aboutit lorsque les modules d'interface ne sont pas installés, cela signifie qu'un module interface est probablement défectueux. Débranchez et réinstallez chaque module individuellement, puis réamorcez pour détecter celui qui est défaillant. Une fois le module défaillant identifié, remplacez-le par un module valide connu et redémarrez le périphérique.

### **L'image Cisco IOS en Flash est corrompue.**

Si le fichier image de Flash est corrompu ou manquant, le chargeur d'amorçage ne trouvera aucun fichier Cisco IOS valide à charger. Certains périphériques Cisco IOS ont une image dotée de fonctionnalités limitées, qui peut être chargée et exécutée en l'absence d'image dans la Flash ou dans un autre emplacement spécifié. Cette image s'appelle « boothelper », ou auxiliaire d'amorçage. Les images de cet auxiliaire ne sont pas toujours dotées des fonctionnalités nécessaires à l'exécution des commandes de configuration requises pour la remise en service du périphérique. En l'absence de boothelper, le périphérique passe automatiquement en mode ROMmon. Utilisez les commandes ROMmon pour recharger l'image Cisco IOS correcte depuis un serveur TFTP.

| 1841 Voyants LED au processus de démarrage |                 |                                                                                                                                                                                     |
|--------------------------------------------|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LED                                        | Couleur         | État                                                                                                                                                                                |
| Voyant SYS PWR                             | Vert            | Le processus de démarrage du routeur est terminé et le logiciel est opérationnel. Clignotement lent et continu lorsque le système est en cours de démarrage ou dans le moniteur ROM |
| Voyant SYS ACT                             | Vert            | Clignotant lors de la transmission ou réception de paquets sur une interface de réseau étendu ou local, ou lors de la surveillance de l'activité du système                         |
| Voyant CF                                  | Vert clignotant | La mémoire flash est occupée. Ne retirez pas la carte mémoire CompactFlash lorsque ce voyant est allumé.                                                                            |

**La mémoire n'est pas reconnue ou est défectueuse.**

Si la mémoire disponible est insuffisante pour décompresser l'image, le périphérique fait défiler les messages d'erreur à grande vitesse, ou se bloque sur le processus d'amorçage. Le périphérique peut démarrer en mode ROMmon, en exécutant la commande **Ctrl-Break** lors du processus de démarrage. En mode ROMmon, les commandes peuvent être exécutées pour déterminer l'état de la mémoire. Dans certains cas, la mémoire doit être remplacée ou augmentée pour que le périphérique puisse fonctionner correctement.

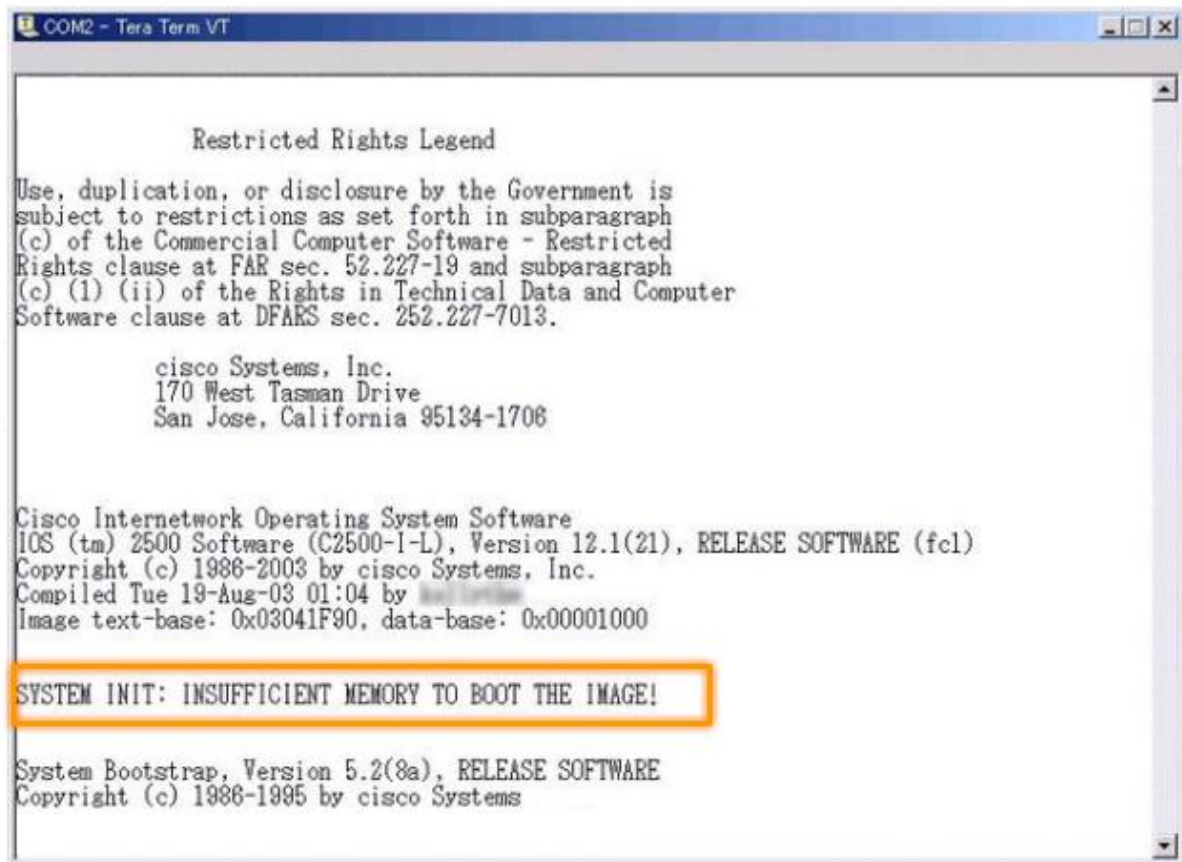
**Les modules d'interface ne sont pas reconnus.**

Il se peut que des modules d'interface défectueux ou incorrectement configurés ne soient pas reconnus lors du test POST ou du chargement de Cisco IOS. Dans ce cas, la liste des interfaces disponibles affichée via la commande show version ne correspond pas aux modules physiquement installés. En présence d'un nouveau module d'interface, vérifiez s'il est pris en charge par la version de Cisco IOS installée et que vous disposez de suffisamment de mémoire pour la prise en charge du module. Il est recommandé de toujours éteindre le périphérique et de le débrancher avant de réinstaller le module dans le périphérique pour déterminer si le problème provient d'une défaillance matérielle. Une fois rebranché, si le module n'est pas reconnu lors du processus de réamorçage, remplacez-le par un module valide connu.

**Le fichier de configuration est corrompu ou manquant.**

Si aucun fichier de configuration valide n'est trouvé, certains périphériques Cisco exécutent un utilitaire d'installation automatique. Cet utilitaire diffuse une requête TFTP pour obtenir un fichier de configuration. Sur d'autres périphériques, une boîte de dialogue de configuration initiale s'affiche immédiatement. Cette boîte de dialogue est appelée « utilitaire de configuration » ou « mode Assistant de configuration ». Les périphériques équipés de l'utilitaire d'installation automatique passent également en mode Assistant de configuration en cas de non réponse du serveur TFTP après cinq tentatives. Utilisez TFTP ou la

configuration manuelle pour recharger ou recréer la configuration. Les périphériques ne transmettront aucun trafic en l'absence d'une configuration valide.



```
COM2 - Tera Term VT

Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-I-L), Version 12.1(21), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Tue 19-Aug-03 01:04 by XXXXXXXXXX
Image text-base: 0x03041F90, data-base: 0x00001000

SYSTEM INIT: INSUFFICIENT MEMORY TO BOOT THE IMAGE!

System Bootstrap, Version 5.2(8a), RELEASE SOFTWARE
Copyright (c) 1986-1995 by cisco Systems
```

### 2.3 Dépannage des erreurs de câblage et de ports de périphériques

Les erreurs d'interface du routeur sont souvent le premier symptôme des erreurs de câblage ou de connectivité des couches 1 et 2. Pour dépanner ces erreurs, commencez par examiner les statistiques enregistrées sur l'interface problématique, en utilisant la commande **show interfaces**, et vérifiez l'état des interfaces en utilisant la commande **show ip interface brief**.

Le résultat de la commande **show ip interface brief** comporte un résumé des interfaces du périphérique, notamment l'adresse IP et l'état de l'interface.

- **État up/up** : indique un fonctionnement normal et signale que le support et le protocole de couche 2 sont opérationnels.
- **État down/down** : signale la présence d'un problème de connectivité ou de support.
- **État up/down** : indique que le support est correctement connecté, mais que le protocole de couche 2 ne fonctionne pas correctement ou est mal configuré.

Problèmes liés au câblage ou au support et pouvant induire un résultat down/down :

- Câble lâche ou tension du câble trop élevée : si l'ensemble des broches ne peut initier une bonne connexion, le circuit est désactivé.
- Raccordement incorrect : assurez-vous du respect de la norme appropriée, et vérifiez si toutes les broches sont correctement raccordées au connecteur.

- Connecteur de l'interface série endommagé : des broches de la connexion de l'interface sont courbées ou manquantes.
- Blocage ou court-circuit dans le câble : en cas de dysfonctionnement du circuit, l'interface ne peut détecter les signaux corrects.

Les problèmes de couche 2 les plus courants pouvant induire un résultat up/down sont les suivants :

- L'encapsulation n'est pas correctement configurée.
- Aucun message de test d'activité n'est reçu sur l'interface.

```
R1#show ip interface brief
Interface          IP-Address      OK? Method Status          Protocol
FastEthernet0/0    192.168.1.1     YES manual up              up
FastEthernet0/1    unassigned      YES manual administratively down down
Serial0/0/0        192.168.2.1     YES manual up              up
Serial0/0/1        unassigned      YES manual administratively down down
Vlan1              unassigned      YES manual administratively down down
```

Dans certains cas, les erreurs enregistrées sur le support ne sont pas suffisamment graves pour entraîner une panne du circuit, mais elles peuvent entraîner une diminution sensible des performances. La commande **show interfaces** fournit des informations de dépannage supplémentaires, qui peuvent vous aider à identifier les erreurs du support.

Le résultat de la commande **show interfaces** comprend les données suivantes :

- **Bruit excessif** : la présence d'un nombre élevé d'erreurs CRC et d'un nombre peu élevé de collisions est une indication de bruit excessif (parasites). Les erreurs CRC indiquent généralement une erreur de support ou de câblage. Les causes courantes sont les interférences électriques, des connexions lâches ou endommagées, ou l'utilisation d'un type de câble incorrect.
- **Collisions excessives** : les collisions surviennent généralement en mode bidirectionnel non simultané, ou sur des connexions Ethernet de supports partagés. Des câbles endommagés peuvent provoquer des collisions excessives.
- **Trames tronquées excessives** : des cartes réseau défaillantes sont généralement à l'origine des trames tronquées, mais elles peuvent également être occasionnées par les mêmes erreurs que les collisions excessives.
- **Collisions tardives** : un réseau correctement conçu et configuré ne doit jamais présenter de collisions tardives. Les collisions tardives sont généralement provoquées par des longueurs de câbles excessives. Les conflits du mode bidirectionnel peuvent également en être la cause.

| Solution liée au bruit excessif (parasites) |                                                                                                                                                                                                                               |
|---------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Étape 1                                     | Utilisation de la commande show interface pour déterminer l'état des interfaces Ethernet La présence d'un nombre élevé d'erreurs CRC et d'un nombre peu élevé de collisions est une indication de bruit excessif (parasites). |
| Étape 2                                     | Inspection des câbles pour localiser les défauts ou sources d'interférences                                                                                                                                                   |
| Étape 3                                     | Vérification du câblage et des normes de raccordement par rapport à la vitesse de l'interface                                                                                                                                 |
| Étape 4                                     | Vérification qu'un câblage de catégorie 5e ou supérieure est utilisé si 1000BASE-TX est utilisé                                                                                                                               |

| Solution liée aux collisions excessives |                                                                                                                                                                                             |
|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Étape 1                                 | Utilisation de la commande show interface pour déterminer le taux de collisions Le nombre total de collisions, par rapport au nombre total de paquets de sortie, doit être de 1 % ou moins. |
| Étape 2                                 | Utilisation d'un TDR pour localiser les câbles endommagés                                                                                                                                   |

| Trames tronquées excessives |                                                                                                                                                                                                                                |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Étape 1                     | Dans un environnement Ethernet partagé, les trames tronquées sont presque toujours provoquées par des collisions. Si le taux de collisions est élevé, reportez-vous à la section relative au problème "Collisions excessives". |
| Étape 2                     | Si les trames tronquées surviennent lorsque le taux de collisions n'est pas élevé, ou dans un environnement Ethernet commuté, elles proviennent probablement d'un logiciel défectueux sur une carte réseau.                    |
| Étape 3                     | Utilisation d'un analyseur de protocole pour tenter de déterminer l'adresse source des trames tronquées                                                                                                                        |

| Collisions tardives |                                                                                                                                                                                                                                                                                                                  |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Étape 1             | Utilisation d'un analyseur de protocole pour rechercher la cause des collisions tardives Les collisions tardives ne doivent pas survenir dans un réseau Ethernet correctement configuré. Elles surviennent généralement lorsque les câbles Ethernet sont trop longs ou en cas de conflit du mode bidirectionnel. |
| Étape 2             | Vérification du diamètre du réseau par rapport aux spécifications                                                                                                                                                                                                                                                |

**Travaux pratiques :** Utiliser les commandes **show ip interface brief** et **show interfaces** pour identifier les erreurs possibles de câblage ou de support

#### 2.4 Dépannage des problèmes de connectivité du réseau local

Le dépannage d'un réseau local est généralement associé à des problèmes de commutateurs, car la majorité des utilisateurs de réseaux locaux se connectent au réseau via les ports de commutation. Un grand nombre de commandes **show** de Cisco IOS peuvent être utilisées sur les commutateurs pour collecter des informations de dépannage. De surcroît, chaque port d'un commutateur est pourvu d'un indicateur LED fournissant des informations de dépannage utiles.

La première étape du dépannage des problèmes de connectivité du réseau local consiste à vérifier si le port de commutateur connecté à l'utilisateur est actif et si les indicateurs LED appropriés sont allumés. Si le commutateur est équipé d'un accès physique, examinez les LED du port, qui vous indiqueront l'état de la liaison et vous signaleront les éventuels états d'erreur (si le LED s'allume en rouge ou en orange). Vérifiez si les deux extrémités de la connexion sont dotées d'une liaison.

En l'absence de voyant de liaison, assurez-vous que le câble est connecté aux deux extrémités et qu'il est connecté au port approprié. Vérifiez que les deux périphériques sont allumés, et qu'ils ne présentent aucune erreur d'amorçage. Remplacez les câbles de raccordement par des câbles valides connus et vérifiez si les terminaisons de câble sont appropriées au type de connectivité souhaitée. Si les voyants de liaison sont toujours éteints, vérifiez si le port n'a pas été désactivé par l'administrateur. Utilisez la commande **show running-config interface** pour afficher les paramètres configurés sur un port de commutateur :

```
switch#sh run interface fastEthernet 4/2
!  
interface FastEthernet4/2  
shutdown  
duplex full  
speed 100  
end
```

Même si le voyant de liaison est allumé, cela ne garantit pas que le câble est fonctionnel à 100 %. Il se peut que le câble soit endommagé, ce qui peut provoquer des problèmes de performances intermittents. En règle générale, cette situation est identifiée par les commandes **show** de Cisco IOS pour déterminer si le port présente un grand nombre d'erreurs de paquets, ou si le port est constamment instable (pertes et restaurations constantes de la liaison).

Les commandes **show version** et **show interfaces**, exécutées sur un commutateur, fournissent des informations similaires à ces mêmes commandes exécutées sur un routeur. Pour accéder rapidement aux statistiques d'erreurs du port de commutation, utilisez la commande **show interface port counters errors**.

Les conflits de bidirectionnalité sont plus fréquents sur les commutateurs que sur les routeurs. La plupart des périphériques sont configurés pour autonégocier les paramètres de bidirectionnalité et de vitesse. Si l'un des deux périphériques d'une liaison est configuré pour l'autonégociation et que l'autre est configuré manuellement avec des paramètres de bidirectionnalité et de vitesse, des conflits peuvent survenir et entraîner des collisions et des abandons de paquets.



Pour afficher les paramètres de bidirectionnalité et de vitesse sur un port et savoir si la fonction de négociation manuelle ou automatique est activée, exécutez la commande **show interface port status**.

Si le conflit survient entre deux périphériques Cisco dont le protocole CDP (Cisco Discovery Protocol) est activé, des messages d'erreur CDP s'affichent sur la console ou dans le tampon d'ouverture de session des deux périphériques. CDP permet de détecter les erreurs et d'afficher les statistiques de port et de système sur les périphériques Cisco avoisinants.

Pour corriger les conflits de bidirectionnalité, définissez l'autonégociation de la vitesse et du mode bidirectionnel. Si la négociation ne produit pas les résultats escomptés, définissez manuellement les paramètres de correspondance de vitesse et de mode bidirectionnel sur chaque périphérique.

```
Jun  2 11:16:45 %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on
FastEthernet6/2 (not half duplex), with TBA04251336 3/2 (half duplex).
```

Message d'erreur indiquant la détection d'un conflit de mode bidirectionnel simultané.

```
Switch# sh interfaces fas 6/1 status
Port Name      Status      Vlan    Duplex  Speed  Type
Fa6/1          notconnect  1       auto    auto   10/100BaseTX
```

**Exercice Packet Tracer** : Configurer un réseau commuté et résoudre les conflits de bidirectionnalité

**Travaux pratiques** : Vérifier la connectivité à l'aide des LED et des commandes show

## **2.5 Dépannage des problèmes de connectivité d'un réseau étendu**

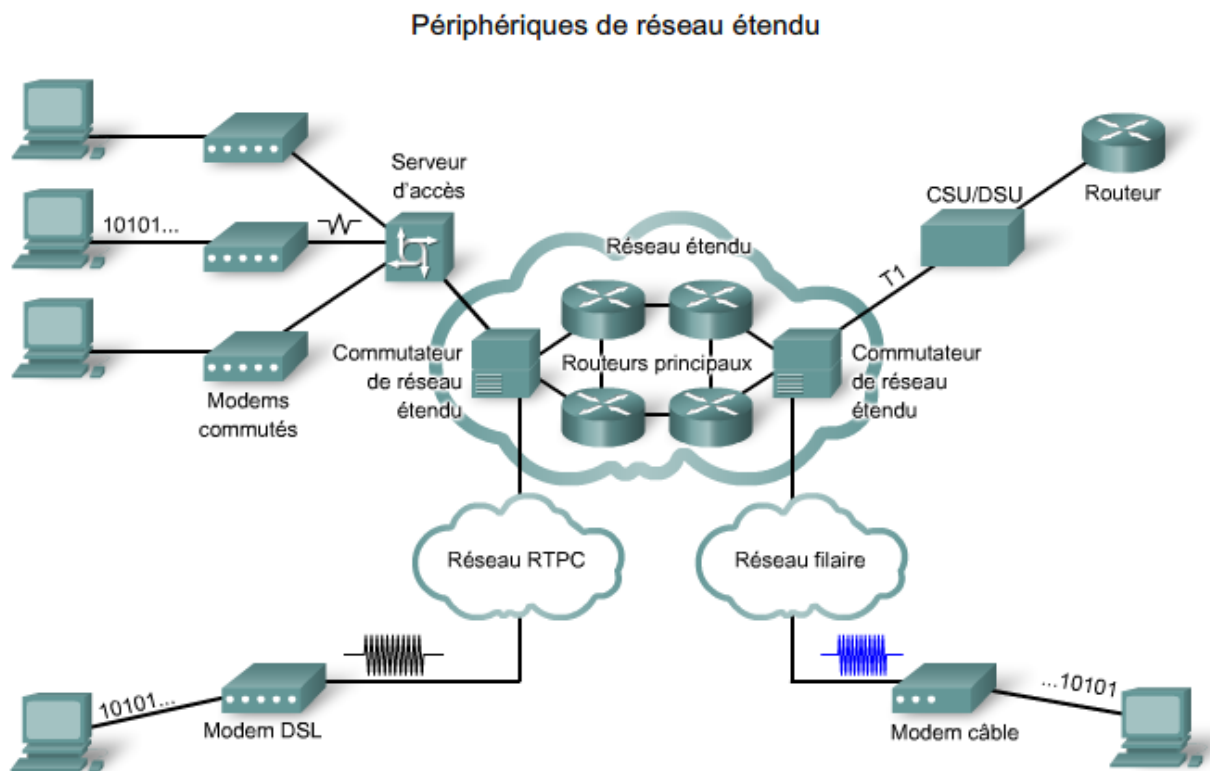
Le dépannage d'une connexion série de réseau étendu diffère de celui d'une connexion Ethernet de réseau local. En règle générale, la connectivité de réseau étendu repose sur des équipements et des supports qui appartiennent et sont gérés par un fournisseur de services de télécommunications. De ce fait, il est essentiel que les ingénieurs sachent comment dépanner



les équipements placés chez le client par l'opérateur et comment communiquer ces résultats au fournisseur de services de télécommunications.

La plupart des problèmes d'interfaces série et de lignes peuvent être identifiés et corrigés à l'aide des informations provenant du résultat de la commande **show interfaces serial**. Les connexions série peuvent présenter des problèmes causés par des erreurs de paquets, des erreurs de configuration ou des conflits d'encapsulation et de synchronisation. Étant donné que les connexions série des réseaux étendus dépendent généralement d'une unité CSU/DSU ou d'un modem pour la synchronisation, ces périphériques doivent être examinés lors du dépannage des lignes série. Sur les réseaux prototype, un routeur peut être configuré pour offrir des fonctions de synchronisation DCE (équipement de communication de données), ce qui permet de supprimer le CSU/DSU ou le modem de la connexion.

Pour résoudre efficacement les problèmes de connectivité série des réseaux étendus, il est important de connaître le type de modem ou d'unité CSU/DSU installé, et comment placer le périphérique dans un état de bouclage à des fins de test.



La ligne d'état de l'interface de la commande **show interfaces serial** peut afficher six états possibles :

- **Serial x is down, line protocol is down (DTE mode)** : lorsque l'interface série du routeur ne peut détecter aucun signal sur la ligne, cela signifie que la ligne et le protocole de couche 2 sont tous deux désactivés.

- **Serial x is up, line protocol is down (DTE mode)** : lorsque l'interface série du routeur ne reçoit aucun message de test d'activité, ou en présence d'une erreur d'encapsulation, le protocole de couche 2 est désactivé (down).
- **Serial x is up, line protocol is down (DCE mode)** : lorsque le routeur fournit le signal d'horloge, si un câble DCE est relié, mais qu'aucune fréquence d'horloge n'est configurée, le protocole de couche 2 est désactivé (down).
- **Serial x is up, line protocol is up (looped)** : il est fréquent de placer un circuit dans une condition de bouclage pour tester la connectivité. Si l'interface série reçoit à nouveau ses propres signaux dans le circuit, la ligne est consignée comme bouclée.
- **Serial x is up, line protocol is down (disabled)** : en présence d'un taux d'erreur élevé, le routeur peut placer la ligne dans un mode de protocole désactivé. Ce type de problème est généralement d'origine matérielle.
- **Serial x is administratively down, line protocol is down** : une interface désactivée par l'administrateur est celle qui est configurée avec la commande **shutdown**. La seule chose généralement nécessaire pour résoudre cette erreur est d'exécuter la commande **no shutdown** sur l'interface. Si l'interface ne s'active pas en exécutant la commande **no shutdown**, recherchez un message d'adresse IP dupliquée dans les messages de la console. S'il existe une adresse IP dupliquée, corrigez le problème et exécutez à nouveau la commande **no shutdown**.
- **Serial x is up, line protocol is up** : l'interface fonctionne comme prévu.

**Exercice Packet Tracer** : Résolution des conflits d'encapsulation de réseau étendu

**Travaux pratiques** : Vérifier la connectivité des réseaux étendus à l'aide des LED et des commandes show

### 2.6 Guide de certification du participant

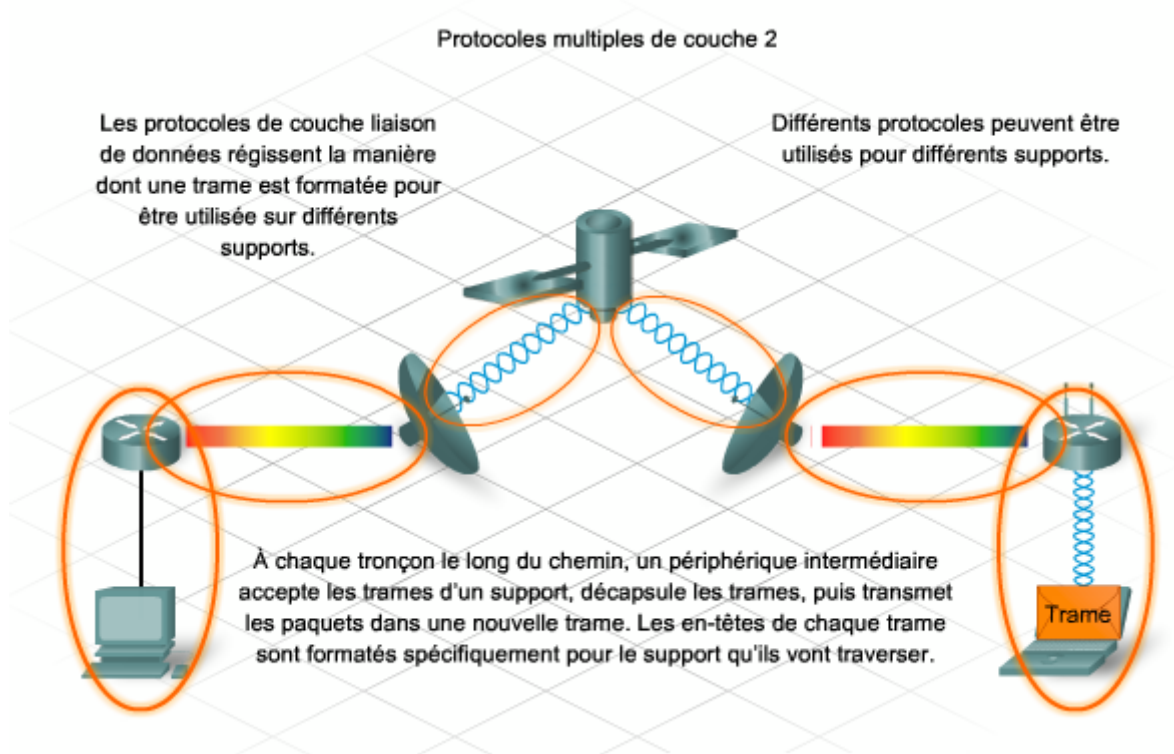
Cliquez sur l'icône des travaux pratiques pour télécharger la section 9.2 du Guide du participant CCENT.

## 3 Dépannage de problèmes d'adressage IP de couche 3

### 3.1 Examen des fonctionnalités de la couche 3 et de l'adressage IP

Les réseaux de couche 1 sont créés en interconnectant les périphériques à l'aide d'un support physique. Les protocoles réseau de couche 2 sont basés sur le matériel. Ethernet ne peut pas

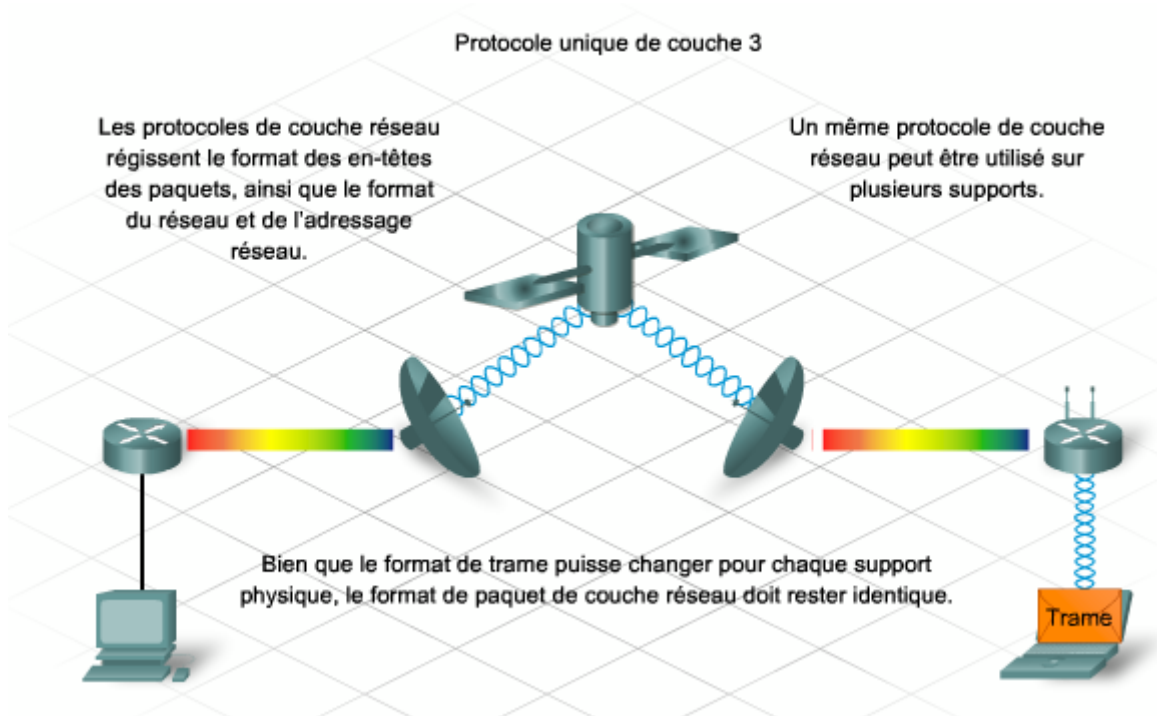
fonctionner sur une liaison série, et les communications série sont impossibles à l'aide d'une carte réseau Ethernet.



Les protocoles de couche 3 (couche réseau) ne sont pas attachés à un type de support spécifique, ni à un protocole de trame de couche 2. Les mêmes protocoles de couche 3 peuvent fonctionner sur Ethernet, ou sur des réseaux sans fil, des réseaux série ou d'autres réseaux de couche 2. Les réseaux de couche 3 peuvent contenir des hôtes connectés à l'aide de plusieurs technologies de couche 1 et 2. Les principales fonctions mises en œuvre sur la couche 3 du modèle OSI sont l'adressage réseau et le routage. Les réseaux de couche 3 sont appelés réseaux logiques car ils sont créés uniquement à l'aide de logiciels.

À l'heure actuelle, la plupart des réseaux implémentent les protocoles TCP/IP pour échanger des informations entre les hôtes. Par conséquent, le dépannage des problèmes de couche 3 se concentre sur des erreurs d'adressage IP et sur le fonctionnement du protocole de routage.

La résolution des problèmes de couche 3 requiert une connaissance approfondie des périphériques réseau et de l'adressage IP. Des schémas d'adressage IP mal conçus ou incorrectement configurés sont à l'origine d'un grand nombre de problèmes de performances réseau.



Au niveau de la couche 3, chaque paquet doit être identifié par les adresses source et de destination des systèmes des deux côtés. Avec l'adressage IPv4, cela implique que chaque paquet comporte, dans l'en-tête de la couche 3, une adresse source 32 bits et une adresse de destination 32 bits.

L'adresse IP identifie non seulement l'hôte individuel, mais également le réseau local de couche 3 sur lequel l'hôte peut communiquer. Un réseau IP simple peut être créé en configurant deux hôtes interconnectés avec des adresses uniques partageant le même préfixe réseau et le même masque de sous-réseau.

Un périphérique doit être configuré avec une adresse IP pour pouvoir échanger des messages via TCP/IP. Les réseaux IP individuels de couche 3 comportent une plage d'adresses IP. Ces limites sont définies par le nombre de bits contenus dans la partie préfixe réseau de l'adresse. Retenez cette règle simple : plus le préfixe réseau est long, plus la plage d'adresses IP pouvant être configurée sur les hôtes d'un réseau IP sera petite.

Pour dépanner des problèmes de couche 3, un administrateur doit pouvoir déterminer la plage d'adresses hôtes appartenant à chaque réseau IP individuel. La plage d'adresses est déterminée par le nombre et la position des bits d'hôtes. Par exemple, dans un réseau 192.168.1.0/24, vous consacrez trois bits à la création de sous-réseaux. Cela laisse 5 bits pour les adresses d'hôtes. Cette configuration permet de créer 8 sous-réseaux ( $2^3=8$ ) et 30 hôtes par sous-réseau ( $2^5 - 2 = 30$ ).

Dans le sous-réseau 192.168.1.96/27, le premier hôte du sous-réseau sera 192.168.1.97, et le dernier sera 192.168.1.126. L'adresse de diffusion de ce sous-réseau sera 192.168.1.127. Vous pouvez le constater en consultant le nombre binaire du dernier octet :

(sous-réseau 011) 96 + (premier hôte 00001) 1 = (01100001) 97 en décimal

(sous-réseau 011) 96 + (dernier hôte 11110) 30 = (01111110) 126

(sous-réseau 011) 96 + (diffusion 11111) 31 = (01111111) 127

Cet exemple utilise une adresse de classe C. La même technique peut être appliquée aux adresses de classe A et B. Notez que l'emplacement des bits d'hôtes peut s'étendre à plus d'un octet.

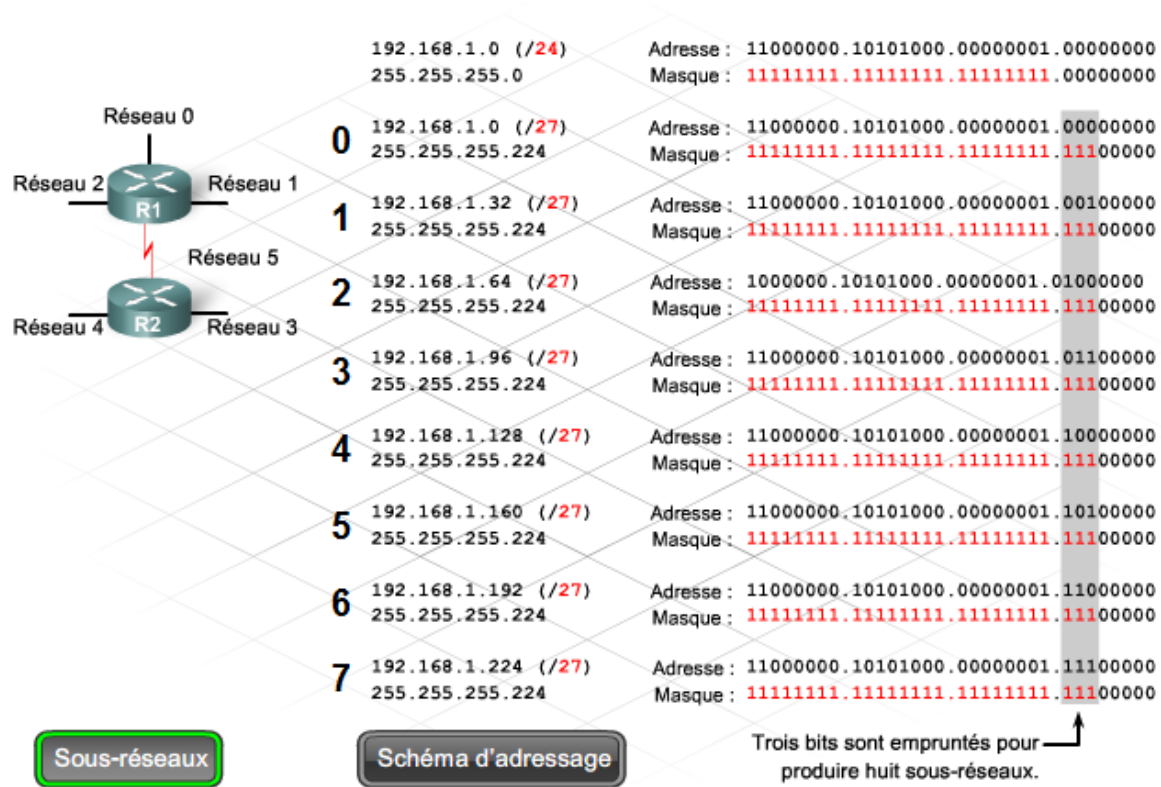


Schéma d'adressage : exemple de 8 réseaux

| Sous-réseau | Adresse réseau   | Plage d'hôtes                 | Adresse de diffusion |
|-------------|------------------|-------------------------------|----------------------|
| 0           | 192.168.1.0/27   | 192.168.1.1 - 192.168.1.30    | 192.168.1.31         |
| 1           | 192.168.1.32/27  | 192.168.1.33 - 192.168.1.62   | 192.168.1.63         |
| 2           | 192.168.1.64/27  | 192.168.1.65 - 192.168.1.94   | 192.168.1.95         |
| 3           | 192.168.1.96/27  | 192.168.1.97 - 192.168.1.126  | 192.168.1.127        |
| 4           | 192.168.1.128/27 | 192.168.1.129 - 192.168.1.158 | 192.168.1.159        |
| 5           | 192.168.1.160/27 | 192.168.1.161 - 192.168.1.190 | 192.168.1.191        |
| 6           | 192.168.1.192/27 | 192.168.1.193 - 192.168.1.222 | 192.168.1.223        |
| 7           | 192.168.1.224/27 | 192.168.1.225 - 192.168.1.254 | 192.168.1.255        |

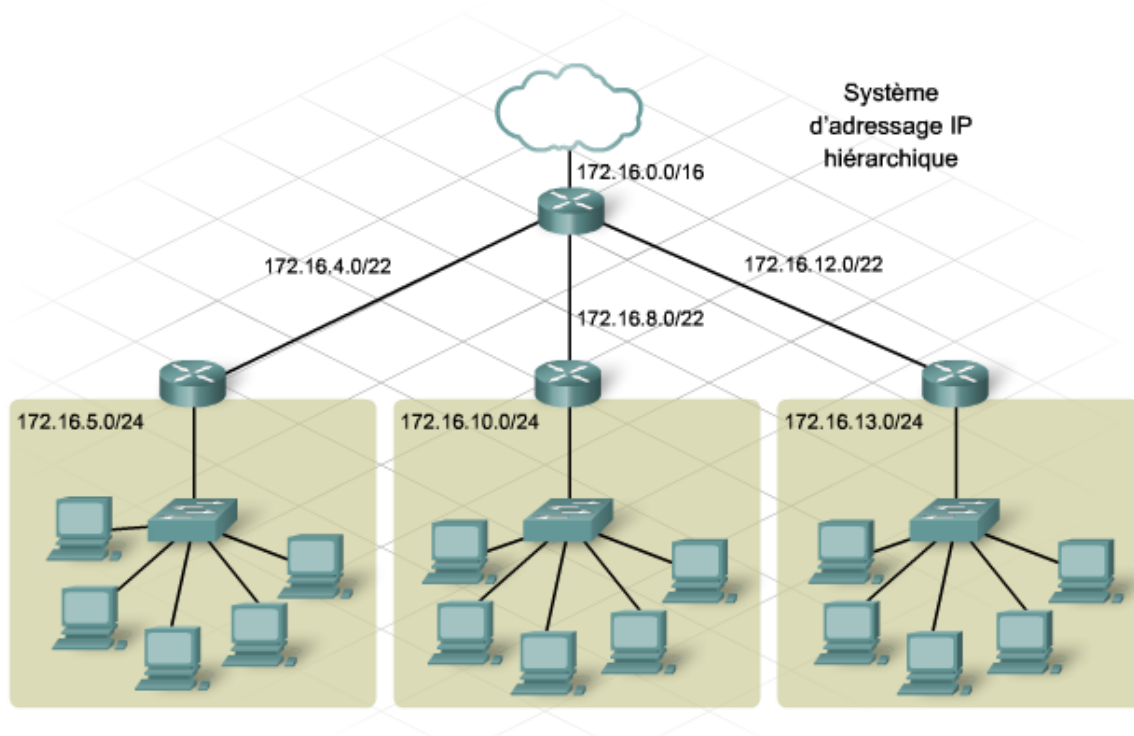
## Exercice Packet Tracer : Dépannage d'un petit réseau

### 3.2 Problèmes de conception IP et de configuration

Si l'adressage IP est attribué de façon aléatoire, il est difficile de déterminer l'emplacement d'une adresse source ou de destination. À l'heure actuelle, la plupart des réseaux emploient un schéma d'adressage IP hiérarchique. Les schémas d'adressage IP hiérarchiques présentent des avantages multiples, notamment des tables de routage plus petites, peu gourmandes en puissance de traitement. L'adressage IP hiérarchique permet également de créer un environnement plus structuré, facile à documenter, à dépanner et à étendre.

Toutefois, un réseau hiérarchique incorrectement planifié, ou un plan mal documenté peut créer des problèmes tels que le chevauchement de sous-réseaux ou la configuration incorrecte des masques de sous-réseaux sur des périphériques. Ces deux situations sont à l'origine d'un grand nombre de problèmes d'adressage IP et de routage.

Un chevauchement de sous-réseaux survient lorsque la plage d'adresses de deux sous-réseaux distincts comporte certaines adresses d'hôtes ou certaines adresses de diffusion identiques. Le chevauchement résulte généralement d'un réseau mal documenté, ou lors de la saisie accidentelle d'un masque de sous-réseau ou d'un préfixe réseau incorrect. Le chevauchement de sous-réseaux ne provoque pas toujours la panne générale du réseau. Il arrive que certains hôtes seulement soient affectés, en fonction de l'emplacement du masque de sous-réseau incorrectement configuré.



Le logiciel Cisco IOS vous permet de configurer une adresse IP à partir du chevauchement des sous-réseaux sur deux interfaces différentes. Cependant, le routeur n'active pas la seconde interface.

Par exemple, l'interface Fast Ethernet 0/0 du routeur R1 est configurée avec une adresse IP et un masque de sous-réseau sur le réseau 192.168.1.0/24. Si Fast Ethernet 0/1 est configuré



avec une adresse IP sur le réseau 192.168.1.0/30, un message d'erreur de chevauchement apparaît. En cas de tentative d'activation de l'interface via la commande **no shutdown**, un second message d'erreur apparaît. Aucun trafic n'est transféré via l'interface. Le résultat de la commande **show ip interface brief** signale que la seconde interface configurée pour le réseau 192.168.1.0/24, FastEthernet 0/1, est désactivée (down).

Il est important de vérifier l'état des interfaces après tout changement de configuration. Une interface qui reste désactivée par l'administrateur après l'exécution de la commande **no shutdown** peut indiquer un problème d'adressage IP.

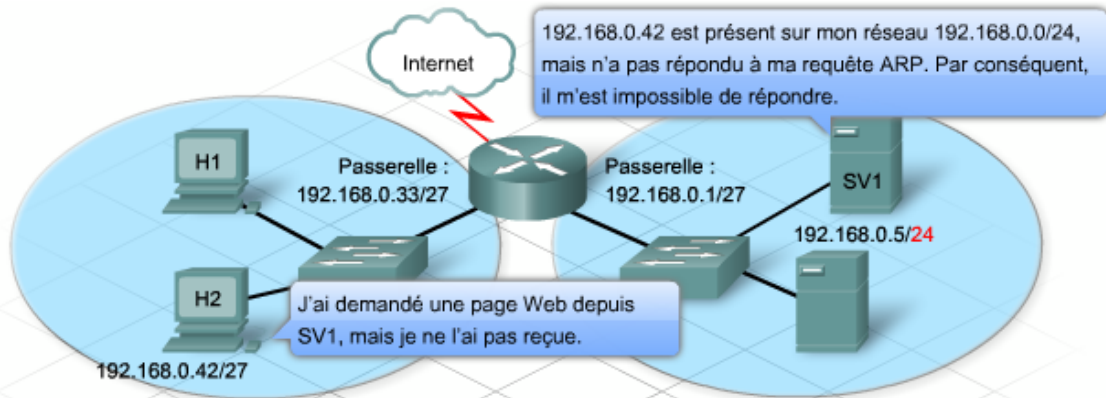
```
R1(config)#interface FastEthernet0/1
R1(config-if)#ip address 192.168.1.2 255.255.255.252
192.168.1.0 overlaps with FastEthernet0/0

R1(config-if)#no shutdown
192.168.1.0 overlaps with FastEthernet0/0
FastEthernet0/1: incorrect IP address assignment
```

```
R1#show ip interface brief
<résultat omis>
FastEthernet0/1 192.168.1.2 YES manual administratively down down
```

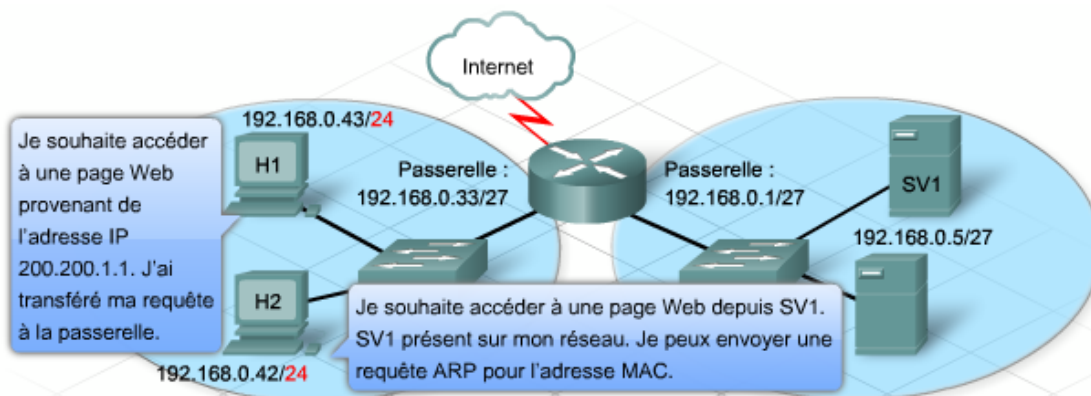
Bien que le logiciel Cisco IOS soit pourvu de protections destinées à éviter que des sous-réseaux en chevauchement ne soient configurés sur plusieurs interfaces du même périphérique, il ne peut éviter un chevauchement de sous-réseaux configurés sur plusieurs périphériques ou plusieurs hôtes au sein d'un même réseau.

Un masque de sous-réseau incorrectement configuré peut empêcher certains hôtes d'accéder aux services réseau. Des erreurs de configuration détectées au niveau des masques de sous-réseaux peuvent également présenter des symptômes difficiles à identifier.



Un serveur n'est accessible que par les hôtes du même sous-réseau.

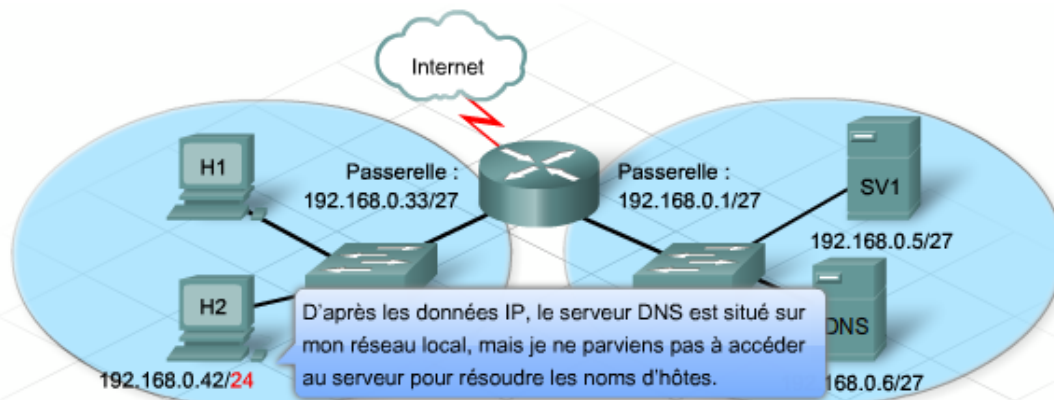
Un serveur de l'un des sous-réseaux est manuellement configuré à l'aide du préfixe réseau par défaut /24 et non /27. En raison de cette configuration incorrecte, le serveur a déterminé que tous les hôtes des différents sous-réseaux sont situés sur le même réseau de couche 3 que le serveur. Le serveur n'envoie aucun trafic à la passerelle par défaut pour les hôtes des sous-réseaux /27. Si ce problème survient, vérifiez les configurations du serveur.



Les hôtes obtiennent des réponses des serveurs Internet, mais pas des serveurs des autres sous-réseaux.

Un hôte ou un groupe d'hôtes est configuré avec un masque de sous-réseau /24 qui provoque un chevauchement avec les adresses de sous-réseau du serveur. Chaque hôte détermine correctement que les adresses Internet ne sont pas situées sur le réseau local de couche 3 et transmet le trafic à la passerelle par défaut. Les hôtes déterminent à tort que les adresses de serveurs internes sont situées sur leur réseau local, et utilisent des requêtes ARP pour tenter d'accéder aux adresses MAC du serveur. Lorsque ce symptôme est évident, vérifiez les configurations DHCP du serveur et les configurations de l'hôte. Un analyseur de réseau peut être utilisé pour afficher les trames ARP.

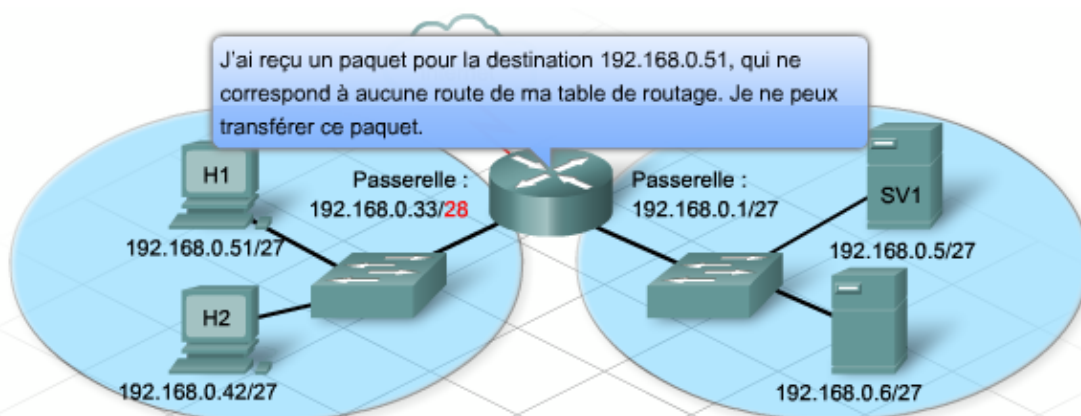




À l'aide des noms d'hôtes, les hôtes ne peuvent obtenir de réponses des serveurs Internet, ni des serveurs des autres sous-réseaux.

Un hôte ou un groupe d'hôtes est configuré avec un masque de sous-réseau /24 qui provoque un chevauchement avec les adresses de sous-réseau du serveur, notamment le serveur DNS. En règle générale, les erreurs de masques de sous-réseaux détectées sur les hôtes n'affectent pas la connectivité Internet. Toutefois, si l'erreur de masque de sous-réseau provoque le chevauchement du sous-réseau contenant le serveur DNS, le ou les hôtes ne pourront pas contacter le serveur DNS. Sans DNS, aucune adresse IP ne peut être résolue, et tous les services

DNS seront inaccessibles. Si vous ne pouvez accéder à Internet, vérifiez les configurations des hôtes et les configurations DNS.



Certains hôtes obtiennent des réponses des serveurs Internet et des serveurs des autres sous-réseaux, alors que certains autres hôtes n'y parviennent pas.

L'erreur de configuration de masque de sous-réseau est survenue sur une interface de routeur utilisée comme passerelle par défaut pour l'un des sous-réseaux /27. Si l'interface du routeur est configurée par erreur avec un masque de sous-réseau /28, la route indiquée dans la table de routage n'inclut pas tous les hôtes du sous-réseau /27. Les hôtes dont les adresses de la partie inférieure de la plage d'adresses sont dans les limites des adresses IP de sous-réseau /28 peuvent envoyer et recevoir des paquets via le routeur. Ceux dont les adresses sont situées

dans la partie supérieure de la plage d'adresses peuvent envoyer des paquets aux destinations distantes, mais lorsque les réponses arriveront, le routeur ne disposera pas de la route adéquate vers les adresses IP de destination. Vérifiez toujours toutes les routes connectées dans la table de routage, en utilisant la commande show IP route.

### **3.3 Problèmes de planification des adresses IP et erreurs d'attribution**

La planification incorrecte d'attribution d'adresses peut engendrer d'autres problèmes. Lors de la conception des sous-réseaux, les administrateurs sous-estiment parfois le potentiel d'extension d'un réseau. Par conséquent, le schéma de sous-réseaux IP n'autorise pas suffisamment d'adresses hôtes dans chaque sous-réseau. L'incapacité de certains hôtes à recevoir une adresse IP du serveur DHCP indique parfois qu'un sous-réseau possède un trop grand nombre d'hôtes.

Lorsqu'un hôte équipé de Microsoft Windows ne reçoit pas une adresse d'un serveur DHCP, il s'affecte automatiquement une adresse sur le réseau 169.254.0.0. Dans ce cas, exécutez la commande **show ip dhcp binding** pour vérifier si le serveur DHCP possède des adresses disponibles.

Une autre indication d'un manque d'adresses IP est un message d'erreur affiché sur l'hôte, indiquant la présence d'adresses IP dupliquées. Si un périphérique hôte est désactivé à l'expiration du bail DHCP, l'adresse est renvoyée au pool DHCP et peut être attribuée à un autre hôte. Si le détenteur du bail initial souhaite réactiver son compte, il peut demander le rétablissement de sa précédente adresse IP. Dans un réseau Microsoft Windows, les deux hôtes reçoivent une erreur d'adresse IP dupliquée.

```
R1#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/
                   Hardware address/
                   User name
192.168.10.10       0100.e018.5bdd.35   Oct 03 2007 06:14 PM   Automatic
192.168.10.11       0100.b0d0.d817.e6   Oct 03 2007 06:18 PM   Automatic
```

**Travaux pratiques :** Création d'un schéma d'adressage IP permettant une extension de 20 % du nombre d'hôtes attachés

### **3.4 Problèmes DHCP et NAT**

DHCP ajoute un degré de complexité au dépannage des problèmes réseau. Si des hôtes configurés pour l'utilisation de DHCP ne parviennent pas à se connecter au réseau, vérifiez l'attribution de l'adressage IP en exécutant la commande **ipconfig /all**. Si les hôtes ne reçoivent pas les attributions d'adressage IP, il est nécessaire de dépanner la configuration DHCP.

Que le service DHCP soit configuré sur un serveur dédié ou sur le routeur, la première étape du dépannage consiste à vérifier la connectivité physique. En cas d'utilisation d'un serveur

distinct, vérifiez si le serveur reçoit correctement le trafic réseau. Si le service DHCP est configuré sur un routeur, exécutez la commande **show interfaces** sur le routeur pour confirmer que l'interface est opérationnelle. Si l'état de l'interface connectée au réseau hôte est down (désactivée), le port n'achemine pas le trafic, y compris les requêtes DHCP.

Vérifiez ensuite si le serveur DHCP est correctement configuré et dispose d'adresses IP disponibles. Enfin, vérifiez la présence éventuelle de conflits d'adresses. Les conflits d'adresses peuvent survenir malgré la présence d'adresses disponibles dans le pool DHCP. C'est le cas, par exemple, si un hôte est configuré en mode statique avec une adresse qui est également présente dans la plage du pool DHCP.

La commande **show ip dhcp conflict** affiche tous les conflits d'adresses enregistrés par le serveur DHCP. Si un conflit d'adresse est détecté, l'adresse est retirée du pool et n'est pas attribuée tant qu'un administrateur n'a pas résolu le conflit.

Si aucune de ces étapes ne permet de diagnostiquer le problème, vérifiez que l'erreur provient bien de DHCP. Configurez un hôte avec une adresse IP statique, un masque de sous-réseau et une passerelle par défaut. Si la station de travail ne peut pas atteindre les ressources réseau avec une adresse IP configurée de façon statique, la cause première du problème n'est pas le protocole DHCP. Le dépannage de la connectivité du réseau est alors nécessaire.

```

C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Bob>ipconfig /all

Configuration IP de Windows

    Nom de l'hôte. . . . . : ciscolab
    Suffixe DNS principal. . . . . :
    Type de noeud. . . . . : Inconnu
    Routage IP activé. . . . . : Non
    Proxy WINS activé. . . . . : Non

Carte Ethernet Connexion au réseau local :

    Suffixe DNS propre à la connexion. . : span.com
    Description. . . . . : Carte Fast Ethernet PCI SiS 900
    Adresse physique. . . . . : 00-E0-18-5B-DD-35
    DHCP activé. . . . . : Oui
    Configuration automatique activée. : Oui
    Adresse IP . . . . . : 192.168.10.10
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 192.168.10.1
    Serveur DHCP. . . . . : 192.168.10.1
    Bail obtenu. . . . . : mardi 2 octobre 2007 13:06:22

    Bail expirant. . . . . : Mercredi 3 octobre 2007 13:06:22

C:\Documents and Settings\Bob>
    
```

DHCP est un protocole de diffusion, ce qui signifie que le serveur DHCP doit être accessible via un message de diffusion. Étant donné que les routeurs ne transmettent généralement pas

de messages de diffusion, il faut que le serveur DHCP soit situé sur le même réseau local que les hôtes, ou que le routeur soit configuré pour le relais des messages de diffusion.

Un routeur peut être configuré pour transmettre tous les paquets de diffusion, notamment les requêtes DHCP, à un serveur spécifique, à l'aide de la commande **ip helper-address**. La commande suivante permet à un routeur de remplacer les adresses de diffusion de destination d'un paquet vers une adresse de [monodiffusion](#) spécifiée :

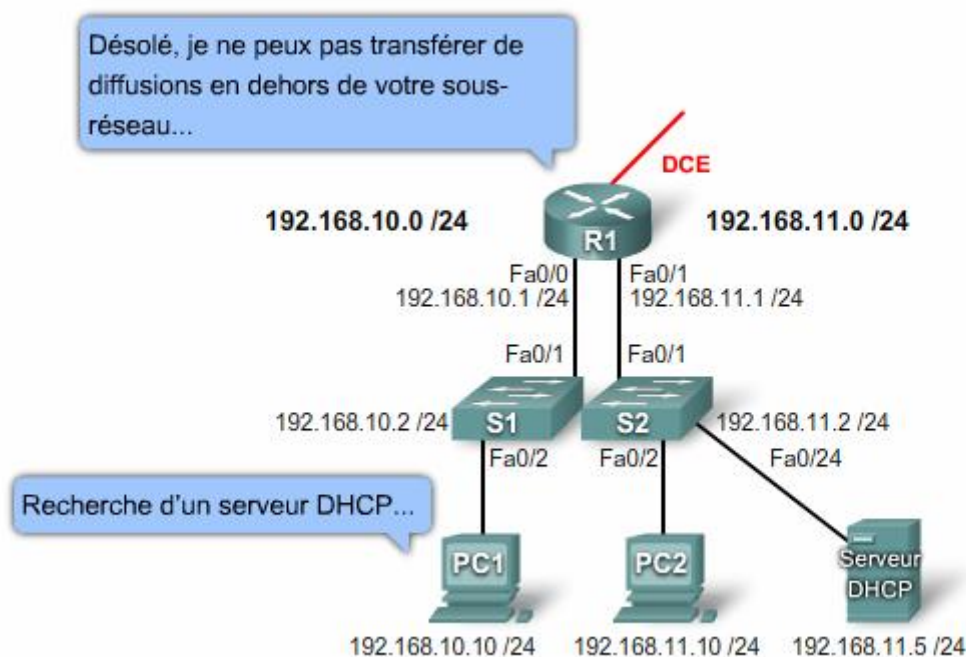
**monodiffusion**

Type de message envoyé à une destination réseau unique. Comparer monodiffusion à diffusion et multidiffusion.

Router(config-if)# **ip helper-address x.x.x.x**

Une fois cette commande configurée, tous les paquets de diffusion seront transmis à l'adresse IP du serveur spécifiée dans la commande, y compris les requêtes DHCP.

Lorsqu'un routeur transfère des requêtes d'adresse, il agit comme agent de relais DHCP. Si le relais DHCP n'est pas opérationnel, aucun hôte ne peut obtenir d'adresse IP. Lorsqu'aucun hôte ne peut obtenir d'adresse IP d'un serveur DHCP situé sur un autre réseau, il est conseillé de vérifier si la commande helper-address est correctement configurée sur le routeur.



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrateur>ipconfig /release

Configuration IP de Windows

Carte Ethernet Connexion au réseau local :

    Suffixe DNS propre à la connexion. :
    Adresse IP . . . . . : 0.0.0.0
    Masque de sous-réseau. . . . . : 0.0.0.0
    Passerelle par défaut. . . . . :

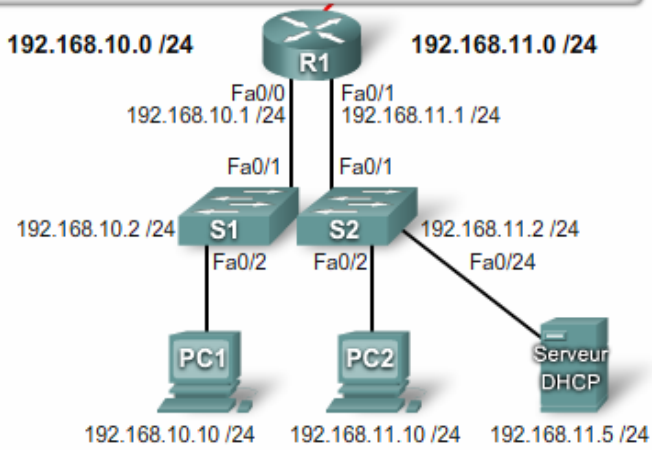
C:\Documents and Settings\Administrateur>ipconfig /renew

Configuration IP de Windows

Une erreur s'est produite lors du renouvellement de l'interface Connexion au
réseau local : impossible de contacter votre serveur DHCP. Le délai d'attente
de la demande est dépassé.
```

- Problème de DHCP
- Problème d'hôte**
- Config. relais
- Renouv. hôte

```
R1# config t
R1(config)# interface Fa0/0
R1(config-if)# ip helper-address 192.168.11.5
R1(config-if)# end
```



- Problème de DHCP
- Problème d'hôte
- Config. relais**
- Renouv. hôte

```

C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrateur>ipconfig /release

Configuration IP de Windows

Carte Ethernet Connexion au réseau local :

    Suffixe DNS propre à la connexion. :
    Adresse IP . . . . . : 0.0.0.0
    Masque de sous-réseau. . . . . : 0.0.0.0
    Passerelle par défaut. . . . . :

C:\Documents and Settings\Administrateur>ipconfig /renew

Configuration IP de Windows

Carte Ethernet Connexion au réseau local :

    Suffixe DNS propre à la connexion. :
    Adresse IP . . . . . : 192.168.10.11
    Masque de sous-réseau. . . . . : 255.255.255.0
    
```



Si des adresses privées sont attribuées au hôtes du réseau interne, la fonction NAT est requise pour communiquer avec le réseau public. Un accès impossible aux sites Internet est généralement la première indication d'un problème lié à la fonction NAT. Il existe trois types de traduction d'adresses : statique, dynamique et PAT. Deux types d'erreurs de configuration courantes affectent ces trois méthodes de traduction.

**Désignation incorrecte des interfaces interne et externe**

Pour la fonction NAT, il est essentiel que les interfaces correctes soient désignées en tant qu'interface interne ou externe. Dans la plupart des implémentations NAT, l'interface interne se connecte au réseau local, qui utilise un espace d'adresses IP privé. L'interface externe se connecte au réseau public, généralement le FAI. Vérifiez cette configuration en exécutant la commande **show running-config interface**.

**Attribution incorrecte de l'adresse IP de l'interface ou des adresses du pool**

Dans la plupart des implémentations NAT, le pool d'adresses IP et les entrées de la traduction NAT statique doivent utiliser des adresses IP situées sur le même réseau local que l'interface externe. Dans le cas contraire, les adresses sont traduites, mais les routes des adresses traduites restent introuvables. Examinez la configuration pour vérifier si toutes les adresses traduites sont accessibles. Lorsque la traduction d'adresse est configurée pour utiliser l'adresse de l'interface externe dans PAT, assurez-vous que l'adresse d'interface est située sur le réseau approprié et est configurée avec le masque de sous-réseau correct.

Il arrive également que des utilisateurs externes ne puissent se connecter aux périphériques internes lorsque la fonction NAT ou PAT est activée. Si des utilisateurs externes peuvent accéder aux serveurs du réseau interne, vérifiez la configuration des traductions statiques.

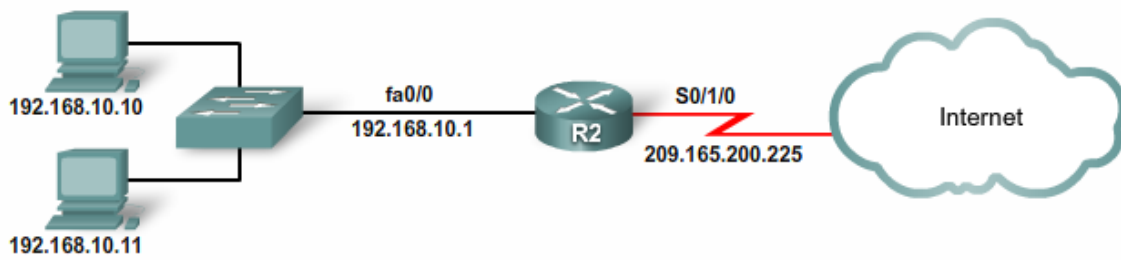


```
access-list 1 permit 192.168.0.0 0.0.255.255
!- Définit les adresses qui peuvent être traduites.
ip nat pool NAT-POOL2 209.165.200.226 209.165.200.240
!- Définit un pool d'adresses nommé NAT-POOL2 à utiliser dans la traduction NAT.
ip nat inside source list 1 pool NAT-POOL2 overload
!- Associe le pool de traduction d'adresses de réseau à la liste de contrôle d'accès 1.
interface serial 0/0/0
ip nat inside
!- Identifie l'interface Serial 0/0/0 en tant qu'interface NAT interne.
interface serial 0/1/0
ip nat outside
!- Identifie l'interface Serial 0/1/0 en tant qu'interface NAT externe.
```

Si vous êtes certain que la fonction NAT est correctement configurée, il est important de vérifier si elle est opérationnelle.

L'une des commandes les plus efficaces pour vérifier le fonctionnement de NAT est la commande **show ip nat translations**. Après avoir examiné les traductions existantes, effacez-les en utilisant la commande **clear ip nat translation \***. Soyez prudent, car la suppression de toutes les traductions IP d'un routeur peut perturber les services utilisateur. Ensuite, exécutez à nouveau la commande **show ip nat translations**. Si de nouvelles traductions apparaissent, la perte de connectivité Internet peut provenir d'une autre erreur.

Vérifiez s'il existe une route vers Internet pour les adresses traduites. Exécutez la commande **traceroute** pour déterminer le chemin emprunté par paquets traduits et vérifiez si cette route est correcte. Si possible, tracez ensuite la route vers une adresse traduite, depuis un périphérique distant sur le réseau externe. Cette action peut permettre d'isoler la cible du dépannage suivant. Il se peut qu'un problème de routage soit présent sur le routeur à l'emplacement où les résultats de la commande trace s'arrêtent.



```

access-list 1 permit 192.168.10.0 0.0.0.255
ip nat inside source list 1 interface serial 0/1/0 overload
interface fastethernet0/0
 ip nat inside
interface serial 0/1/0
 ip nat outside
    
```

Surcharge NAT

Traductions NAT

NAT effacées

```

R2#show ip nat translations
Pro Inside global      Inside local          Outside local         Outside global
tcp 209.165.200.225:16642 192.168.10.10:16642 209.165.200.254:80 209.165.200.254:80
tcp 209.165.200.225:62452 192.168.10.11:62452 209.165.200.254:80 209.165.200.254:80

R2#show ip nat translations verbose
Pro Inside global      Inside local          Outside local         Outside global
tcp 209.165.200.225:16642 192.168.10.10:16642 209.165.200.254:80 209.165.200.254:80
  create 00:01:45, use 00:01:43 timeout:86400000, left 23:58:16, Map-Id(In): 1,
  flags:
  extended, use_count: 0, entry-id: 4, lc_entries: 0
tcp 209.165.200.225:62452 192.168.10.11:62452 209.165.200.254:80 209.165.200.254:80
  create 00:00:37, use 00:00:35 timeout:86400000, left 23:59:24, Map-Id(In): 1,
  flags:
  extended, use_count: 0, entry-id: 5, lc_entries: 0
R2#
    
```

Surcharge NAT

Traductions NAT

NAT effacées



```
R2#clear ip nat translation *
R2#show ip nat translations
R2#
```

Surcharge NAT

Traductions NAT

NAT effacées

**Exercice Packet Tracer** : Les commandes **show** permettent de dépanner des erreurs DHCP et NAT.

### 3.5 Guide de certification du participant

**Guide du participant CCENT.** Cliquez sur l'icône des travaux pratiques pour télécharger la section 9.3 du Guide du participant CCENT.

## 4 Dépannage de problèmes de routage de couche 3

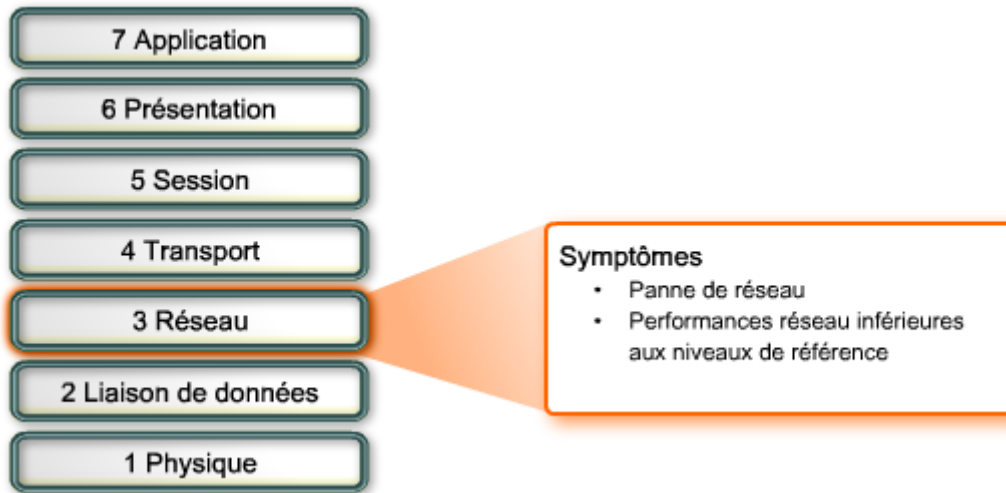
### 4.1 Problèmes de routage de couche 3

La couche 3 englobe l'adressage des réseaux et des hôtes, ainsi que les protocoles acheminant les paquets entre les réseaux.

La plupart des réseaux possèdent une combinaison de plusieurs types de routes : statiques, dynamiques et par défaut. Les problèmes de routage peuvent provoquer des pannes réseau ou affecter les performances. Ces problèmes peuvent provenir d'erreurs de saisie manuelle de routes, d'erreurs de configuration et de fonctionnement du protocole de routage, ou encore de défaillances des couches inférieures du modèle OSI.

Pour dépanner des problèmes de couche 3, il est important de comprendre le fonctionnement du routage, notamment les opérations et la configuration de chaque type de route.

Avant de poursuivre ce chapitre, il peut être intéressant de réviser les cours et les exercices de CCNA Discovery : Réseaux domestiques et pour petites entreprises et CCNA Discovery : Travailler dans une PME ou chez un fournisseur de services Internet concernant le routage et les protocoles de routage.



L'état d'un réseau peut être modifié fréquemment, pour plusieurs raisons :

- Une interface est désactivée.
- Un fournisseur de services perd une connexion.
- La bande passante disponible est surchargée.
- Un administrateur a effectué une configuration incorrecte.

En cas de changement de l'état du réseau, il se peut que certaines routes soient perdues, ou qu'une route incorrecte soit installée dans la table de routage.

L'outil principal de dépannage des problèmes de routage de couche 3 est la commande **show ip route**. Cette commande permet d'afficher toutes les routes utilisées par le routeur pour la transmission du trafic. La table de routage est constituée d'entrées de routes provenant des sources suivantes :

- Réseaux connectés directement
- Routes statiques
- Protocoles de routage dynamiques

Les protocoles de routage choisissent les routes en fonction de la mesure de la route. Les réseaux directement connectés ont une mesure de 0, les routes statiques ont également une mesure par défaut de 0 et les routes dynamiques ont plusieurs mesures de route, selon le protocole de routage utilisé.

Si plusieurs routes sont définies vers un réseau de destination spécifique, c'est la route possédant la distance administrative (DA) la plus faible qui sera installée dans la table de routage.

Si vous suspectez un problème de routage, exécutez la commande **show ip route** pour vous assurer que toutes les routes nécessaires sont installées dans la table de routage.

| Origine de la route     | Distance administrative | Mesure(s) par défaut                               |
|-------------------------|-------------------------|----------------------------------------------------|
| Connecté                | 0                       | 0                                                  |
| Statique                | 1                       | 0                                                  |
| Résumé du routage EIGRP | 5                       |                                                    |
| BGP externe             | 20                      | Valeur attribuée par l'administrateur              |
| EIGRP interne           | 90                      | Bande passante, délai                              |
| IGRP                    | 100                     | Bande passante, délai                              |
| OSPF                    | 110                     | Coût de la liaison (bande passante)                |
| IS-IS                   | 115                     | Coût ligne (valeur attribuée par l'administrateur) |
| RIP                     | 120                     | Nombre de sauts                                    |
| EIGRP externe           | 170                     |                                                    |
| BGP interne             | 200                     | Valeur attribuée par l'administrateur              |

### Problèmes de route connectée

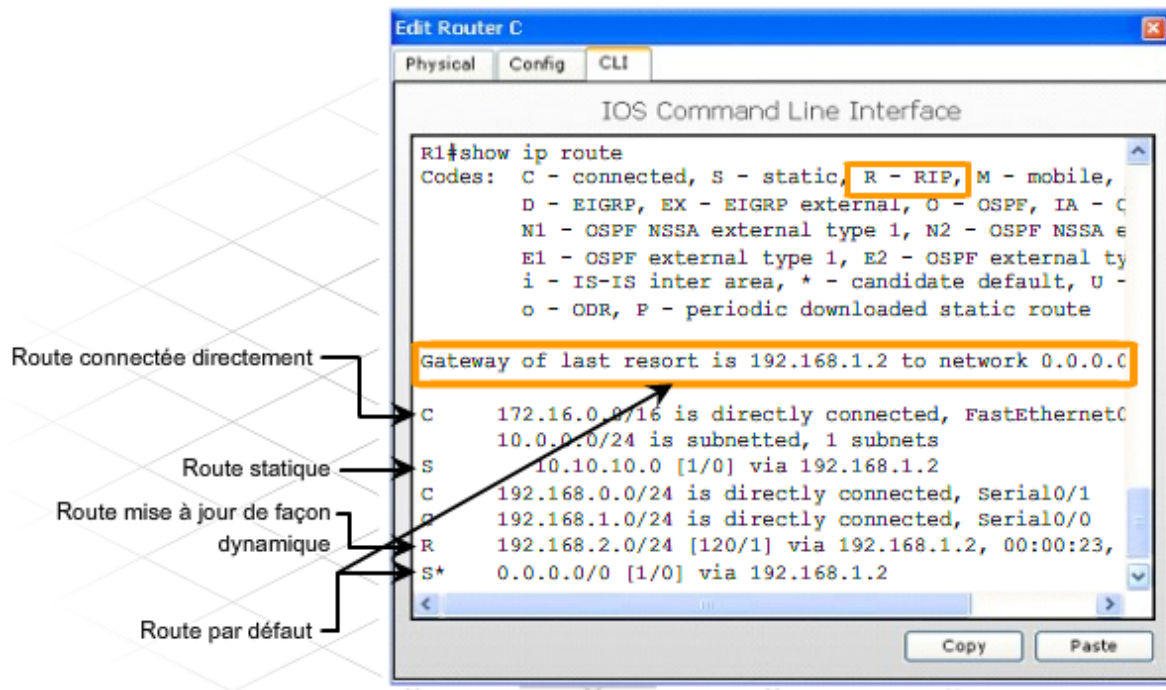
Les routes connectées directement sont automatiquement installées dans la table de routage lorsqu'une adresse IP est configurée sur une interface, et que l'interface est activée via la commande **no shutdown**. Si une route connectée directement ne s'affiche pas dans la table, utilisez la commande **show interfaces** ou la commande **show ip interface brief** pour vérifier l'attribution de l'adresse et l'état de l'interface (up/up).

### Problèmes de routes statiques et par défaut

Si une route statique ou par défaut n'apparaît pas dans la table de routage, il s'agit probablement d'une erreur de configuration. Les routes statiques et par défaut doivent utiliser une interface de sortie ou l'adresse IP d'un routeur de tronçon suivant. Des erreurs de route statique peuvent survenir lorsque l'adresse de tronçon suivant n'est pas située dans la plage d'adresses IP correcte du réseau connecté directement. Vérifiez si les instructions de configuration sont correctes et vérifiez si l'état des interfaces de sortie utilisées par les routes est bien up/up.

### Problèmes de route dynamique

Un grand nombre de types de problèmes peuvent être à l'origine de l'absence de routes dynamiques dans la table de routage. Étant donné qu'un grand nombre de protocoles de routage dynamiques échangent des tables de routage avec les autres routeurs d'un réseau, une route manquante peut provenir d'une erreur de configuration sur l'un ou l'autre des routeurs situé sur le chemin d'accès à la destination.



## Exercice Packet Tracer : Utiliser les principes de la table de routage pour dépanner un problème de routage

### 4.2 Erreurs de routage dynamique

Des mises à jour de la table de routage sont généralement effectuées lors de la configuration d'un nouveau réseau, ou lorsqu'un réseau précédemment configuré est devenu inaccessible.

Si les routes connectées directement apparaissent dans la table du routeur, la table de routage est accessible et ne sera modifiée qu'en cas de changement d'état de l'interface connectée directement. Si des routes statiques ou par défaut sont configurées, la table de routage ne changera que si de nouvelles routes sont spécifiées ou en cas de changement d'état de l'interface de sortie définie dans la route statique ou par défaut.

Les protocoles de routage dynamique envoient automatiquement des mises à jour de routage aux autres routeurs du réseau. Si le routage dynamique est activé, un routeur accède et modifie sa propre table de routage à chaque modification consignée dans une mise à jour d'un routeur voisin.

RIP est un protocole de routage dynamique utilisé dans les réseaux locaux de petite taille ou de taille moyenne. Lors de dépannage de problèmes RIP, vérifiez le numéro de version et les instructions de configuration.

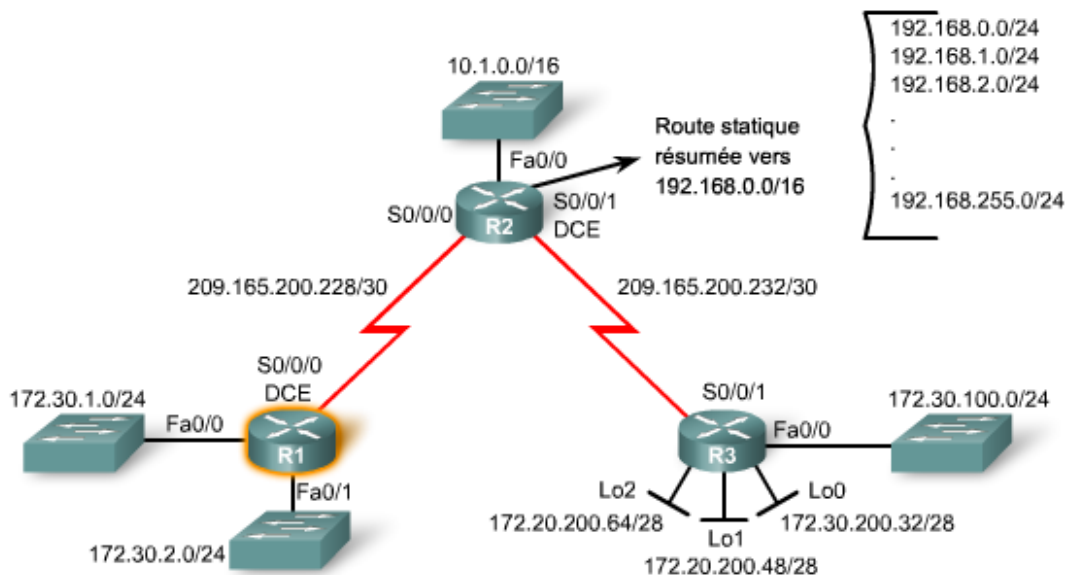
Il est toujours préférable d'utiliser la même version de protocole de routage sur tous les routeurs. Malgré la compatibilité de RIPv1 et de RIPv2, RIPv1 ne prend pas en charge le routage sans classe, ni les masques de sous-réseaux de longueur variable (VLSM). Ces situations peuvent causer des problèmes si RIPv1 et RIPv2 sont configurés pour une

exécution sur le même réseau. De plus, alors que RIPv2 accepte automatiquement des mises à jour pour RIPv1 et RIPv2 des voisins, RIPv1 n'accepte pas de mises à jour RIPv2.

Des problèmes de routage peuvent également survenir en cas d'instructions réseau incorrectes ou manquantes. N'oubliez pas que l'instruction réseau a deux objectifs :

- Elle active le protocole de routage pour envoyer et recevoir des mises à jour sur toutes les interfaces locales qui appartiennent à ce réseau.
- Elle inclut ce réseau dans ses mises à jour de routage vers les routeurs avoisinants.

Une instruction réseau manquante ou incorrecte peut entraîner des mises à jour de routage inappropriées et empêcher une interface d'envoyer ou de recevoir des mises à jour de routage.



De nombreux outils permettent de résoudre les problèmes de routage dynamique.

Utilisez les utilitaires TCP/IP tels que ping et traceroute, pour vérifier la connectivité. Telnet permet également de vérifier la connectivité et d'apporter les changements de configuration requis. Les commandes show de Cisco IOS permettent d'afficher un cliché instantané d'une configuration ou le statut d'un composant spécifique. Le jeu de commandes Cisco IOS comporte un grand nombre de commandes debug.

Les commandes debug sont dynamiques et fournissent des informations en temps réel sur le trafic et l'interaction des protocoles. Par exemple, la commande **debug ip rip** affiche immédiatement l'échange des mises à jour de routage RIP et des paquets.

Les fonctions debug utilisent une grande partie des ressources de l'UC, ce qui peut entraîner un ralentissement ou une interruption des opérations courantes du routeur. Utilisez donc les commandes debug pour isoler les problèmes et non pour surveiller le fonctionnement normal du réseau.

```
R1#show ip protocols
Routing Protocol is "rip"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Sending updates every 30 seconds, next due in 26 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Redistributing: rip
  Default version control: send version 2, receive version 2
    Interface          Send Recv Triggered RIP Key-chain
  Serial0/0/0         2     2
  Automatic network summarization is in effect
```

show ip protocols    show running-config    show interfaces

show ip interface    show ip route    debug ip rip

```
R1#show running-config
Building configuration...
<partie du résultat omise>
Current configuration : 1120 bytes
!
version 12.4
!
hostname R1
!
enable secret 5 $1$kbVM$rgp031Y42AhaHURL9BXTl0
```

show ip protocols    show running-config    show interfaces

```
R1#show interfaces
<partie du résultat omise>
FastEthernet0/0 is up, line protocol is up
  Hardware is Gt96k FE, address is 001b.5325.256e (bia 001b.5325.256e)
  Description: LAN gateway for 192.168.1.0
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
```

show ip protocols    show running-config    show interfaces

```
R1#show ip interface
<partie du résultat omise>
FastEthernet0/0 is up, line protocol is up
  Internet address is 192.168.1.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.9
```

show ip protocols    show running-config    show interfaces  
show ip interface    show ip route    debug ip rip



```
R1#show ip route
```

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP  
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
E1 - OSPF external type 1, E2 - OSPF external type 2  
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2  
ia - IS-IS inter area, \* - candidate default, U - per-user static route  
o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

- show ip protocols
- show running-config
- show interfaces
- show ip interface
- show ip route
- debug ip rip

```
R1#debug ip rip
```

RIP protocol debugging is on  
R1#  
\*Sep 12 21:08:51.959: RIP: build update entries  
\*Sep 12 21:08:51.959: 192.168.1.0/24 via 0.0.0.0, metric 1, tag 0  
\*Sep 12 21:09:16.399: RIP: received v2 update from 172.20.1.2 on Serial0/0/0  
\*Sep 12 21:09:16.399: 192.168.2.0/24 via 0.0.0.0 in 1 hops  
\*Sep 12 21:09:18.575: RIP: sending v2 update to 224.0.0.9 via Serial0/0/0 (172.20.1.1)

- show ip protocols
- show running-config
- show interfaces
- show ip interface
- show ip route
- debug ip rip

**Exercice Packet Tracer** : Découper un espace d'adressage en sous-réseau, configurer les périphériques et utiliser conjointement RIPv2 avec le routage statique pour activer une connectivité entre des hôtes distants

**Travaux pratiques** : Dépanner un réseau de routeurs RIP comportant des erreurs de configuration

#### **4.3 Guide de certification du participant**

#### **Guide du participant CCENT**

Cliquez sur l'icône des travaux pratiques pour télécharger la section 9.4 du Guide du participant CCENT.

## **5 Dépannage de problèmes de couches 4 et supérieures**

### **5.1 Erreurs de filtrage de trafic de la couche 4**

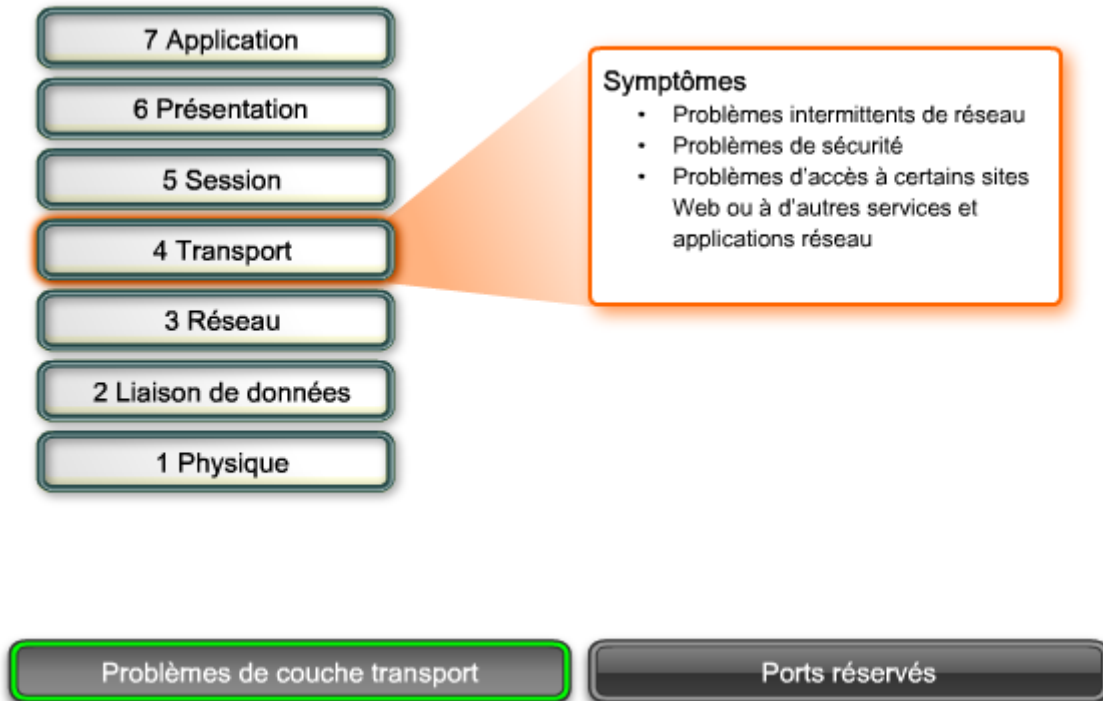
La couche 4, ou couche de transport, est considérée comme une transition entre les couches supérieure et inférieure du modèle OSI. La couche 4 est responsable du transport des paquets de données. Elle spécifie le numéro de port utilisé pour accéder à des applications spécifiques. Des problèmes de réseau de couche 4 peuvent survenir en périphérie du réseau, où les technologies de sécurité examinent et modifient le trafic. Beaucoup de problèmes sont signalés en raison de pare-feu configurés pour refuser le trafic basé sur les numéros de port, même si ce trafic doit être transféré.

La couche 4 prend en charge les trafics UDP et TCP. Certaines applications utilisent TCP, d'autres utilisent UDP, d'autres encore utilisent les deux. En cas d'interdiction de trafic basé sur le numéro de port, il est nécessaire de spécifier le protocole de transport utilisé. Certains ingénieurs réseau ne connaissent pas le protocole de transport utilisé par des applications spécifiques et refusent donc le numéro de port pour les trafics TCP et UDP. Cette situation peut provoquer l'interdiction d'un trafic qui devrait être autorisé.

Les pare-feu sont souvent configurés pour interdire tous les éléments autres que les applications spécifiées dans les instructions permit. Si le trafic qui doit être autorisé n'est pas inclus dans les instructions du pare-feu, ou si une nouvelle application est ajoutée au réseau sans la permission correspondante ajoutée au pare-feu, cela peut provoquer des problèmes de filtrage.

Une indication fréquente de problèmes de couche 4 est l'accès impossible à certains services Web, généralement des services vidéo ou audio.

Vérifiez si les ports autorisés et interdits par le pare-feu sont appropriés aux applications. Pour connaître les ports correspondant à des applications spécifiques, révisez les sections consacrées à TCP, UDP et aux ports dans CCNA Discovery : Réseaux domestiques et pour petites entreprises et CCNA Discovery : Travailler dans une PME ou chez un fournisseur de services Internet.



| Numéro du port de destination | Abréviation     | Définition                                                            |
|-------------------------------|-----------------|-----------------------------------------------------------------------|
| 20                            | Données FTP     | Protocole FTP (File Transfer Protocol) (pour le transfert de données) |
| 21                            | Contrôle FTP    | Protocole FTP (File Transfer Protocol) (pour établir la connexion)    |
| 23                            | TELNET          | TELEtype NETwork                                                      |
| 25                            | SMTP            | Simple Mail Transfer Protocol                                         |
| 53                            | DNS             | Service de noms de domaine                                            |
| 67                            | Client DHCP v4  | Protocole DHCP (Dynamic Host Configuration Protocol) (client)         |
| 68                            | Serveur DHCP v4 | Protocole DHCP (Dynamic Host Configuration Protocol) (serveur)        |
| 69                            | TFTP            | Trivial File Transfer Protocol                                        |
| 80                            | HTTP            | Hypertext Transfer Protocol                                           |
| 110                           | POP3            | Protocole POP3 (Post Office Protocol version 3)                       |
| 137                           | NBNS            | Microsoft NetBIOS Name Service (service de noms NetBIOS de Microsoft) |
| 143                           | IMAP4           | Protocole IMAP4 (Internet Message Access Protocol version 4)          |
| 161                           | SNMP            | Simple Network Management Protocol                                    |
| 443                           | HTTPS           | Protocole HTTPS (Hypertext Transfer Protocol Secure)                  |

Problèmes de couche transport

Ports réservés

## **5.2 Dépannage des problèmes de la couche supérieure**

La plupart des protocoles de couche supérieure fournissent des services utilisateur généralement utilisés pour l'administration des réseaux, le transfert de fichiers, les services de fichiers distribués, l'émulation de terminal et le courriel. Les protocoles de ces couches sont souvent appelés protocoles d'application TCP/IP, car la couche application du modèle TCP/IP englobe les trois couches supérieures du modèle OSI.

Les protocoles suivants font partie des protocoles de couche application TCP/IP les plus connus et les plus mis en œuvre :

- Telnet : permet aux utilisateurs d'établir des connexions de session de terminal avec des hôtes distants.

- HTTP : prend en charge l'échange sur le Web de fichiers texte, image, son, vidéo et d'autres fichiers multimédia.
- FTP : assure le transfert interactif de fichiers entre des hôtes, à l'aide du protocole TCP.
- TFTP : assure le simple transfert interactif de fichiers, généralement entre des hôtes et des périphériques réseau, à l'aide du protocole UDP.
- SMTP : prend en charge les services de base de livraison des messages électroniques.
- POP3 : se connecte aux serveurs de messagerie et télécharge le courriel vers une application cliente.
- IMAP4 : permet aux clients de messagerie d'accéder aux messages et de stocker les courriels sur les serveurs.
- SNMP : collecte des informations provenant des périphériques gérés.
- NTP : synchronise les hôtes et les périphériques réseau.
- DNS : associe les adresses IP aux noms attribués aux hôtes.
- SSL : garantit le chiffrement et l'authentification des transactions HTTP.
- SSH : permet l'accès à distance des terminaux aux serveurs et aux périphériques réseau.

Il est parfois difficile d'isoler les erreurs des couches supérieures, surtout si la configuration du client ne présente aucun problème évident. Pour déterminer si un problème réseau provient d'une fonction de couche supérieure, commencez par vérifier la connectivité de base.

À l'aide de la méthode de dépannage « Diviser et conquérir », vérifiez tout d'abord la connectivité de couche 3.

**Étape 1** : envoi d'une requête ping à la passerelle par défaut

**Étape 2** : vérification de la connectivité de bout en bout

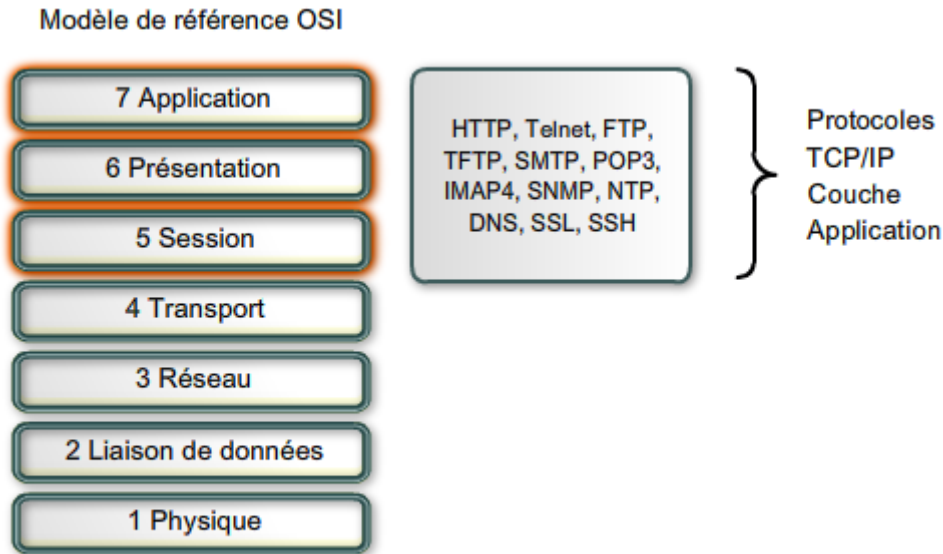
**Étape 3** : vérification de la configuration du routage

**Étape 4** : vérification du fonctionnement de la fonction NAT

**Étape 5** : vérification des règles de filtrage du pare-feu

Si le problème survient sur un réseau distant, la connectivité de bout en bout ne peut pas être vérifiée, car l'ensemble des connexions n'est plus contrôlé. Pour cette raison, il est possible que même si la configuration du périphérique local est correcte, il existe néanmoins un problème avec le réseau distant. Contactez l'ISP pour vous assurer que les connexions réseau sont actives et opérationnelles.

Après avoir effectué toutes ces étapes et avoir vérifié que l'erreur ne provenait pas de la connectivité de bout en bout, si le périphérique ne fonctionne toujours pas correctement, on peut en déduire que l'erreur provient des couches supérieures.



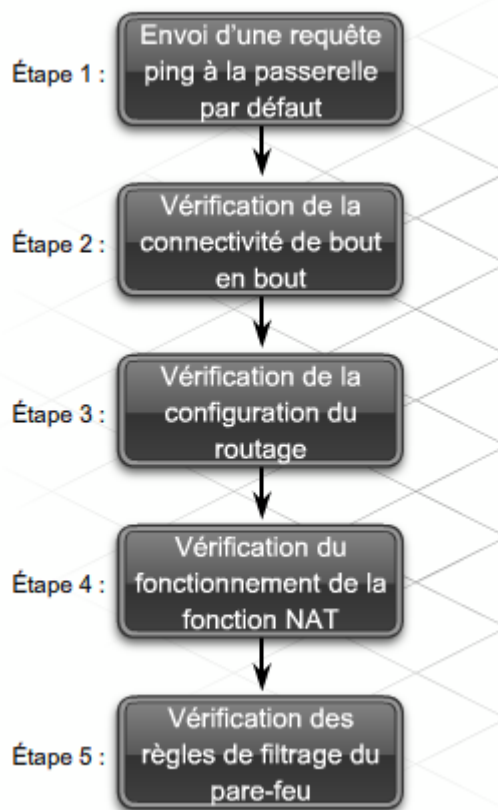
Les problèmes de couche supérieure empêchent les programmes d'application d'accéder aux services. Un problème au niveau des couches supérieures peut empêcher l'accès ou l'utilisation des ressources, même si les couches inférieures sont fonctionnelles. Il est possible que la connectivité réseau soit totale mais que l'application ne puisse pas fournir de données.

Les problèmes associés aux fonctions des couches supérieures n'affectent généralement que quelques applications, parfois même une seule. Les techniciens de support technique sont rarement contactés par des utilisateurs ne pouvant pas recevoir de courriels, même si les autres applications fonctionnent correctement.

Les applications clientes incorrectement configurées sont à l'origine de la majorité des problèmes réseau de couche supérieure. Lorsqu'une adresse électronique ou un serveur FTP incorrects sont spécifiés, le client ne peut pas accéder aux informations. Lorsque plusieurs applications sont affectées, le problème de couche supérieure peut être attribué à une erreur du serveur DNS.

Pour vérifier si le protocole DNS fonctionne correctement et peut résoudre les adresses de serveur, exécutez la commande Windows **nslookup**. Si le protocole DNS ne fonctionne pas de la façon souhaitée, vérifiez si l'adresse du serveur DNS est correctement configurée sur l'hôte. Lorsque les hôtes reçoivent des données du serveur DNS depuis un serveur DHCP, vérifiez si le serveur DHCP possède l'adresse IP appropriée au serveur DNS.

Si le serveur DNS est opérationnel et accessible, vérifiez l'éventuelle présence d'erreurs de configuration de la zone DNS. Recherchez une erreur typographique dans une adresse ou un nom contenu dans les fichiers.

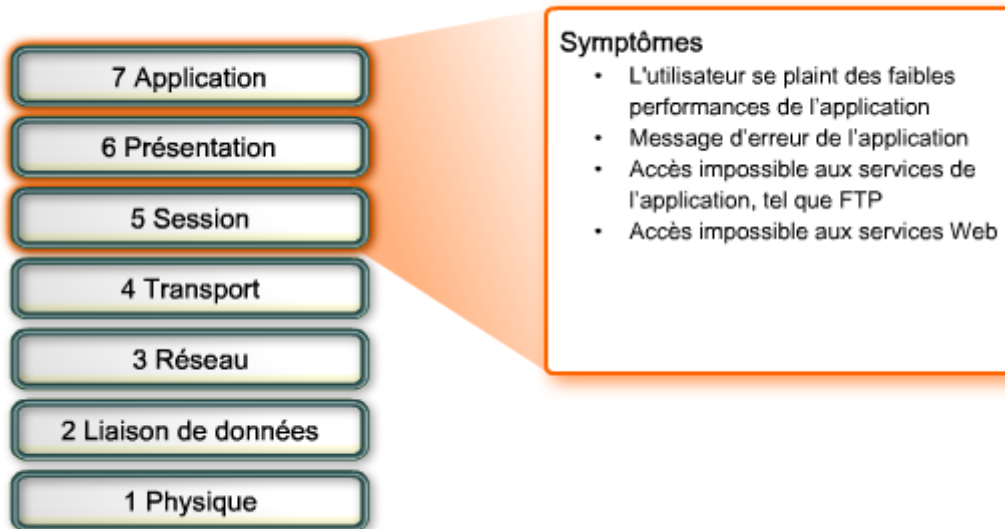


Les couches supérieures sont responsables du chiffrement et de la compression. Un conflit entre le mode de chiffrement ou de compression des données d'un client et le mode d'interprétation du serveur peut provoquer l'arrêt du fonctionnement ou le dysfonctionnement des applications.

Lorsqu'un problème survient sur un seul hôte ou sur une seule station de travail, il se peut qu'il provienne du mode d'interprétation des données dans le logiciel hôte. Des programmes d'extension du navigateur, tels qu'Adobe Reader, exécutent généralement des fonctions de couche supérieure. Pour assurer un affichage correct, ces programmes doivent être mis à jour pour les pages Web.

L'utilisation d'un protocole incorrect lors de la requête de données peut rendre une page Web inaccessible. Par exemple, il est parfois nécessaire de spécifier **https://** dans la ligne d'adresse du navigateur, plutôt que **http://** pour accéder à une page Web protégée par SSL.





### **5.3 Utilisation de Telnet pour vérifier la connectivité des couches supérieures**

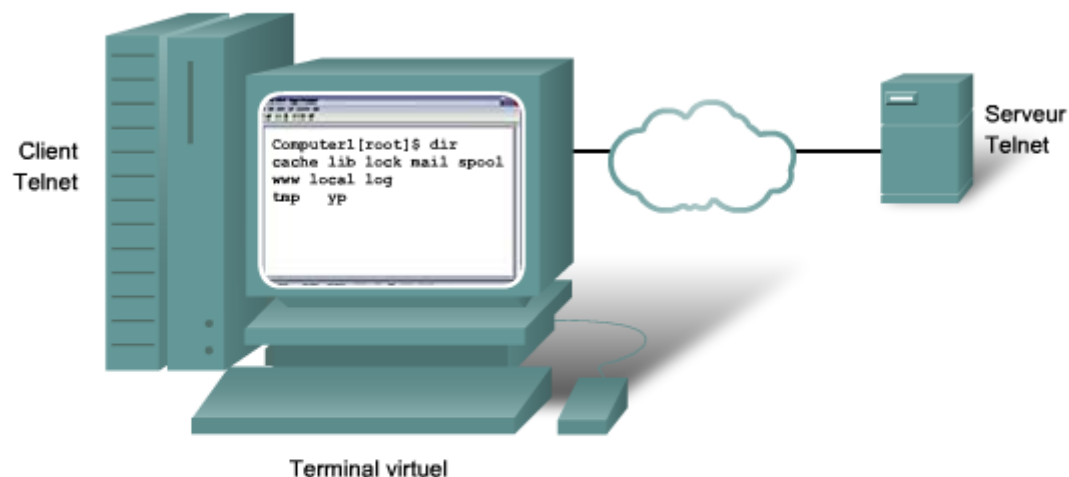
Telnet est un excellent outil de dépannage de problèmes liés aux fonctions des couches supérieures. L'utilisation de Telnet pour accéder aux périphériques réseau permet aux techniciens d'exécuter des commandes sur chaque périphérique, comme s'il s'agissait de périphériques locaux. En outre, la possibilité d'accéder aux périphériques via Telnet indique qu'il existe une connectivité des couches inférieures entre les périphériques.

Toutefois, Telnet est un protocole non sécurisé, ce qui signifie que toutes les données transmises peuvent être capturées et lues. S'il existe un risque que les communications soient interceptées par des utilisateurs non autorisés, il est conseillé d'utiliser de préférence le protocole SSH (Secure Shell). Le protocole SSH permet un accès distant plus sécurisé aux périphériques distants.

La plupart des versions récentes du logiciel Cisco IOS contiennent un serveur SSH. Dans certains périphériques, ce service est activé par défaut. D'autres périphériques requièrent une activation manuelle du serveur SSH.

Les périphériques Cisco IOS incluent également un client SSH permettant d'établir des sessions SSH avec d'autres périphériques. De même, vous pouvez utiliser un ordinateur distant doté d'un client SSH pour démarrer une session ILC sécurisée. Le logiciel de client SSH n'est pas fourni par défaut sur tous les systèmes d'exploitation. Il peut donc s'avérer nécessaire d'acquérir, d'installer et de configurer un logiciel de client SSH pour votre ordinateur.

Réviser la section de CCNA Discovery : Travailler dans une PME ou chez un fournisseur de services Internet consacrée à la configuration et à l'utilisation du protocole SSH.



Telnet permet d'utiliser un ordinateur, connecté via le réseau, pour accéder à un périphérique réseau comme si le clavier et le moniteur étaient connectés directement au périphérique.

**Travaux pratiques : Accéder aux périphériques réseau à l'aide de Telnet et SSH**

#### 5.4 Guide de certification du participant

#### Guide du participant CCENT

Cliquez sur l'icône des travaux pratiques pour télécharger la section 9.5 du Guide du participant CCENT

## 6 Préparation à la certification Cisco

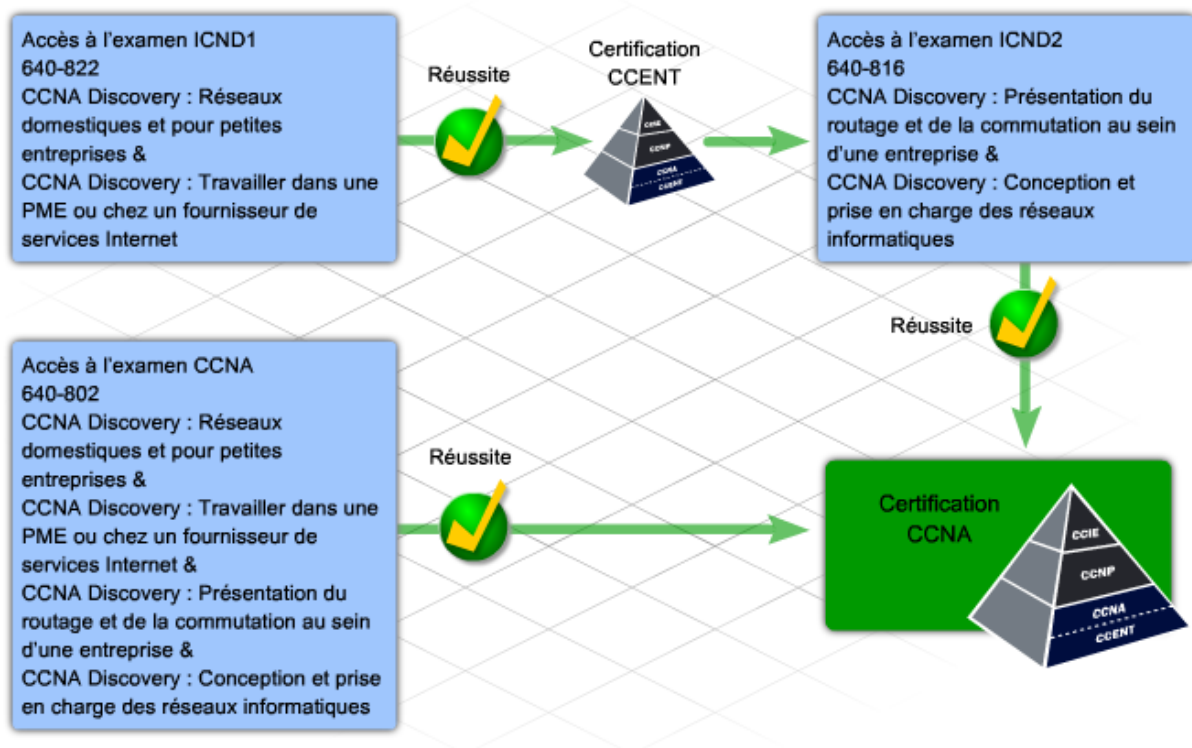
### 6.1 KSA (Connaissances, Compétences et Capacités)

La certification Cisco CCENT (Certified Entry Networking Technician) valide les compétences requises pour les emplois de base dans les domaines de prise en charge des réseaux, et constitue le point de départ d'un grand nombre de carrières liées à la gestion des réseaux. La certification CCENT est la première étape de la certification CCNA (Cisco Certified Network Associate), qui concerne la prise en charge de réseaux d'entreprise de taille moyenne, présentant des connexions plus complexes. Pour obtenir la certification CCENT, un candidat doit passer l'examen ICND1 dans un centre de tests certifié Cisco.

L'examen ICND1 (640-822) teste les capacités à installer, faire fonctionner et dépanner un petit réseau d'entreprise. Cet examen teste l'acquisition des notions de base sur les réseaux, et comporte les sections suivantes :

- Connexion à un réseau étendu
- Concepts de sécurité de base et de configuration d'un réseau sans fil
- Routage et commutation
- Modèles OSI et TCP/IP
- Adressage IP
- Technologies de réseau étendu
- Fonctionnement et configuration des périphériques Cisco IOS
- Configuration des routages RIPv2, statique et par défaut
- Implémentation de NAT et DHCP
- Configuration de réseaux simples

Réussir l'examen de certification Cisco n'est pas une tâche facile. La difficulté de la réussite de la série d'examens du CCNA de Cisco provient notamment des changements constants des exigences des examens Cisco. Certains candidats réussissent l'examen en première session, d'autres le réussissent après plusieurs épreuves, et d'autres ne le réussissent jamais. Pour réussir cet examen en première session, le meilleur conseil est de vous y préparer efficacement.



Avant de vous préparer à un examen de certification, il est essentiel de comprendre les objectifs de cet examen. Les examens de certification Cisco sont destinés à évaluer les connaissances, compétences et capacités des candidats dans un domaine particulier. Les examens utilisent une combinaison de techniques permettant à un candidat de démontrer sa préparation et sa faculté à remplir un grand nombre de tâches propres à la prise en charge des réseaux. L'examen comporte des Questions à Réponses Multiples (QRM), de nombreux exercices et des tâches de simulation de configuration de réseaux. Chaque question ou tâche

est destinée à remplir un but précis. Le site Web de la certification Cisco présente les objectifs de l'examen ICND1.

## **6.2 KSA : Connaissances, Compétences et Capacités pour la gestion des réseaux**

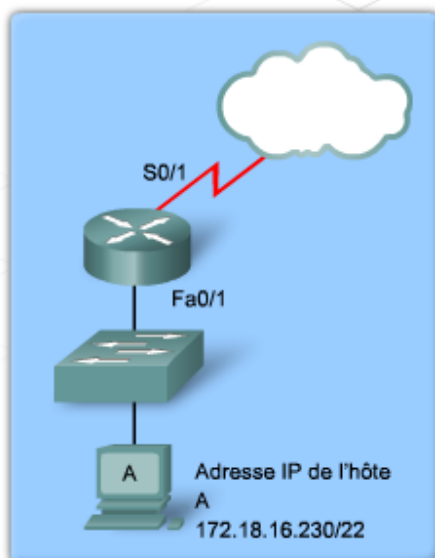
Pour remplir la plupart des tâches liées à la gestion réseau, certaines connaissances font appel à votre mémoire. Ce type de connaissances est composé de faits. Lors de la préparation à un examen de certification, il est utile d'identifier les faits pertinents associés à chaque objectif de l'examen. Certains candidats jugent utile de créer des cartes éclair pour s'aider à mémoriser ces faits. Bien que certaines questions de l'examen exigent des réponses évoquant des faits de base, la connaissance factuelle est plus souvent interpellée pour pouvoir diagnostiquer ou résoudre un problème réseau.

Un grand nombre de compétences sont indispensables à l'exécution des tâches de gestion d'un réseau. Certaines compétences sont relativement simples. C'est le cas, par exemple, de la création et du raccordement d'un câble croisé. D'autres tâches, telles que la maîtrise d'une structure de sous-réseaux IP, sont nettement plus complexes.

La maîtrise des compétences réseau requiert de l'expérience. Les travaux pratiques et les exercices Packet Tracer sont destinés à fournir aux candidats un environnement structuré de mise en pratique.

Les certifications Cisco évaluent et valident les compétences réseau d'un candidat, en fonction de leur interaction avec les périphériques réseau de Cisco. La pratique du logiciel Cisco IOS constitue donc un élément essentiel. Un grand nombre de questions de l'examen requièrent l'interprétation des résultats des commandes Cisco IOS, plus précisément celles des résultats des nombreuses commandes **show**.

Ce questionnaire d'exemple est destiné à tester les compétences du candidat en matière d'adressage IP. Dans le cadre de ce questionnaire, il est conseillé au candidat de se familiariser avec la configuration du logiciel Cisco IOS.



Reportez-vous à l'illustration. Quelle commande Cisco IOS permet d'attribuer la première adresse IP utilisable dans le sous-réseau à FastEthernet 0/1 de RTA ?

- A. RTA(config-if)#ip address 172.18.13.1 255.255.254.0
- B. RTA(config-if)#ip address 172.18.14.1 255.255.252.0
- C. RTA(config-if)#ip address 172.18.14.1 255.255.255.252
- D. RTA(config-if)#ip address 172.18.16.1 255.255.252.0
- E. RTA(config-if)#ip address 172.18.16.1 255.255.255.252
- F. RTA(config-if)#ip address 172.18.16.229 255.255.255.252

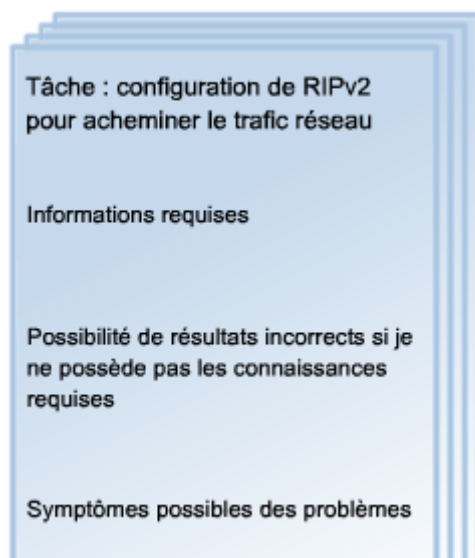
Les capacités à planifier, organiser, exécuter et résoudre les problèmes constituent les éléments essentiels de la réussite d'un technicien de support chargé de la gestion de réseaux

de petite envergure. Dans le cadre des examens de certification, ces capacités sont généralement évaluées par le biais de tâches de configuration et de dépannage. Lors de la conception des examens, un effort particulier est apporté pour simuler les conditions que rencontre quelqu'un chargé d'effectuer une tâche sur un réseau. Au cours de l'examen, ces conditions sont représentées dans les scénarios et les simulations.

Se préparer à une tâche de scénario ou de simulation n'est pas si simple que de mémoriser un fait ou de mettre une compétence spécifique en pratique. Ces types de tâches requièrent l'application des faits et des compétences nécessaires à la résolution d'un problème ou au respect d'une instruction.

Un des meilleurs moyens de développer ces capacités consiste à analyser tout d'abord les connaissances et les compétences nécessaires à la réussite de tâches réseau spécifiques. Une fois les informations requises identifiées, anticipez et demandez-vous ce qui se passerait si vous ne disposiez pas de ces informations. Dressez la liste des conséquences possibles et déterminez les compétences qui peuvent vous permettre d'identifier et de corriger les problèmes engendrés. Cela peut vous paraître difficile, mais voici quelques exemples susceptibles de vous aider.

- Qu'advierait-il si un technicien réseau utilisant un masque de sous-réseau spécifique ne connaissait pas le nombre exact d'adresses hôtes disponibles ? Comment les erreurs pourraient-elles être identifiées et corrigées ?
- Quels sont les problèmes que peut présenter un réseau RIPv2 possédant plus de 15 sauts entre une adresse source et une adresse de destination ? Quelle situation représenterait un symptôme de ce problème ? Comment ce problème peut-il être corrigé ?



**Travaux pratiques** : Identification des KSA : connaissances, compétences et capacités requises pour effectuer les tâches de ces travaux pratiques

### **6.3 Formulation de votre engagement**

Être prêt à passer l'examen de certification peut s'avérer une tâche des plus ardues. Le contenu des cours à étudier est volumineux, les compétences à acquérir sont nombreuses et la peur de l'échec peut vous déstabiliser. Tout comme l'installation du réseau chez un client, la préparation à l'examen est plus efficace si elle est fractionnée en petites étapes :

1. Formulation de votre engagement
2. Création d'un plan
3. Mise en pratique du test

Après avoir effectué ces différentes étapes, vous êtes prêt à commencer la préparation de l'examen.

La première chose à faire pour obtenir une certification Cisco est de vous engager à consacrer le temps et les efforts nécessaires à la préparation de l'examen. Il est essentiel d'affecter une priorité de sommet à cet engagement, car il vous prendra une partie du temps que vous consacriez à d'autres activités.

Outre le temps que vous devrez y consacrer, la préparation à un examen de certification requiert également de la concentration. Déterminez un endroit, à la maison ou dans l'établissement de formation, où vous pourrez passer de longues heures d'étude ininterrompue. Les efforts que vous devrez accomplir pour acquérir les compétences réseau, tant au niveau de l'étude que de la pratique, peuvent s'avérer extrêmement difficiles en présence de distractions.

Disposer des équipements et des ressources appropriés est aussi un élément très important. Vérifiez si vous disposez bien d'un ordinateur, si vous pouvez accéder au cursus en ligne et si Packet Tracer est installé sur votre ordinateur. Discutez avec votre formateur de la planification des travaux pratiques afin de pouvoir y insérer la durée nécessaire à la mise en pratique de vos compétences sur un équipement réel. Informez-vous de savoir si vous pouvez disposer d'un accès distant aux travaux pratiques, depuis Internet.

Informez vos amis et votre famille de votre volonté d'obtenir la certification CCENT. Expliquez-leur que leur assistance et leur soutien, pendant votre préparation à l'examen, peut constituer un élément de réussite non négligeable. Même s'ils ne disposent d'aucune connaissance en matière de gestion des réseaux, ils peuvent vous aider à étudier en rédigeant des cartes éclair ou en vous faisant réviser. Au minimum, ils peuvent vous aider en respectant le temps d'étude dont vous avez besoin pour préparer l'examen. Si d'autres participants de votre cours préparent l'examen en même temps que vous, il peut être intéressant d'organiser un groupe d'étude.

### **6.4 Création d'un plan**

Après avoir pris l'engagement de consacrer le temps nécessaire à la préparation de l'examen ICND1, la prochaine étape consiste à créer un plan. Un plan de préparation à l'examen de

certification contient des informations sur la manière dont vous souhaitez préparer l'examen, un calendrier de dates et heures et une liste des ressources.

Il existe deux approches d'étude d'un examen de certification : individuelle ou en groupe. Beaucoup de participants estiment qu'il est plus facile de se concentrer sur les différentes matières et de respecter un calendrier au sein d'un groupe d'étude.

Si vous étudiez avec un partenaire, ou au sein d'un groupe, il est essentiel pour chaque participant de savoir comment contacter les autres participants, de connaître le calendrier et les endroits des réunions et d'avoir accès à toutes les informations utiles. Il peut s'avérer nécessaire d'attribuer des responsabilités aux différents membres du groupe. Par exemple :

- Recherche et distribution des outils utiles à la préparation de l'examen
- Planification de la durée des travaux pratiques
- Vérification de la disponibilité de tous les équipements requis
- Traçage du suivi de la progression du groupe
- Recherche des réponses aux problèmes

Si vous décidez d'étudier seul, la coordination des ressources sera évidemment plus simple, mais l'importance d'une planification appropriée est toujours évidente.

Définissez une date cible réaliste pour passer l'examen, établie sur la base du temps dont vous disposez chaque semaine pour préparer l'examen.

Prévoyez des temps d'étude restreints pour la mémorisation des faits, et des durées plus conséquentes pour la mise en pratique des compétences. En effet, il est frustrant de commencer des travaux pratiques ou un exercice, et de ne pas disposer du temps nécessaire pour le terminer.

Le Guide du participant CCENT de Cisco Press, intitulé « 31 Days to the CCENT » (les 31 jours du CCENT) vous donne les clefs de la structuration d'un plan. Cet ouvrage présente chaque objectif de l'examen et met en évidence les données importantes à étudier. Il comporte également des références aux sections et rubriques des cursus CCNA Discovery : Réseaux domestiques et pour petites entreprises et CCNA Discovery : Travailler dans une PME ou chez un fournisseur de services Internet qu'il est important de réviser et de mettre en pratique.

Le meilleur moyen de créer un plan de travail consiste à consigner le temps disponible sur un calendrier. Affectez ensuite une tâche spécifique à chaque temps d'étude, par exemple « Étude des couches des modèles OSI et de leurs fonctions » ou « Mise en pratique de la création de sous-réseaux IP ». Une fois toutes les tâches consignées, déterminez la date de l'examen.

Étudiez les possibilités qu'offrent les outils et les ressources disponibles dans le cadre de votre étude. La certification ICND1 teste les connaissances et compétences obtenues dans ce cours, ainsi que tout le contenu du cursus CCNA Discovery : Réseaux domestiques et pour petites entreprises. Souvenez-vous que l'accès au cursus en ligne, aux Travaux pratiques et aux exercices Packet Tracer constituent des éléments essentiels à une préparation efficace à l'examen.



En plus de ces outils, le site Web de préparation à la certification Cisco propose divers auxiliaires de préparation. Le lien vers le centre de préparation Cisco CCNA Prep Center est le suivant :

[Centre de préparation Cisco CCNA Prep Center](#)

Cisco Press publie des carnets de notes couvrant les objectifs des examens du CCENT. Vous pouvez acquérir ces documents en les achetant dans la boutique Cisco Marketplace Bookstore.

[Boutique Cisco Marketplace Bookstore](#)

Une fois les ressources nécessaires rassemblées, il est important de les organiser. L'étude et la pratique des compétences et capacités du CCENT peuvent s'avérer difficiles si vous les approchez de façon anarchique. Il est plus facile de mémoriser et d'utiliser des informations qui ont été acquises de façon structurée.

### **6.5 Mise en pratique du test**

Se rappeler et exécuter des tâches réseau dans un environnement de test formel est différent de la réalisation de ces mêmes fonctions en classe ou à la maison. Il est important de comprendre la structure de l'examen et la façon dont il est géré.

#### **Visitez le centre de tests.**

Avant de passer l'examen, visitez le centre de tests pour comprendre le mode de gestion de l'examen. Posez des questions sur le déroulement des opérations. Certains centres de tests fournissent aux participants des salles de tests individuelles. D'autres font passer les examens dans des salles plus grandes, où plusieurs participants passent l'examen en même temps. Renseignez-vous sur ce qui est autorisé dans la salle d'examen et, surtout, ce qui est interdit. Visitez le site Web de certification Cisco pour trouver le centre de tests le plus proche de chez vous.

#### **Structure de l'examen**

Les examens de certification ont lieu en ligne, de façon similaire aux évaluations de la Networking Academy. Des différences existent cependant.

- Les questions d'évaluation peuvent être présentées avant le début de l'examen proprement dit. Il est important de répondre sincèrement à ces questions. Les questions d'évaluation n'ont aucun impact sur le contenu de l'examen, ni sur votre note finale.
- Les examens de certification sont chronométrés. Le temps restant s'affiche à l'écran pour que vous puissiez décider de la durée que vous souhaitez consacrer aux autres questions ou aux autres tâches.
- Un examen peut comporter un grand nombre de questions ou de tâches de type différent.

- Lorsque vous avez répondu à une question et que vous êtes passé à la suivante, vous ne pouvez plus y revenir.

Vous ne pouvez pas ignorer une question, ni la marquer pour y revenir par la suite. Si vous ne savez pas répondre à une question, tâchez de deviner la réponse et passez à la question suivante.

Les questions des examens de certification Cisco se présentent sous les formats suivants :

- Questions à Réponse Unique (QRU)
- Questions à Réponses Multiples (QRM)
- Glisser / Déposer
- Questions à renseigner
- Petit test (testlet)
- Petite simulation (simlet)
- Simulations

Avant de passer l'examen, il est conseillé de se familiariser avec le fonctionnement de tous les types de questions, particulièrement avec le testlet, le simlet et l'outil de simulation. Ceci vous permet de vous concentrer sur les questions de l'examen, plutôt que sur l'utilisation correcte des outils. Entraînez-vous en utilisant le didacticiel de l'examen, disponible sur le site Web du centre de préparation Cisco CCNA Prep Center, jusqu'à ce que vous soyez familiarisé avec le format et le fonctionnement de chaque type de question et de tâche.

**Travaux pratiques : Utiliser le site Web du centre de préparation Cisco CCNA Prep Center pour accéder aux contenus et aux outils utiles à la préparation de l'examen CCENT**

Bien que rien ne remplace l'expérience de la situation réelle de l'examen, il est parfois utile de s'entraîner avec des situations d'évaluation. Le Centre de préparation Cisco CCNA Prep Center propose des exemples de tests de l'examen ICND1 sous forme de Questions à Réponses Multiples (QRM). Si vous préparez l'examen avec d'autres participants, vous pouvez créer des questions et les partager avec les autres participants. De plus, des exemples de questions d'examen sont disponibles sur le marché et téléchargeables sur Internet.

Les certifications Cisco contiennent des tâches qui simulent le fonctionnement des routeurs et commutateurs Cisco. Il est conseillé de refaire tous les exercices Packet Tracer et tous les travaux pratiques de ce cours pour vous préparer efficacement à l'examen ICND1. Toutefois, la simple lecture du cursus et la réalisation des travaux pratiques ne constituent pas une préparation suffisante quant aux types de tâches intégrées qui vous seront présentées à l'examen de certification. Il est important d'effectuer des recherches pour savoir ce qui peut se passer en cas d'erreur de définition ou de configuration d'un périphérique. Vous pourrez en savoir beaucoup plus en créant des situations d'erreur et en observant les modifications dans les résultats des commandes exécutées et en examinant le fonctionnement des équipements.

Un grand nombre des questions de scénario et de tâches de l'examen ICND1 mettent en scène le dépannage de problèmes réseau.

**Exercice Packet Tracer : Utiliser Telnet et d'autres outils pour dépanner un petit réseau.**

### ***6.6 Guide de certification du participant***

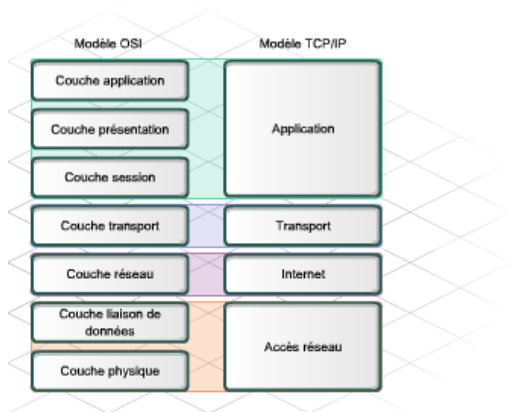
#### **Guide du participant CCENT**

#### **Guide du participant CCENT**

Outre les rubriques du Guide du participant présentées précédemment, la certification CCENT concerne également les réseaux étendus sans fil. Cette rubrique est présentée dans CCNA Discovery : Réseaux domestiques et pour petites entreprises. Pour des raisons pratiques, un Guide du participant consacré aux réseaux étendus est disponible [ici](#).

**Cliquez sur l'icône des travaux pratiques pour télécharger la rubrique du Guide du participant CCENT consacrée aux réseaux étendus.**

## 7 Résumé du chapitre

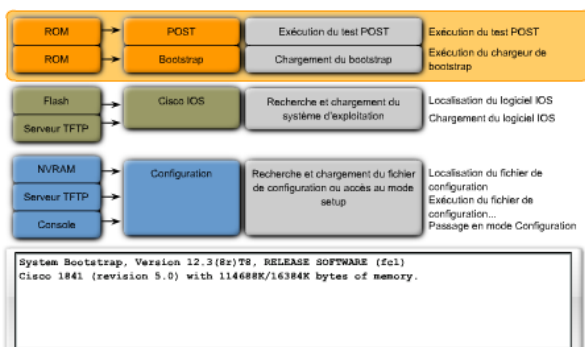
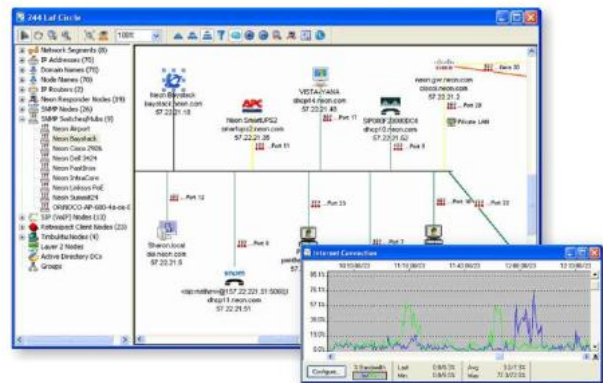


- Chaque couche du modèle OSI ou TCP/IP présente des fonctions et des protocoles spécifiques. Une connaissance des capacités, fonctions et périphériques de chaque couche, ainsi que des relations de chaque couche avec les couches avoisinantes, permet au technicien réseau de procéder efficacement au dépannage.
- Les couches supérieures (5-7) du modèle OSI traitent de la fonctionnalité de l'application et ne sont généralement implémentées que dans le logiciel. Les couches inférieures (1-4) du modèle OSI gèrent les fonctions de transport de données et les fonctions physiques du réseau.
- Il existe trois principales méthodes de dépannage des réseaux :
  - Descendant
  - Ascendant
  - Diviser et conquérir

Les outils qui peuvent vous aider dans les tâches de dépannage d'un réseau sont les suivants :

- Schémas et documentation du réseau
- Documentation du réseau et outils de création d'une ligne de base
- Systèmes d'administration de réseaux (NMS)
- Bases de connaissances
- Analyseurs de protocoles

Certaines défaillances des couches inférieures du modèle OSI ne sont pas facilement identifiées par les outils logiciels. Par conséquent, il est parfois nécessaire d'utiliser des outils matériels de dépannage tels que des testeurs de câble, des multimètres et des analyseurs réseau.



- La couche physique et la couche liaison de données englobent les fonctions matérielles et logicielles.
- La couche physique, ou Couche 1, est responsable des spécifications physiques et électriques de la transmission de bits d'un hôte à l'autre sur le support physique, qu'il soit filaire ou non filaire.
- Les problèmes qui peuvent être associés à la couche 1 sont les suivants :
  - Problèmes liés au type ou à la longueur des câbles, ou problèmes de raccordement
  - Conflit du mode bidirectionnel
  - Interférences et bruits (parasites) perturbant les transmissions
  - Erreurs liées aux périphériques matériels et erreurs d'amorçage
- Les erreurs d'interface du routeur constituent parfois le premier symptôme d'erreurs de câblage ou de connectivité des couches 1 et 2.
- Les LED des périphériques apportent des informations précieuses pour le dépannage et permettent parfois d'identifier les problèmes de connectivité.

- La couche liaison de données, ou couche 2, spécifie le mode de formatage des données transmises sur le réseau. Elle régle également les autorisations d'accès au réseau. La couche 2 fournit le lien entre les fonctions logicielles des couches réseau et les éléments matériels de la couche 1 pour les applications de réseau local et étendu.
- Les problèmes pouvant être liés à la couche 2 sont les suivants :
  - Conflits d'encapsulation
  - Messages de test d'activité non générés ou non reçus
  - Problèmes de synchronisation sur les connexions de réseau étendu
- Les commandes **show version**, **show interfaces** et **show interface brief** fournissent des informations de dépannage permettant d'isoler et d'identifier les erreurs et les problèmes des couches 1 et 2.

```

R1#show ip interface brief
Interface      IP-Address      OK? Method Status      Protocol
FastEthernet0/0 192.168.1.1    YES manual up          up
FastEthernet0/1 unassigned      YES manual administratively down down
Serial0/0/0     192.168.2.1    YES manual up          up
Serial0/0/1     unassigned      YES manual administratively down down
Vlan1           unassigned      YES manual administratively down down
    
```

Schéma d'adressage: exemple de 8 réseaux

| Sous-réseau | Adresse réseau   | Piège d'hôtes                 | Adresse de diffusion |
|-------------|------------------|-------------------------------|----------------------|
| 0           | 192.168.1.0/27   | 192.168.1.1 - 192.168.1.30    | 192.168.1.31         |
| 1           | 192.168.1.32/27  | 192.168.1.33 - 192.168.1.62   | 192.168.1.63         |
| 2           | 192.168.1.64/27  | 192.168.1.65 - 192.168.1.94   | 192.168.1.95         |
| 3           | 192.168.1.96/27  | 192.168.1.97 - 192.168.1.126  | 192.168.1.127        |
| 4           | 192.168.1.128/27 | 192.168.1.129 - 192.168.1.158 | 192.168.1.159        |
| 5           | 192.168.1.160/27 | 192.168.1.161 - 192.168.1.190 | 192.168.1.191        |
| 6           | 192.168.1.192/27 | 192.168.1.193 - 192.168.1.222 | 192.168.1.223        |
| 7           | 192.168.1.224/27 | 192.168.1.225 - 192.168.1.254 | 192.168.1.255        |

- Les principales fonctions mises en œuvre sur la couche 3 du modèle OSI concernent l'adressage réseau et le routage.
- Des schémas d'adressage non correctement conçus ou configurés, particulièrement au niveau du chevauchement des adresses de sous-réseau, sont à l'origine d'un grand nombre de problèmes de performances des réseaux.
- Le chevauchement des sous-réseaux peut être causé par une attribution d'adresse incorrecte, ou par une configuration incorrecte des masques de sous-réseaux sur les périphériques.
- Les problèmes d'attribution d'adresses IP depuis un serveur DHCP peuvent entraîner sur les ordinateurs clients la configuration automatique d'une adresse sur le réseau 169.254.0.0.
- Des problèmes liés à la configuration NAT et à son fonctionnement peuvent vous empêcher d'accéder à certains sites Internet depuis le réseau local à adressage privé.

- La plupart des réseaux utilisent une combinaison de routes statiques, dynamiques et par défaut.
- Les problèmes de routage peuvent provenir d'erreurs lors de la saisie manuelle des routes, d'erreurs de configuration et de fonctionnement des protocoles de routage, ou de défaillances des couches inférieures du modèle OSI.
- La commande **show ip route** constitue le principal outil de dépannage des problèmes de routage de la couche 3. La table de routage est constituée d'entrées de route provenant des sources suivantes :
  - Réseaux connectés directement
  - Routes statiques
  - Protocoles de routage dynamiques
- Les problèmes potentiels liés au routage RIPv2 sont les suivants :
  - Version non spécifiée, provoquant un conflit de version entre les routeurs.
  - Instructions réseau incorrectement configurées ou manquantes
  - Adresses IP d'interface incorrectement configurées

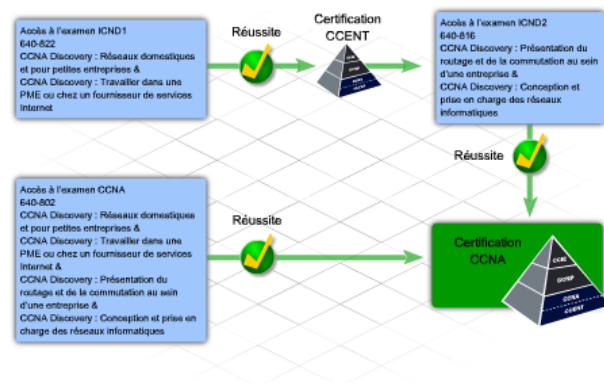


Telnet permet d'utiliser un ordinateur, connecté via le réseau, pour accéder à un périphérique réseau comme si le clavier et le moniteur étaient connectés directement au périphérique.

- La couche 4 est responsable du transport des paquets de données et de la spécification du numéro de port d'accès aux applications.
- Le pare-feu et les règles de filtrage de port qui régissent l'autorisation ou le refus d'accès aux ports incorrects peut empêcher l'accès aux périphériques requis depuis les ordinateurs clients.
- Les services des couches supérieures incluent la résolution de noms DNS, ainsi que la compression et le chiffrement. Des erreurs au niveau de ces fonctions peuvent rendre certaines applications utilisateur inutilisables.
- La commande Windows **nslookup** fournit des informations susceptibles de vous aider à résoudre les pannes de trafic DNS.

- La certification CCENT (Cisco Certified Entry Networking Technician) valide les compétences requises pour les emplois de base dans les domaines de prise en charge des réseaux, et constitue le point de départ d'un grand nombre de carrières liées à la gestion des réseaux.
- Pour obtenir la certification CCENT, les candidats doivent réussir l'examen ICND1 (640-822), qui teste leurs capacités à installer, faire fonctionner et dépanner le réseau d'une petite entreprise.
- Les certifications Cisco mesurent et valident les compétences des candidats en matière de gestion de réseaux, sur base de leur interaction avec les équipements réseau de Cisco. Un grand nombre de questions de l'examen requièrent l'interprétation des résultats des commandes Cisco IOS, particulièrement ceux des nombreuses commandes show.
- Tout comme l'installation du réseau chez un client, la préparation à l'examen est plus efficace si elle est fractionnée en petites étapes :

1. Acquisition des compétences
2. Création d'un plan
3. Positionnement en situation d'évaluation



## 8 Questionnaire du chapitre

### Question 1

Un administrateur réseau procède au dépannage de la connexion à un routeur et constate que l'adresse IP de l'interface S0/0/0 n'a pas été correctement configurée. Sur quelle couche du modèle OSI le problème trouve-t-il son origine ?

- Couche 1
- Couche 3
- Couche 4
- Couche 7

### Question 2

Faites glisser les paires de périphériques affichées à gauche sur le type de câble UTP auquel elles sont connectées sur la partie droite.

|                             |              |
|-----------------------------|--------------|
| Hôte / périphérique         | Câble droit  |
| Concentrateur / commutateur |              |
| Routeur / commutateur       |              |
| Routeurs Fa0/0 / hôte       | Câble croisé |
| Concentrateur / routeur     |              |
| Commutateur / commutateur   |              |

### Question 3

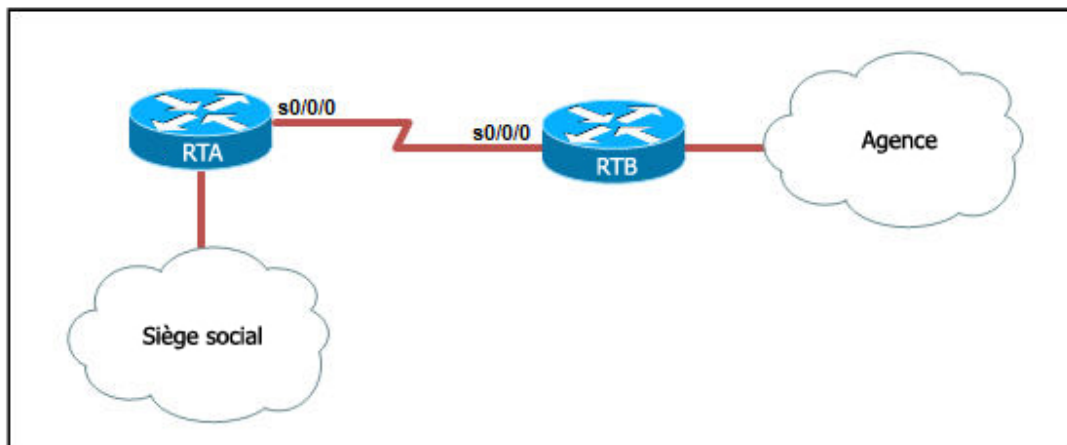


Sur la partie gauche, faites glisser chaque situation de réseau vers la couche OSI correspondante dans la partie droite.

|                                           |                                      |
|-------------------------------------------|--------------------------------------|
| Nombre excessif de diffusions             | Couche 1<br>[ ]<br>[ ]<br>[ ]<br>[ ] |
| Erreur d'encapsulation                    |                                      |
| Connexion câblée lâche                    |                                      |
| Alimentation sans coupure                 |                                      |
| Serial 0/0/0 activé, protocole désactivé  | Couche 2<br>[ ]<br>[ ]<br>[ ]<br>[ ] |
| Carte réseau mal configurée               |                                      |
| Type de câble incorrect                   |                                      |
| Connecteur de l'interface série endommagé |                                      |

#### Question 4

Reportez-vous à l'illustration. Un administrateur réseau procède au dépannage de la connexion entre le siège social et l'agence. Quelle information de dépannage importante l'administrateur doit-il obtenir du résultat de la commande **show interface serial 0/0/0** ?



- Type d'encapsulation
- Type de CSU/DSU
- Durée du CSU/DSU
- Type de protocole de routage

#### Question 5

Quel état de l'interface indique un taux d'erreur élevé ?

- Serial 0/0/0 désactivé, protocole de ligne désactivé
- Serial 0/0/0 activé, protocole de ligne désactivé
- Serial 0/0/0 activé, protocole de ligne désactivé (création de boucle)
- Serial 0/0/0 activé, protocole de ligne désactivé
- Serial 0/0/0 désactivé par l'administrateur, protocole de ligne désactivé

### Question 6

Reportez-vous à l'illustration. Les hôtes du réseau local peuvent communiquer avec les hôtes sur ce même réseau, mais ne peuvent se connecter en dehors du réseau. Quelle est la cause probable du problème ?

```
RouteurA(config)# ip dhcp pool LANpool
RouteurA(dhcp-config)# network 192.168.1.0 255.255.255.240
RouteurA(dhcp-config)# default-router 192.168.1.30
RouteurA(dhcp-config)# dns-server 192.168.1.2
RouteurA(dhcp-config)# end
%SYS-5-CONFIG_I: Configured from console by console
RouteurA#show ip dhcp binding
IP address      Client-ID/
                Hardware address
192.168.1.4     00D0.BCBD.993B   Feb 01 2008 8:15 AM   Automatic
192.168.1.5     00D0.D30B.C23E   Feb 01 2008 9:25 AM   Automatic
192.168.1.7     0001.C91C.D0EC   Feb 01 2008 10:21 AM  Automatic
```

- La commande **pool** n'est pas appliquée à une interface.
- L'adresse DNS est incorrecte.
- L'adresse DHCP est manquante.
- L'adresse de la passerelle par défaut est située sur un autre réseau.

### Question 7

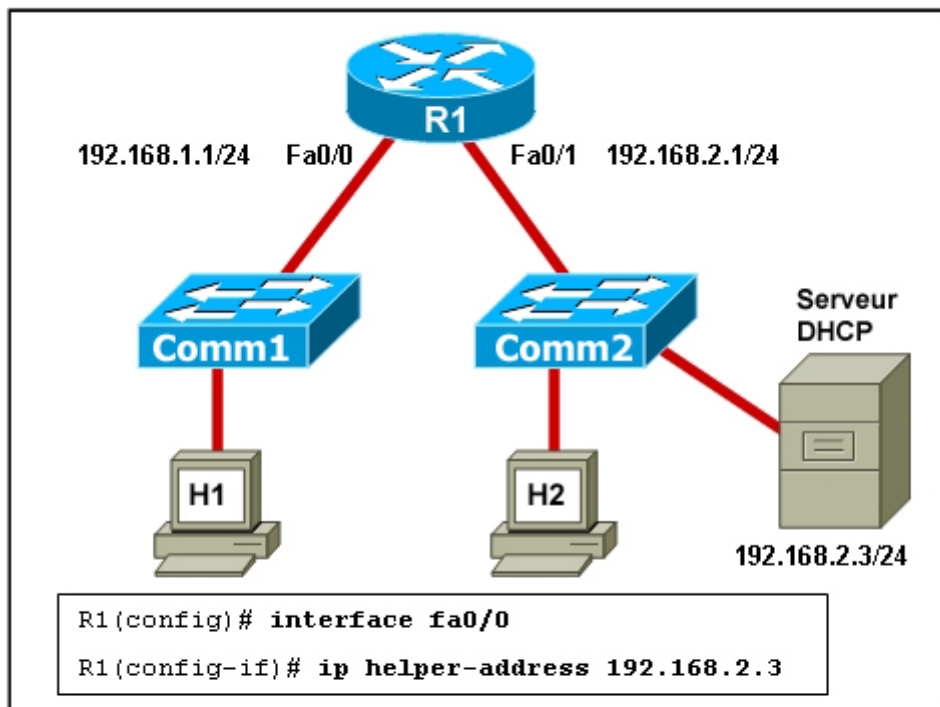
Reportez-vous à l'illustration. Quelles conclusions pouvez-vous tirer du résultat de la commande **debug ip rip** ?  
(Choisissez deux réponses.)

```
R1# debug ip rip
RIP protocol debugging is on
R1#
8d05h: RIP: sending v1 update to 255.255.255.255 via FastEthernet0/0 (172.16.1.1)
8d05h: RIP: build update entries
8d05h: network 10.0.0.0 metric 1
8d05h: network 192.168.1.0 metric 2
8d05h: RIP: sending v1 update to 255.255.255.255 via Serial0/0/0 (10.0.8.1)
8d05h: RIP: build update entries
8d05h: network 172.16.0.0 metric 1
R1#
8d05h: RIP: received v1 update from 10.0.15.2 on Serial0/0/0
8d05h: 192.168.1.0 in 1 hops
8d05h: 192.168.168.0 in 16 hops (inaccessible)
```

- Le réseau 10.0.0.0 est à deux sauts de distance du routeur R1.
- Une requête ping vers 192.168.168.10 aboutira.
- Le routeur a envoyé des informations concernant cinq destinations dans la mise à jour.
- R1 a envoyé une diffusion RIP sur Fa0/0, qui annonce deux réseaux.
- R1 a reçu des mises à jour d'un routeur à l'adresse source 10.0.15.2.

Question 8

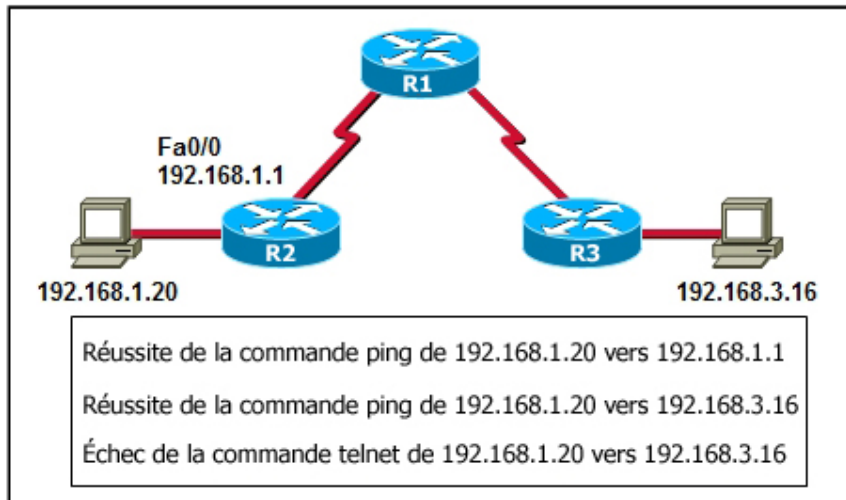
Reportez-vous à l'illustration. Quel est le résultat de la commande exécutée sur R1 ?



- Le réseau 192.168.1.0 ne recevra pas de paquets DHCP.
- Les accusés de réception DHCP seront émis depuis le réseau 192.168.1.0.
- Le commutateur COMM2 agit en tant qu'agent de relais DHCP pour le réseau 192.168.1.0.
- Les requêtes DHCP sont transmises à 192.168.2.3.

Question 9

Reportez-vous à l'illustration. D'après les résultats des commandes de dépannage, quelle est la cause probable du problème ?

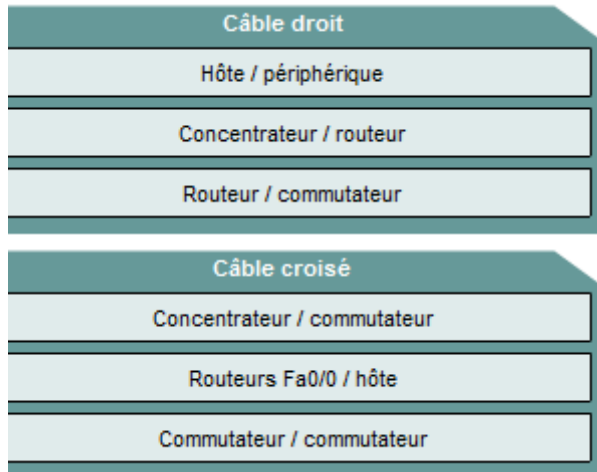


- Une adresse IP incorrecte a été affectée.
- Il se peut que les paquets soient bloqués par un pare-feu.
- Le protocole de routage n'est pas correctement configuré.
- Il existe une erreur d'encapsulation de couche 2.

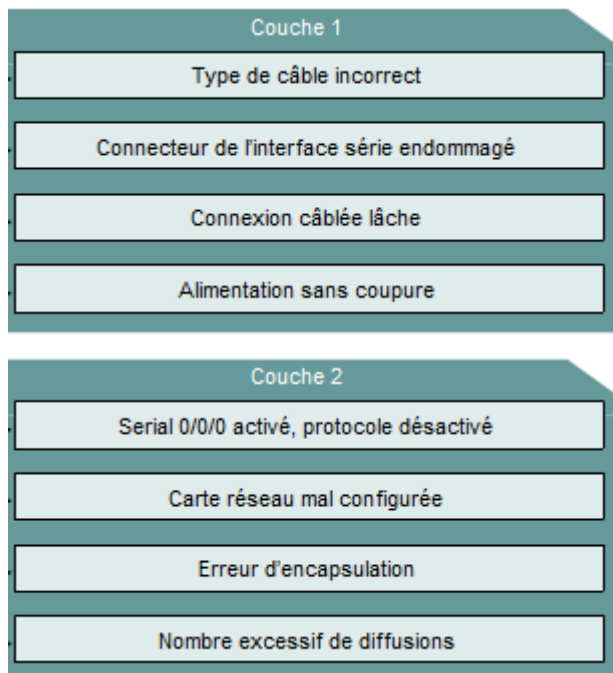
## Corrigé

Réponse 1 : 2

Reponse 2 :



Reponse 3 :



Reponse 4 : 1

Reponse 5 : 4

Reponse 6 : 4

Reponse 7 : 4 et 5

Reponse 8 : 4

Reponse 9 : 2