Microsoft®
Training &
Certification

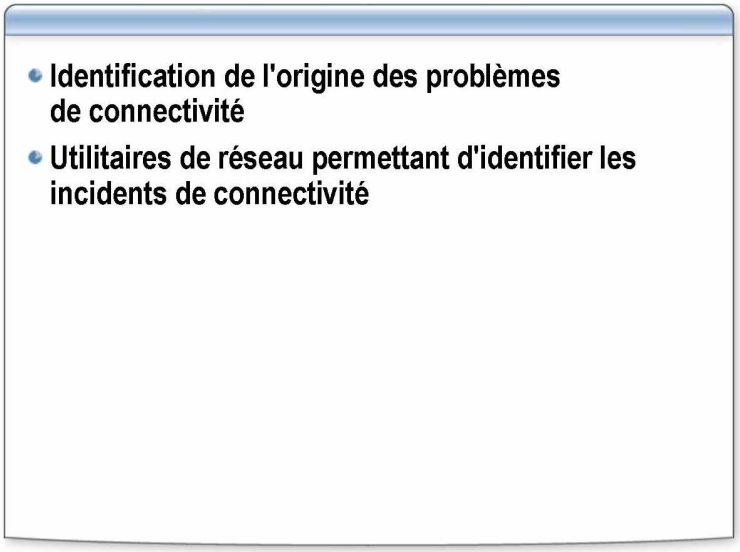
Microsoft® Official
Curriculum

Module 5 : Identification des incidents courants de connectivité

Table des matières

Microsoft®

Vue d'ensemble



**********DOCUMENT À L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

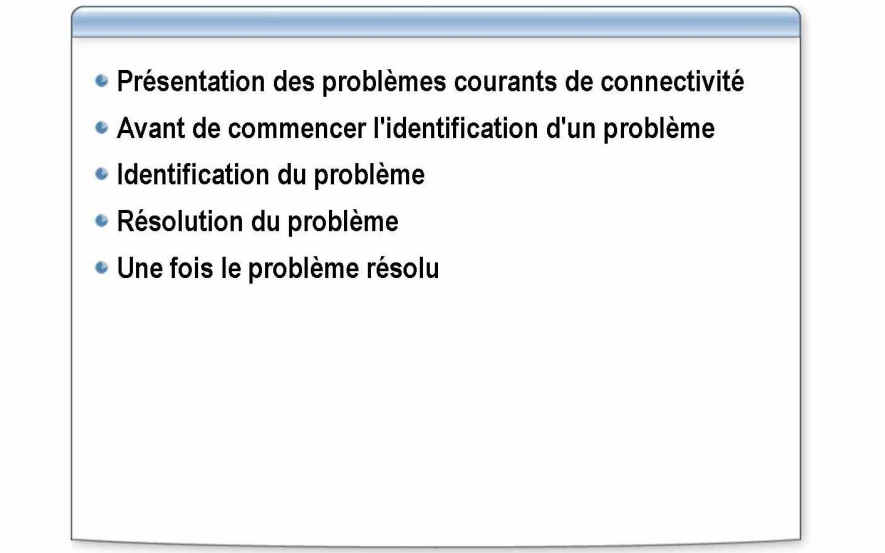
Ce module contient des informations sur la procédure d'identification des incidents courants de connectivité et sur le fonctionnement des outils et utilitaires de réseau mis en œuvre dans le cadre de cette procédure. Pour garantir la connexion au réseau, vous devez être en mesure d'identifier les incidents qui pourraient l'interrompre. Lorsqu'un problème de connectivité est détecté, vous secondez les ingénieurs système pour accélérer sa résolution.

Objectifs

À la fin de ce module, vous serez à même d'effectuer les tâches suivantes :

- suivre une procédure pour résoudre méthodiquement les problèmes de connectivité ;
- recourir à des utilitaires et à une aide extérieure pour identifier les problèmes de connectivité.

Leçon : Identification de l'origine des problèmes de connectivité



**********DOCUMENT À L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

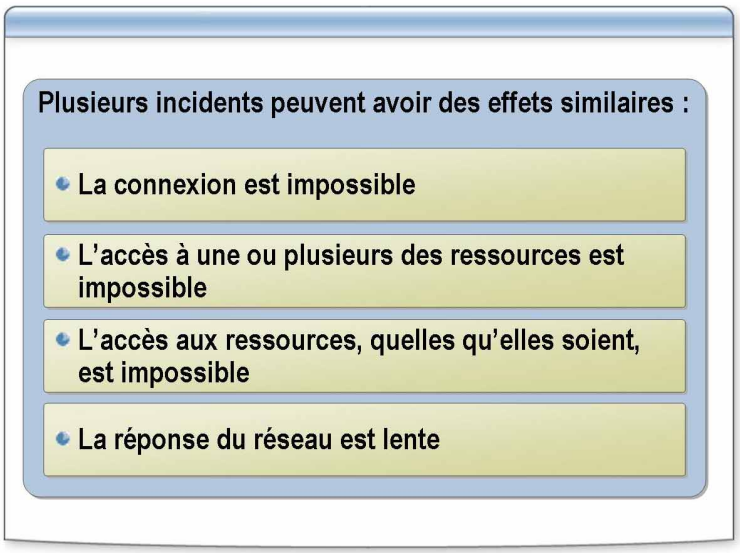
L'un des éléments clés de l'identification d'un problème réseau consiste à appliquer une stratégie efficace et systématique. Lorsque vous recevez un appel concernant un problème causé par l'utilisateur lui-même, il suffit de former rapidement ce dernier pour y remédier. En revanche, lorsque vous rencontrez un incident plus complexe, il est recommandé de suivre un ensemble de procédures pour identifier et résoudre le problème.

Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire les problèmes courants de connectivité ;
- élaborer une procédure permettant de gagner du temps lors de l'identification du problème ;
- suivre la procédure d'identification de l'incident pour remonter jusqu'à la source du problème ;
- établir un plan prévoyant l'implémentation de la solution ;
- organiser une réunion une fois le problème corrigé et noter les actions ayant permis sa résolution.

Présentation des problèmes courants de connectivité



**********DOCUMENT À L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

En tant qu'administrateur système, vous n'êtes pas en mesure de résoudre seul tous les incidents réseau. Cependant, vous devez être capable d'identifier la nature du problème et de déterminer s'il est de votre ressort ou si vous devez le transmettre à une personne plus qualifiée.

Problèmes courants

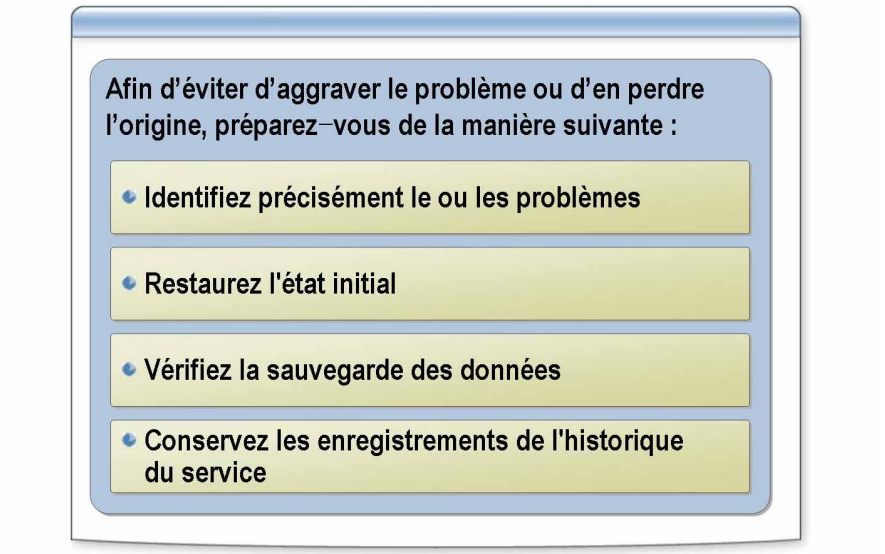
Les problèmes sont signalés, dans leur grande majorité, par les utilisateurs eux-mêmes lorsque ces derniers ne peuvent pas réaliser une action particulière sur leur ordinateur, qu'il s'agisse d'une action qu'ils pouvaient faire auparavant ou d'une action qu'ils pensaient pouvoir faire.

Il n'existe qu'un nombre limité de types de réclamations de base :

- L'utilisateur ne peut pas ouvrir de session.
- L'utilisateur ne peut pas accéder à une ou plusieurs ressources.
- L'utilisateur ne peut accéder à *aucune* ressource.
- La réponse du réseau est lente.

Un simple incident peut avoir plusieurs causes. Par exemple, si un utilisateur n'arrive pas à ouvrir une session, il se peut que le mot de passe entré soit incorrect, que tous les contrôleurs de domaine soient hors connexion ou qu'il y ait un problème au niveau d'un autre composant. La procédure d'identification d'un incident peut être longue et complexe (ou prendre seulement quelques minutes) en fonction de la nature du problème. Votre rôle consistera à identifier l'origine du problème parmi plusieurs causes possibles.

Avant de commencer l'identification d'un problème



**********DOCUMENT À L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

Si vous estimez qu'un incident va demander beaucoup d'efforts pour être résolu, la meilleure solution consiste à vous y préparer de façon à agir rapidement et efficacement et éviter que le problème ne s'aggrave.

Identifier précisément le ou les problèmes

Il est parfois difficile de déterminer la nature exacte d'un problème à partir de la description faite par l'utilisateur. La première démarche consiste donc à obtenir des informations précises sur le problème.

Pour vous aider à identifier le ou les problèmes, posez les questions suivantes :

- Quelles opérations étiez-vous en train d'effectuer lorsque le problème s'est produit ?
- L'ordinateur fonctionnait-il normalement avant l'apparition du problème ?
- Ce problème s'était-il déjà produit ?
- Aviez-vous rencontré d'autres problèmes ?
- Des composants matériels ou logiciels ont-ils été installés, supprimés ou reconfigurés récemment ?
- Avez-vous, ou quelqu'un d'autre, modifié quelque chose en essayant de résoudre le problème ?

Restaurer l'état initial

Avant de modifier la configuration de l'ordinateur ou d'un périphérique, pensez à noter ses paramètres d'origine. Effectuez les actions suivantes :

- noter la configuration réseau du client, qui inclut l'adresse IP (Internet Protocol), l'adresse IP de la passerelle par défaut et le masque de sous-réseau ;
- noter les services qui sont paramétrés pour s'exécuter automatiquement mais qui ne fonctionnent pas ;

- consulter le journal des événements pour connaître les erreurs qui s'étaient déjà produites avant que vous ne modifiiez la configuration ;
- utiliser la commande Ping pour déterminer le niveau de connectivité à la passerelle et aux ordinateurs distants avant de commencer.

Si le fait de désactiver une fonction ou de modifier un paramètre ne produit pas les résultats escomptés, restaurez cette fonction ou ce paramètre à l'aide de vos notes avant de tester une autre configuration. Si vous ne rétablissez pas les paramètres, d'autres problèmes pourraient survenir et il serait difficile de déterminer quelle action a entraîné quel résultat.

Vérifier la sauvegarde des données

Les sauvegardes sont importantes pour tous les ordinateurs, qu'il s'agisse de clients ou de serveurs à haute disponibilité. Si vous jugez que les efforts à fournir pour identifier un problème risquent d'aggraver la situation ou que les données importantes sont menacées, effectuez une sauvegarde avant de procéder à une modification quelconque. Vous serez ainsi en mesure de rétablir le système en cas de perte de données, d'erreurs d'arrêt ou de problèmes de démarrage.

Votre sauvegarde doit inclure les éléments suivants :

- le dossier personnel de l'utilisateur qui se trouve dans le dossier Documents and Settings. Celui-ci comprend le dossier Mes documents, ainsi que les dossiers qui contiennent des informations de personnalisation, telles que la liste des Favoris ou les paramètres du Bureau ;
- l'état du système, qui inclut le registre et d'autres fichiers système indispensables.

Remarque Un moyen rapide de sauvegarder les données importantes du client est d'utiliser l'Assistant Sauvegarde ou Restauration fourni avec Microsoft® Windows® XP. Pour lancer l'Assistant, cliquez sur **Panneau de configuration**, **Performances et maintenance**, puis sur **Sauvegarder vos données**.

Une fois la sauvegarde terminée, suivez les étapes ci-dessous pour vérifier que les données ont été correctement enregistrées sur le support de sauvegarde :

- Utilisez l'option de vérification fournie avec le logiciel de sauvegarde.
- Restaurez quelques fichiers à partir du support de sauvegarde.

Conserver les enregistrements de l'historique du service

Pour connaître les tendances et les caractéristiques des performances de votre réseau, conservez une trace de toutes les opérations du service. Si votre réseau est de petite taille, vous pouvez simplement garder vos notes dans un carnet. En revanche, si votre réseau est important, une solution plus polyvalente est nécessaire.

Un moyen utile pour stocker un grand nombre d'enregistrements consiste à utiliser un système de gestion de base de données qui permet de créer une base de données de l'historique du service comportant un enregistrement par périphérique réseau. L'utilisation d'une base de données permet de rechercher dans tous les enregistrements les types d'incidents ou d'occurrences similaires qui ont eu lieu dans un intervalle de temps donné.

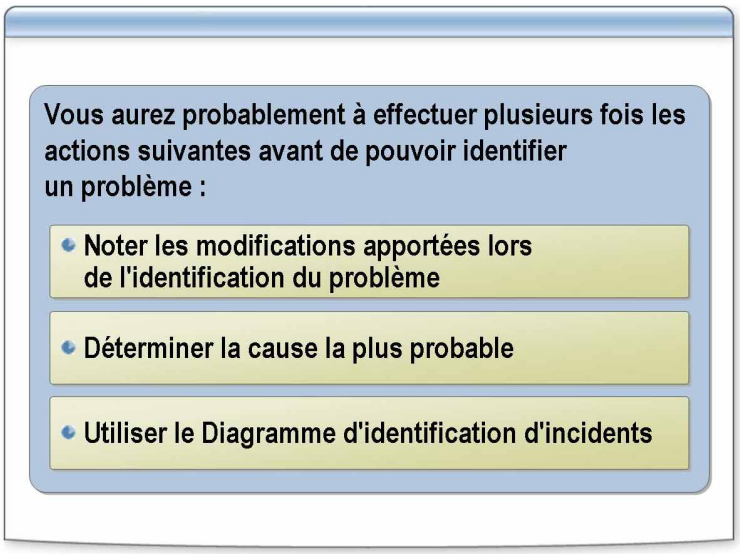
Quel que soit son support de stockage, chaque enregistrement doit d'abord fournir les informations sur les performances de base qui sont collectées pendant l'ajout de l'hôte sur le réseau. Mettez à jour les informations de base après chaque installation de composants matériels ou logiciels pour pouvoir comparer le comportement actuel et passé avec les niveaux de performances.

Les enregistrements de l'historique du service doivent comporter :

- les données sur les performances de base ;
- les dates et heures des problèmes et de leur résolution ;
- les modifications apportées ;
- les raisons de ces modifications ;
- le nom de la personne qui a effectué les modifications ;
- les effets positifs et négatifs qu'ont eu les modifications sur la stabilité et les performances du client et du réseau ;
- les informations fournies par le support technique.

Remarque Pour plus d'informations sur la création d'une base de données de gestion de la configuration, cliquez sur les liens Information Technology Infrastructure Library (ITIL) et Microsoft Operations Framework (MOF), accessibles depuis le CD-ROM du stagiaire.

Identification du problème



**********DOCUMENT À L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

La recherche de l'origine d'un problème peut s'avérer longue et difficile, ou prendre quelques minutes seulement. Dans un cas comme dans l'autre, le Diagramme d'identification d'incidents peut vous aider à trouver la solution la plus rapide.

Noter les modifications apportées lors de l'identification du problème

Le fait de noter les différentes étapes de la résolution d'un problème permet de revenir dessus une fois le problème corrigé. Ceci est utile lorsque vous rencontrez des problèmes complexes qui demandent de longues procédures avant d'être résolus. Cette technique permet :

- de vérifier que vous n'oubliez ni ne répétez aucune étape ;
- de vous faire aider par d'autres personnes ;
- d'évaluer l'efficacité de vos efforts ;
- d'identifier les étapes à suivre au cas où le problème se reproduirait.

Il est préférable de noter vos actions dès le début de la procédure d'identification, plutôt que d'attendre la fin et d'essayer de vous souvenir des étapes effectuées.

Déterminer la cause la plus probable

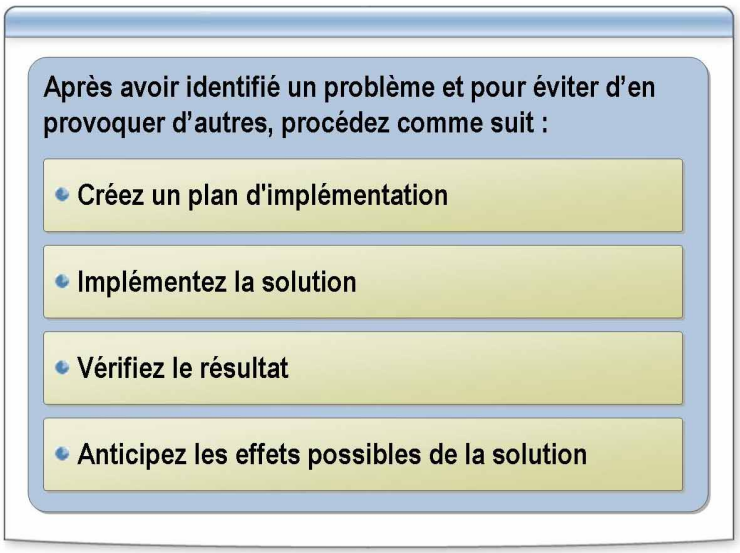
Lorsque vous recherchez l'origine d'un problème, commencez par les hypothèses les plus vraisemblables. Par exemple, si un client ne peut pas communiquer avec un serveur de fichiers, ne commencez pas par vérifier les routeurs situés entre les deux systèmes. Commencez par des choses plus simples, sur le client tout d'abord, telles que la vérification du câble reliant l'ordinateur au réseau.

Utiliser le Diagramme d'identification d'incidents

Le Diagramme d'identification d'incidents est joint en annexe C. Il traite en premier lieu des problèmes de connexion simples, puis s'intéresse aux problèmes de plus en plus complexes liés à la configuration du client, la résolution de noms, les routeurs, les pare-feux et les autres serveurs. Vous pouvez recourir à ce diagramme pour identifier un problème, comme par exemple un client unique ne pouvant obtenir l'adresse du protocole DHCP (Dynamic Host Configuration Protocol). Grâce à l'arbre de décision, vous ne perdez pas votre temps à essayer de résoudre un problème associé à une application ou à un périphérique spécifique, tel qu'un routeur ou un pont, qui concerne plusieurs ordinateurs. Sachant que ce problème ne touche qu'un seul ordinateur, le diagramme exclut toutes les tâches d'identification qui s'appliquent à plusieurs ordinateurs.

Le diagramme vous permet d'exécuter les étapes d'identification les plus appropriées et ce, dans un ordre logique. Vous déterminerez plus facilement si l'incident est un problème local que vous pouvez corriger par vous-même ou un problème plus vaste que vous devrez transmettre à des personnes plus qualifiées.

Résolution du problème



**********DOCUMENT À L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

Une fois l'origine du problème décelée, vous devez décider d'une méthode de résolution. Vous pourrez probablement corriger tout de suite un problème client simple. En revanche, un problème plus complexe, impliquant plusieurs serveurs connectés à des centaines de clients, peut nécessiter que plusieurs groupes de votre organisation collaborent entre eux.

Créez un plan d'implémentation

Après avoir identifié le problème et trouvé une solution qui a été testée sur un ou plusieurs des ordinateurs, il se peut que vous ayez besoin d'utiliser un plan d'implémentation si la solution doit être déployée dans toute l'organisation, par exemple sur plusieurs centaines ou milliers d'ordinateurs. Vous devrez synchroniser votre plan avec les responsables et les membres du personnel qui travaillent dans les zones affectées afin de vérifier que celui-ci n'entravera aucune activité importante.

Ce plan doit comprendre :

- une estimation du temps et des ressources nécessaires ;
- des dispositions pour effectuer le dépannage en dehors des heures de pointe ;
- un calendrier prévoyant les différentes phases de travail pendant la durée nécessaire ;
- du matériel de remplacement à utiliser tant que le matériel défaillant n'est pas réparé, au cas où celui-ci aurait un rôle vital.

Le nombre d'utilisateurs croissant sans cesse, le risque de perte de productivité liée à des perturbations augmente. Votre plan doit tenir compte des dépendances, permettre des modifications de dernière minute et inclure des plans de réserve pour faire face aux situations imprévues.

Implémentez la solution

Après avoir défini que le problème provenait d'un équipement particulier, essayez de déterminer s'il s'agit d'un problème matériel ou logiciel. Si le problème est matériel, vous pouvez essayer de remplacer l'unité défaillante. Par exemple, des problèmes de communication peuvent vous obliger à remplacer tous les câbles du réseau jusqu'à ce que vous ayez déterminé lequel est défectueux. De même, si le problème provient du serveur, vous pouvez être amené à remplacer certains composants, tels que les disques durs, en attendant d'avoir trouvé la pièce défaillante. Si le problème est logiciel, vous pouvez essayer de stocker vos données ou d'exécuter une application sur un autre ordinateur ou encore de réinstaller le logiciel sur le client qui pose problème.

Vérifiez le résultat

Une fois le problème corrigé, reprenez la procédure depuis le début et réexécutez la tâche ayant révélé le problème. Si le problème ne se reproduit pas, testez toutes les fonctions qui sont concernées par les modifications que vous avez effectuées afin de vous assurer que la résolution de ce problème n'en a pas entraîné d'autres.

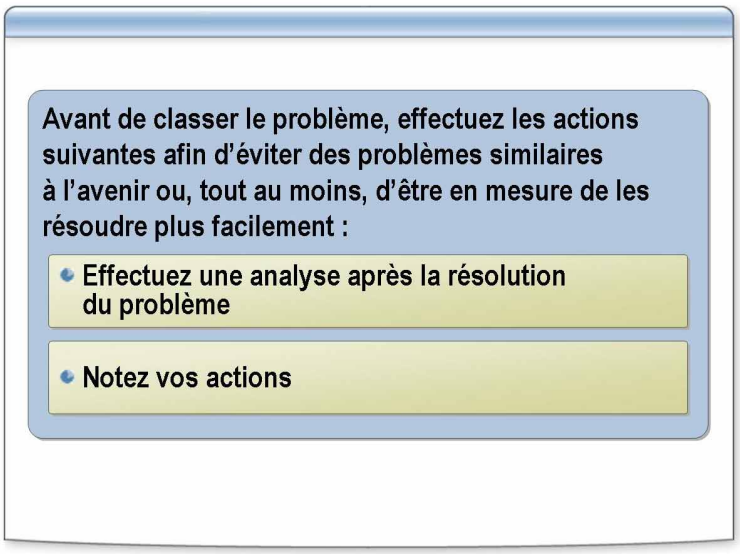
Les notes que vous avez prises sur la procédure d'identification s'avéreront ici fort utiles. Vous devrez suivre à la lettre la procédure dans son intégralité pour reproduire le problème d'origine et être sûr que celui-ci a été complètement éliminé et pas seulement masqué pour quelque temps. Si le problème apparaissait de façon sporadique, cela peut prendre un certain temps avant d'affirmer que votre solution a été efficace. Il peut être utile de vérifier plusieurs fois avec l'utilisateur que le problème a bien été réglé.

Anticipez les effets possibles de la solution

Il est essentiel, tout au long de la procédure de dépannage, de garder l'esprit ouvert sur l'ensemble du réseau et de ne pas s'enfermer dans les problèmes rencontrés par un seul utilisateur. Il peut parfois arriver que, lors de l'implémentation d'une solution, vous provoquiez un problème plus sérieux ou qui affecte un plus grand nombre de personnes.

Par exemple, un niveau de trafic trop élevé sur un sous-réseau qui entraîne une baisse des performances du client peut être corrigé en connectant certains ordinateurs à un autre sous-réseau. Cependant, bien que cette solution satisfasse les utilisateurs du sous-réseau défaillant, vous risquez de surcharger un autre sous-réseau, engendrant ainsi un problème plus grave. Il serait donc plus judicieux de créer un autre sous-réseau et d'y connecter certains des utilisateurs rencontrant des problèmes de trafic.

Une fois le problème résolu



**********DOCUMENT À L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

Après un retour à la normale du réseau, il est recommandé de revoir et de noter les événements passés afin d'éviter que des problèmes similaires n'apparaissent, ou tout du moins d'en minimiser l'impact.

Effectuez une analyse après la résolution du problème

À l'aide de vos documents compilés, effectuez une analyse après dépannage avec les parties concernées qui pourront vous aider, le cas échéant, à apporter des améliorations. Les questions ci-dessous pourront être soulevées lors de l'auto-évaluation :

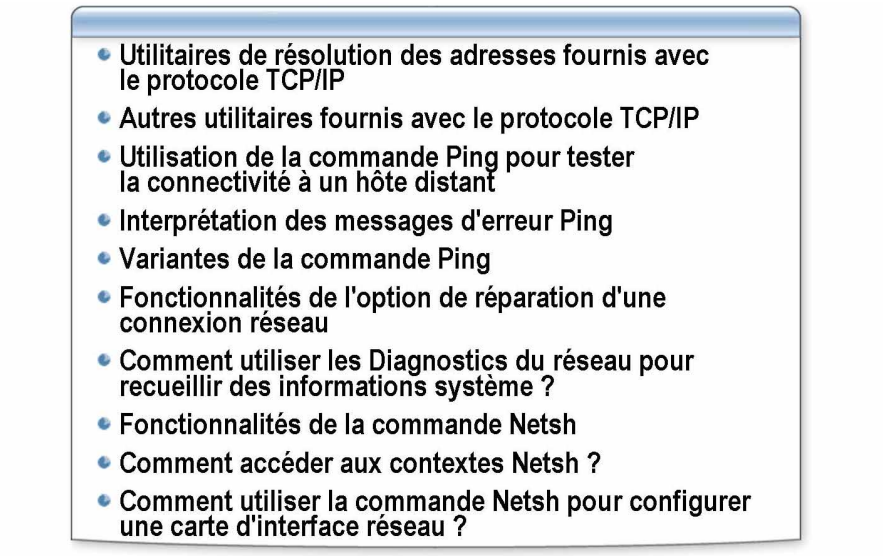
- Quelles modifications ont eu un résultat bénéfique ?
- Quelles modifications ont aggravé le problème ?
- Les performances du système ont-elles été rétablies conformément à ce qui était prévu ?
- Quelle tâche a été redondante ou inutile ?
- Les ressources du support technique se sont-elles avérées efficaces ?
- Quels utilitaires et informations potentiellement utiles n'ont pas été utilisés ?
- Quels problèmes non résolus requièrent une analyse plus poussée des causes premières ?

Lorsque cela est possible, il est également conseillé d'expliquer aux utilisateurs ce qui s'est produit et pourquoi cela s'est produit. L'aspect primordial de cette discussion consiste à faire savoir à l'utilisateur si ses actions ont causé le problème, l'ont aggravé ou l'ont rendu plus difficile à résoudre. De telles discussions peuvent faciliter de manière significative la résolution de problèmes futurs.

Notez vos actions

La phase finale de la résolution d'un problème repose sur la compilation de vos notes et documents afin de rédiger une synthèse du problème et de sa résolution, qui sera ensuite conservée dans la base de données de l'historique du service.

Leçon : Utilitaires de réseau permettant d'identifier les incidents de connectivité



**********DOCUMENT À L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

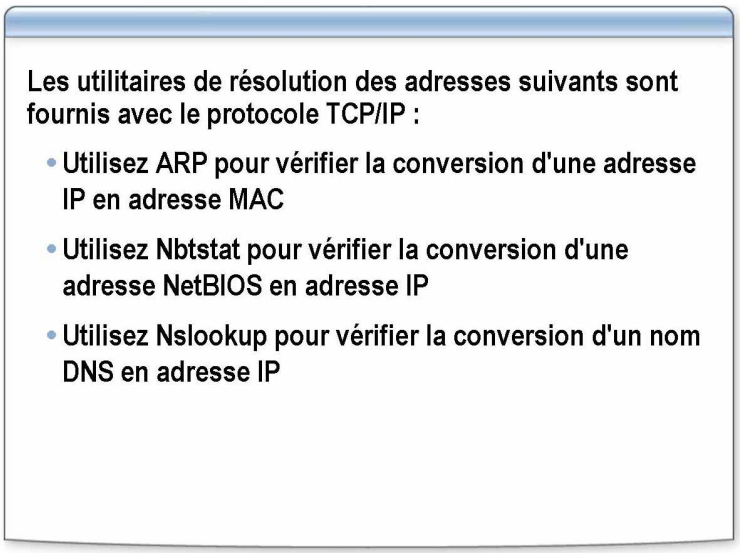
Windows Server™ 2003 installe automatiquement la plupart des utilitaires dont vous avez besoin pour identifier les problèmes de réseau lorsque vous installez le système d'exploitation. Toutefois, il existe un certain nombre d'utilitaires complémentaires que vous pouvez installer à partir du CD-ROM d'installation de Windows Server 2003, si nécessaire.

Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- employer les utilitaires de réseau nécessaires à l'identification des incidents de connectivité ;
- analyser les résultats fournis par les utilitaires pour vous aider à identifier les incidents de connectivité.

Utilitaires de résolution des adresses fournis avec le protocole TCP/IP



**********DOCUMENT À L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

Vous pouvez vous servir de trois utilitaires inclus avec le protocole TCP/IP (Transport Control Protocol/Internet Protocol) pour tester si les adresses IP sont converties en adresses MAC (Media Access Control), si des noms de protocole NetBIOS (Network Basic Input/Output System) sont convertis en adresses IP et si des noms DNS (Domain Name System) sont convertis en adresses IP.

Utilisez ARP pour vérifier la conversion d'une adresse IP en adresse MAC

Le protocole ARP (Address Resolution Protocol) convertit les adresses IP en adresses MAC, nécessaires aux protocoles de couche de liaison de données pour transmettre des trames. Afin de limiter le trafic réseau généré par le protocole ARP, le client stocke l'adresse matérielle convertie dans une mémoire cache de la mémoire système. Les informations restent dans le cache pendant une courte période (généralement entre 2 et 10 minutes), au cas où l'ordinateur aurait des paquets supplémentaires à envoyer à cette même adresse.

L'utilitaire Arp sert à manipuler le contenu du cache ARP. Par exemple, vous pouvez utiliser Arp.exe pour ajouter au cache les adresses matérielles des hôtes que vous contactez fréquemment afin de gagner du temps et limiter le trafic réseau lors de la connexion. Les adresses que vous ajoutez manuellement au cache sont statiques, ce qui signifie qu'elles ne sont pas supprimées à la fin de la période d'expiration. Toutefois, le cache étant stocké uniquement dans la mémoire, il est effacé à chaque redémarrage du client.

Si vous souhaitez précharger le cache à chaque démarrage du client, il est possible de créer un fichier de commandes qui contient les commandes Arp.exe et d'exécuter ce fichier à partir du groupe de démarrage Windows.

Le fichier Arp.exe utilise la syntaxe suivante :

```
ARP [-a {adresseip}] [-N adresseip] [-s adresseip adressehw
{interface}] [-d adresseip {interface}]
```

- **-a *{adresseip}*** Ce paramètre affiche le contenu du cache ARP. Le paramètre facultatif *adresseip* indique l'adresse d'une entrée de cache particulière à afficher.
- **-N *adresseip*** Ce paramètre affiche le contenu du cache ARP. La variable *adresseip* identifie l'interface réseau sur laquelle vous souhaitez afficher le cache.
- **-s *adresseip adressehw* {*interface*}** Ce paramètre ajoute une entrée au cache ARP. Le paramètre *adresseip* contient l'adresse IP du client, le paramètre *adressehw* contient l'adresse matérielle de ce même client et le paramètre *interface* contient l'adresse IP de l'interface réseau du système local dont vous souhaitez modifier le cache.
- **-d *adresseip* {*interface*}** Ce paramètre supprime l'entrée du cache ARP associée à l'hôte représenté par le paramètre *adresseip*. Le paramètre facultatif *interface* indique le cache à partir duquel l'entrée doit être supprimée.

Une table ARP se présente comme suit dans Arp.exe :

```
Interface : 192.168.2.6 sur l'interface 0x1000003
  Adresse Internet    Adresse physique      Type
  192.168.2.10        00-50-8b-e8-39-7a     dynamique
  192.168.2.99        08-00-4e-a5-70-0f     dynamique
```

Utilisez Nbtstat pour vérifier la conversion d'une adresse NetBIOS en adresse IP

Vous pouvez utiliser l'utilitaire de ligne de commande Nbtstat pour identifier les problèmes de conversion des noms NetBIOS. Par exemple, utilisez **nbtstat –n** pour déterminer si un nom NetBIOS spécifique est enregistré.

Lorsqu'un réseau fonctionne normalement, NetBIOS sur TCP/IP (NetBT) associe les noms NetBIOS aux adresses IP. NetBT utilise les options suivantes pour la conversion de nom NetBIOS et la recherche du cache local : requête du serveur WINS (Windows Internet Naming Service), diffusion, recherche LMHOSTS, recherche HOSTS et requête de serveur DNS.

Nbtstat permet d'afficher une grande variété d'informations, incluant :

- des statistiques du protocole NetBT ;
- des tables de noms NetBIOS pour le client local et les hôtes distants. La table de noms NetBIOS répertorie les noms NetBIOS correspondant aux applications NetBIOS qui fonctionnent sur le client ;
- le contenu du cache des noms NetBIOS. Le cache des noms NetBIOS est une table qui contient les mappages entre les noms NetBIOS et les adresses IP.

Nbtstat permet également d'actualiser le cache des noms NetBIOS et les noms enregistrés avec WINS. Voici un exemple des résultats créés à l'aide de Nbtstat :

```
C:\Documents and Settings\Administrateur>nbtstat -c

Connexion au réseau local:
Adresse IP du noeud : [192.168.0.5] ID d'étendue : []

                  Table de nom de cache distant NetBIOS

   Nom               Type       Adresse d'hôte     Vie [sec]
-------------------------------------------------------------
   MYLONDON     <03>  UNIQUE     192.168.0.200    -1
   MYLONDON     <00>  UNIQUE     192.168.0.200    -1
   MYLONDON     <20>  UNIQUE     192.168.0.200    -1
```

Utilisez Nslookup pour vérifier la conversion d'un nom DNS en adresse IP

Nslookup permet de générer des messages de requête DNS et de les envoyer à des serveurs DNS spécifiques via le réseau. Grâce à Nslookup, il est possible de déterminer quelle adresse IP un serveur DNS particulier a associé au nom d'hôte. La syntaxe de base de nslookup est la suivante :

NSLOOKUP *NomDNS ServeurDNS*

- ***NomDNS*** Indique le nom DNS à convertir.
- ***ServeurDNS*** Indique le nom DNS ou l'adresse IP du serveur DNS que vous souhaitez interroger pour connaître le nom spécifié dans le paramètre *NomDNS*.

Voici un exemple des résultats créés par l'utilitaire :

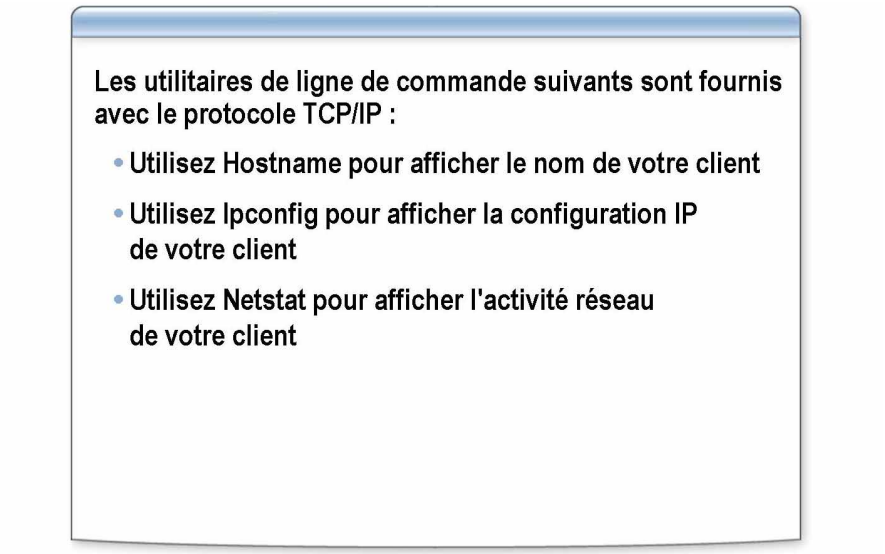
```
C:\>nslookup microsoft.com
Serveur :  dns1.rcsntx.sbcglobal.net
Adresse :  151.164.1.8

Réponse ne faisant pas autorité :
Nom :    microsoft.com
Adresse :  207.46.249.222
```

L'exemple indique que lorsque le serveur dns1.rcsntx.sbcglobal.net DNS est interrogé, il renvoie l'adresse 207.46.249.222 comme étant l'adresse IP associée au nom microsoft.com.

L'avantage de Nslookup est que vous pouvez tester la fonctionnalité et la qualité des informations sur un serveur DNS spécifique en les indiquant sur la ligne de commande.

Autres utilitaires fournis avec le protocole TCP/IP



**********DOCUMENT À L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

Lorsque Windows Server 2003 est installé, il comprend automatiquement le protocole TCP/IP, ainsi qu'un grand nombre d'utilitaires que vous pouvez utiliser pour analyser TCP/IP et vérifier la qualité de son fonctionnement.

Les utilitaires les plus courants sont décrits ci-dessous.

Utilisez Hostname pour afficher le nom de votre client

L'utilitaire Hostname affiche le nom d'hôte qui est attribué à votre client. Par défaut, le nom d'hôte est le nom de l'ordinateur client.

Utilisez Ipconfig pour afficher la configuration IP de votre client

L'utilitaire de ligne de commande Ipconfig permet d'afficher la configuration actuelle de la pile IP sur un ordinateur en réseau et d'actualiser les paramètres DHCP et DNS. L'utilitaire Ipconfig permet d'effectuer les actions suivantes :

- afficher les valeurs de la configuration du réseau TCP/IP actuelles ;
- mettre à jour ou résilier les baux DHCP alloués ;
- afficher, enregistrer ou effacer les noms DNS.

Ipconfig est particulièrement utile pour gérer les ordinateurs qui obtiennent une adresse IP automatiquement, à l'aide notamment du protocole DHCP ou de l'adressage APIPA (Automatic Private IP Addressing).

Utilisez Netstat pour afficher l'activité réseau de votre client

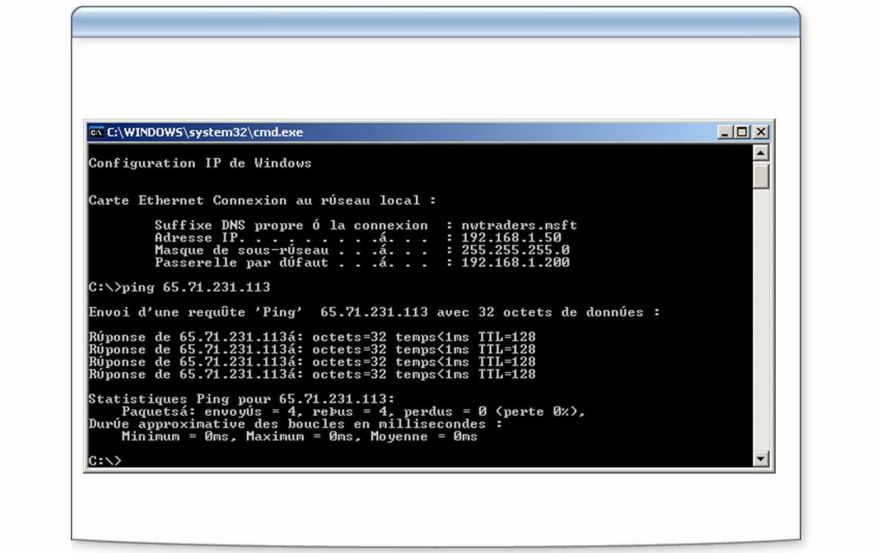
L'utilitaire Netstat affiche des informations sur les connexions réseau actives d'un client exécutant TCP/IP et sur le trafic généré par les divers protocoles TCP/IP. Vous pouvez l'utiliser pour savoir si un port est disponible ou non. Dans netstat, la liste des connexions réseau exécutées sur Windows Server 2003 se présente sous la forme suivante :

```
C:\>netstat

Connexions actives

  Proto  Adresse locale       Adresse distante     Etat
  TCP    bottxp :990          localhost :3124      ESTABLISHED
  TCP    bottxp :999          localhost :3127      ESTABLISHED
  TCP    bottxp :1024         localhost :3040      ESTABLISHED
  TCP    bottxp :3040         localhost :1024      ESTABLISHED
  TCP    bottxp :3119         localhost :7438      ESTABLISHED
  TCP    bottxp :3120         localhost :5679      ESTABLISHED
  TCP    bottxp :3124         localhost :990       ESTABLISHED
  TCP    bottxp :3125         localhost :5678      ESTABLISHED
  TCP    bottxp :3126         localhost :5678      ESTABLISHED
  TCP    bottxp :3127         localhost :999       ESTABLISHED
  TCP    bottxp :5678         localhost :3125      ESTABLISHED
  TCP    bottxp :5678         localhost :3126      ESTABLISHED
  TCP    bottxp :5679         localhost :3120      ESTABLISHED
  TCP    bottxp :7438         localhost :3119      ESTABLISHED
  TCP    bottxp :3098         etcdaldc1 :4092      ESTABLISHED
```

Utilisation de la commande Ping pour tester la connectivité à un hôte distant



**********DOCUMENT À L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

L'utilitaire Ping et ses variantes sont les utilitaires TCP/IP les plus courants. Vous pouvez utiliser Ping comme utilitaire principal de recherche d'incident de connectivité au niveau d'IP entre deux hôtes. Les tests Ping sont effectués de l'hôte le plus proche à l'hôte le plus distant jusqu'à ce que la défaillance soit trouvée. Une série de commandes Ping est à votre disposition pour tester la connectivité entre l'ordinateur local et l'ordinateur distant.

Test de connectivité à un hôte distant

Les étapes ci-dessous indiquent comment utiliser la commande Ping pour réaliser des tests de connectivité réseau sur des ordinateurs de plus en plus éloignés.

1. Exécutez la commande Ping sur l'adresse de bouclage en tapant **ping 127.0.0.1**

   Lorsque la commande Ping est correctement exécutée sur l'adresse de bouclage, elle vérifie l'installation et la configuration de TCP/IP sur le client local. Si le test de bouclage échoue, la pile IP ne répond pas. L'absence de réponse peut provenir d'une défaillance des pilotes TCP, du non-fonctionnement de la carte réseau ou de l'interférence d'un autre service avec IP. Lancez l'**Observateur d'événements** et recherchez les problèmes signalés par l'installation ou par le service TCP/IP.

2. Exécutez la commande Ping sur le client local en tapant **ping *<adresse IP du client local>***

   Lorsque la commande Ping est correctement exécutée sur l'adresse IP du client local, elle vérifie que le client a été ajouté au réseau. Si vous ne pouvez pas exécuter la commande Ping sur l'adresse IP locale après avoir correctement exécuté celle-ci sur l'adresse de bouclage, vérifiez l'adresse IP du client local, la table de routage et le pilote de la carte réseau.

3. Exécutez la commande Ping sur la passerelle par défaut de l'ordinateur local en tapant **ping <*adresse IP de la passerelle par défaut*>**

   Lorsque la commande Ping est correctement exécutée sur la passerelle par défaut du client local, elle vérifie que la passerelle par défaut fonctionne et que vous pouvez communiquer avec un hôte local du sous-réseau local. Si vous ne pouvez pas exécuter la commande Ping sur la passerelle par défaut après avoir exécuté celle-ci sur le client local, vérifiez la passerelle par défaut.

4. Exécutez la commande Ping sur l'adresse IP d'un autre ordinateur ou d'un autre périphérique réseau situé sur un réseau distant en tapant **ping <*adresse IP d'un hôte distant*>**

   Lorsque la commande Ping est correctement exécutée sur l'adresse IP de l'hôte distant, elle vérifie que le client local peut communiquer avec l'hôte distant via un routeur. Si l'hôte distant est situé sur un lien à délai élevé, (tel qu'un lien satellite), utilisez le paramètre **-w** (attente) pour définir un délai d'expiration plus long que le délai par défaut de quatre secondes.

   Si vous ne pouvez pas exécuter la commande Ping sur l'adresse IP de l'hôte distant après avoir exécuté la commande Ping sur la passerelle par défaut, il se peut que l'hôte distant ne réponde pas ou qu'il y ait un problème matériel réseau entre l'hôte source et l'hôte de destination. Pour exclure la possibilité d'un problème matériel réseau, envoyez une requête Ping sur un autre hôte distant du même sous-réseau que celui où se trouve le premier hôte distant.

5. Exécutez la commande Ping sur le nom d'un autre hôte du réseau distant en tapant **ping <*nom d'hôte d'un hôte distant*>**

   Lorsque la commande Ping est correctement exécutée sur le nom de l'hôte distant, elle vérifie qu'elle peut associer le nom d'hôte distant à une adresse IP. Si vous ne pouvez pas exécuter la commande Ping sur le nom d'hôte distant après avoir correctement exécuté la commande Ping sur l'adresse IP de l'hôte distant, le problème provient de l'association du nom d'hôte et non de la connectivité du réseau. Lorsque vous exécutez la commande Ping sur le nom de l'hôte cible, la commande essaie d'associer le nom à une adresse (d'abord via un serveur DNS, puis via un serveur WINS, le cas échéant) avant d'essayer d'envoyer un message à diffusion générale. Vérifiez les propriétés TCP/IP pour voir si le client dispose d'adresses de serveur DNS ou WINS configurées, qu'elles aient été entrées manuellement ou attribuées automatiquement. Si les adresses de serveur DNS et WINS sont configurées dans les propriétés TCP/IP et qu'elles apparaissent lorsque vous tapez **ipconfig /all**, essayez d'exécuter la commande Ping sur les adresses du serveur pour vous assurer qu'elles sont actives.

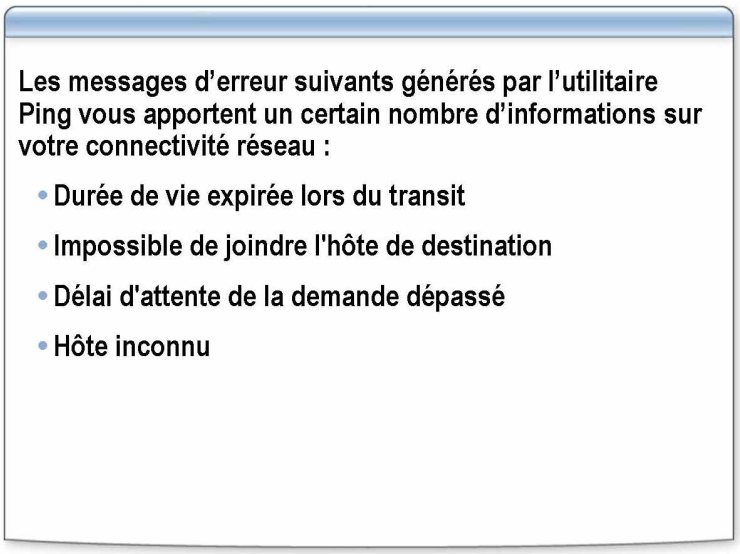
   Lorsqu'un réseau utilise le système DNS pour associer les noms et que le nom entré n'est pas un nom de domaine complet (FQDN, *Fully Qualified Domain Name*), le résolveur de nom DNS ajoute le ou les noms de domaine de l'ordinateur pour générer le nom de domaine complet. La résolution de nom peut échouer si vous n'utilisez pas un nom de domaine complet pour le nom distant. Ces requêtes échouent car le résolveur de nom DNS ajoute le suffixe du domaine local à un nom qui se trouve dans un autre emplacement de la hiérarchie du domaine.

6. Désactivez temporairement la sécurité IP (IPSec) et réexécutez toutes les commandes Ping précédentes.

   Si aucune ne réussit, vérifiez que IPSec est active. Si la sécurité IP est active au niveau local, arrêtez provisoirement les services IPSec dans le composant logiciel enfichable Services et réexécutez la commande Ping. Si la connectivité réseau entre les hôtes reste établie malgré la désactivation de la sécurité IP, contactez l'administrateur sécurité pour qu'il dépanne la stratégie IPSec.

Remarque Pour plus d'informations sur la sécurité IPSec, reportez-vous au module 8, « Protection du trafic réseau à l'aide de la sécurité IPSec et de certificats », du cours 2182A, *Implémentation, administration et maintenance d'une infrastructure réseau Microsoft Windows Server 2003 : services réseau.*

Interprétation des messages d'erreur Ping



**********DOCUMENT À L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

À chaque exécution de la commande Ping sur un hôte, une réponse positive ou un message d'erreur s'affiche pour indiquer le résultat de la requête. Le type d'erreur aide généralement à définir l'origine du problème de connectivité.

Durée de vie expirée lors du transit

Ce message indique que le nombre de sauts requis pour atteindre la destination a dépassé la durée de vie (TTL, *Time To Live*) définie par l'hôte émetteur pour transférer les paquets. La valeur TTL par défaut des demandes d'écho ICMP (Internet Control Message Protocol) qui sont envoyées par la commande Ping est 128. Cependant, il arrive que cette valeur ne soit pas assez élevée pour faire transiter le nombre de liens vers une destination. Vous pouvez alors augmenter cette valeur à l'aide du commutateur -i (maximum de 255 liens).

Si cela ne résout pas le problème, les paquets sont envoyés dans une boucle de routage, c'est-à-dire un chemin circulaire dans les routeurs.

Utilisez la commande Tracert pour connaître l'emplacement de la boucle de routage, qui apparaît comme la répétition des adresses IP contenues dans le rapport Tracert. Modifiez ensuite les tables de routage ou signalez le problème à l'administrateur d'un routeur distant.

Impossible de joindre l'hôte de destination

Ce message peut s'afficher à la suite de deux problèmes : le client local n'a aucune route vers la destination souhaitée ou un routeur distant signale qu'il n'a aucune route vers la destination. Suivant la forme sous laquelle se présente le message, vous pouvez distinguer les deux problèmes. Si le message est simplement « Impossible de joindre l'hôte de destination », cela signifie qu'il n'y a aucune route depuis le client local et que les paquets à envoyer n'ont pas été stockés sur le réseau. Utilisez alors l'utilitaire de routage pour vérifier la table de routage local pour un itinéraire direct vers la destination ou une passerelle par défaut.

Si le message est « Réponse de <*adresse IP*> : Impossible de joindre l'hôte de destination », le problème de routage se situe au niveau du routeur distant.

Délai d'attente de la demande dépassé

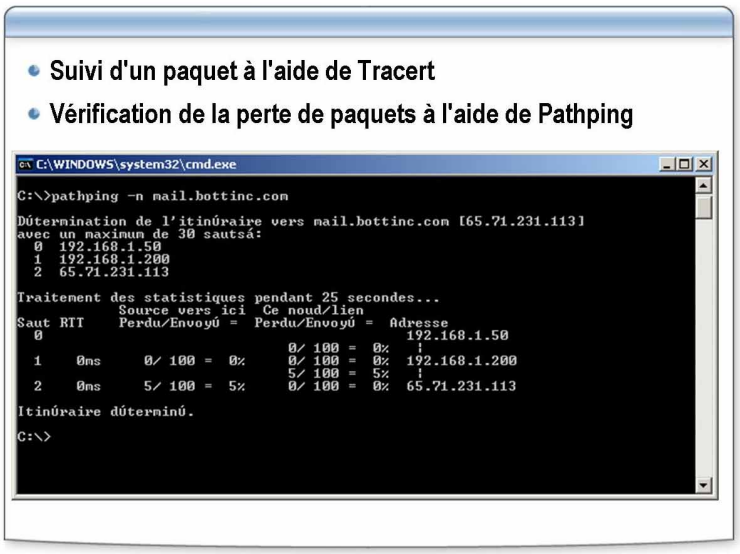
Ce message indique que les messages de réponse d'écho n'ont pas été reçus dans le délai imparti. Par défaut, l'utilitaire Ping attend quatre secondes par réponse devant être renvoyée avant que le délai n'expire. Si le système distant pour lequel a été exécutée la commande Ping se trouve sur un lien à délai élevé (par exemple, un lien satellite), le renvoi des réponses peut prendre plus de temps. Utilisez le commutateur **-w** (attente) pour spécifier un délai d'attente plus long.

Pour vérifier l'encombrement du réseau, augmentez la latence autorisée en définissant un temps d'attente supérieur (par exemple, 5 000 millisecondes) à l'aide du commutateur **-w**. Réexécutez la commande Ping sur la destination. Si la requête se heurte encore à un dépassement de délai, l'encombrement n'est pas la cause du problème. Il s'agit plus vraisemblablement d'un problème de résolution d'adresse ou d'une erreur de routage.

Hôte inconnu

Ce message d'erreur se présente sous la forme « La requête Ping n'a pas pu trouver l'hôte <*nom d'hôte*>. Vérifiez le nom et essayez à nouveau ». Il révèle que le nom d'hôte requis ne peut pas être converti en adresse IP. Vérifiez que le nom entré est correct et que les serveurs DNS sont en mesure de le convertir.

Variantes de la commande Ping



**********DOCUMENT À L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

L'uitilitaire Tracert est une variante de l'utilitaire Ping qui affiche l'itinéraire emprunté par les paquets pour atteindre leur destination, en plus des messages Ping habituels. Grâce à cette commande, vous pouvez définir la distance parcourue par les paquets avant de rencontrer un problème. La commande Pathping allie les fonctions des commandes Ping et Tracert pour obtenir des informations supplémentaires sur les performances du routeur et la fiabilité du lien qui ne sont disponibles avec aucun de ces outils.

Suivi d'un paquet à l'aide de Tracert

Compte tenu de la nature du routage IP, les chemins du réseau d'interconnexion peuvent changer d'une minute à l'autre. Tracert affiche la liste des routeurs qui transmettent actuellement des paquets vers une destination particulière.

Tracert utilise des messages d'écho ICMP et de réponse d'écho de la même façon que la commande Ping, à la différence près que Tracert modifie les messages en changeant la valeur de la durée de vie (TTL) de l'en-tête IP. La durée de vie est destinée à éviter que des paquets ne circulent indéfiniment dans les boucles du routeur sur le réseau. L'ordinateur qui génère le paquet définit une valeur de durée de vie relativement élevée. Sur les systèmes Windows, la valeur par défaut est 128. Chacun des routeurs qui traite le paquet réduit ensuite la valeur de un. Si la valeur atteint zéro, le dernier routeur rejette le paquet et envoie un message d'erreur ICMP à l'émetteur d'origine.

Lorsque vous lancez Tracert à l'aide de la commande Tracert avec le nom ou l'adresse IP d'un ordinateur cible, l'utilitaire génère un premier jeu de messages de demande d'écho dont la durée de vie est de 1 seconde. Lorsque le message atteint le premier routeur situé sur le chemin, le routeur réduit la valeur de la durée de vie à 0, rejette les paquets et signale les erreurs à l'émetteur. Les messages d'erreur contiennent l'adresse du routeur, désignée par Tracert comme le premier tronçon du chemin vers la destination. Le deuxième jeu de messages de demande d'écho généré par Tracert comporte une durée de vie de 2 secondes, ce qui oblige le second routeur situé sur le chemin à rejeter les paquets et à générer des messages d'erreur. Le troisième jeu de messages de demande d'écho comporte une durée de vie de 3 secondes, et ainsi de suite. Chaque jeu de paquets parcourt un saut de plus que le jeu précédent, ce qui force le routeur à envoyer des messages d'erreur à la source. La liste des routeurs affichée par Tracert comme étant l'itinéraire à suivre pour atteindre la destination résulte de tous ces messages d'erreur.

Vérification de la perte de paquets à l'aide de Pathping

Tout comme Tracert, Pathping indique l'itinéraire emprunté pour atteindre la destination. La commande Pathping envoie plusieurs messages de demande d'écho à chacun des routeurs situés entre la source et la destination pendant une certaine période de temps, puis traite les résultats en fonction des paquets renvoyés par chacun des routeurs. Étant donné que Pathping indique le pourcentage de paquets perdus sur tous les routeurs ou liens, vous pouvez déterminer quels routeurs ou sous-réseaux rencontrent des problèmes de réseau. Tout comme Tracert, Pathping identifie les routeurs présents sur le chemin. L'utilitaire exécute ensuite la commande Ping sur tous les routeurs pendant une période de temps spécifiée et traite les statistiques en fonction des valeurs renvoyées par chacun des routeurs.

Les données fournies par Pathping incluent :

- des informations sur les routeurs intermédiaires visités sur le chemin ;
- la valeur de l'heure du parcours circulaire (RTT) ;
- des informations sur la perte de liens.

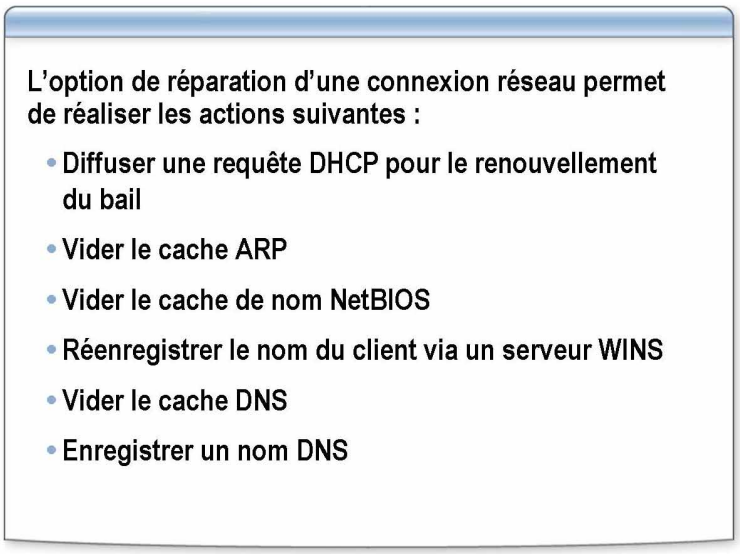
```
C:\Documents and Settings\Administrateur>pathping
microsoft.com

Détermination de l'itinéraire vers microsoft.com
[207.46.249.27]
avec un maximum de 30 sauts :
  0  londonsbs [192.168.0.57]
  1  192.168.0.1
  2  adsl-65-71-231-118.dsl.rcsntx.swbell.net [65.71.231.118]
  3     *     dist1-vlan130.rcsntx.swbell.net
[151.164.162.130]
  4  bb1-g1-0.rcsntx.swbell.net [151.164.1.174]
  5     *     core1-6-0.crdltx.sbcglobal.net [151.164.240.66]
  6  core1-p11-0.crhnva.sbcglobal.net [151.164.243.218]
  7     *     bb1-p10-0.hrndva.sbcglobal.net [151.164.242.70]
  8  bb1-p6-0.pxvnva.sbcglobal.net [151.164.241.26]
  9     *     asn8075-microsoft.pxvnva.sbcglobal.net
[151.164.89.194]
 10     *     gig0-0.core1.was1.us.msn.net [207.46.33.101]
 11  gig4-2.edge2.ash1.us.msn.net [207.46.34.22]
 12  207.46.34.25
 13  207.46.33.61
 14  207.46.36.214
 15  207.46.155.13
 16     *        *        *
```

```
Traitement des statistiques pendant 400 secondes...
           Source vers ici   Ce noeud/lien
Saut  RTT    Perdu/Envoyé = Pct  Perdu/Envoyé = Pct  Adresse
  0                                                 londonsbs
[192.168.0.57]
                                 0/ 100 =  0%   |
  1    2ms     0/ 100 =  0%     0/ 100 =  0%  192.168.0.1
                                 0/ 100 =  0%   |
  2   14ms     1/ 100 =  1%     1/ 100 =  1%  adsl-65-71-231-
118.dsl.rcsntx.swbell.net [65.71.231.118]
                                 0/ 100 =  0%   |
  3   15ms     1/ 100 =  1%     1/ 100 =  1%  dist1-
vlan130.rcsntx.swbell.net [151.164.162.130]
                                 0/ 100 =  0%   |
  4   14ms     0/ 100 =  0%     0/ 100 =  0%  bb1-g1-
0.rcsntx.swbell.net [151.164.1.174]
                                 0/ 100 =  0%   |
  5   15ms     0/ 100 =  0%     0/ 100 =  0%  core1-6-
0.crdltx.sbcglobal.net [151.164.240.66]
                                 0/ 100 =  0%   |
  6   31ms     0/ 100 =  0%     0/ 100 =  0%  core1-p11-
0.crhnva.sbcglobal.net [151.164.243.218]
                                 0/ 100 =  0%   |
  7   30ms     0/ 100 =  0%     0/ 100 =  0%  bb1-p10-
0.hrndva.sbcglobal.net [151.164.242.70]
                                 0/ 100 =  0%   |
  8   31ms     0/ 100 =  0%     0/ 100 =  0%  bb1-p6-
0.pxvnva.sbcglobal.net [151.164.241.26]
                                 0/ 100 =  0%   |
  9   35ms     0/ 100 =  0%     0/ 100 =  0%  asn8075-
microsoft.pxvnva.sbcglobal.net [151.164.89.194]
                                 1/ 100 =  1%   |
 10  ---     100/ 100 =100%    99/ 100 = 99%  gig0-
0.core1.was1.us.msn.net [207.46.33.101]
                                 0/ 100 =  0%   |
 11  ---     100/ 100 =100%    99/ 100 = 99%  gig4-
2.edge2.ash1.us.msn.net [207.46.34.22]
                                 0/ 100 =  0%   |
 12  ---     100/ 100 =100%    99/ 100 = 99%  207.46.34.25
                                 0/ 100 =  0%   |
 13  ---     100/ 100 =100%    99/ 100 = 99%  207.46.33.61
                                 0/ 100 =  0%   |
 14  ---     100/ 100 =100%    99/ 100 = 99%  207.46.36.214
                                 0/ 100 =  0%   |
 15   62ms     1/ 100 =  1%     0/ 100 =  0%  207.46.155.13
                                99/ 100 = 99%   |
 16  ---     100/ 100 =100%     0/ 100 =  0%  londonsbs
[0.0.0.0]

Itinéraire déterminé.
```

Fonctionnalités de l'option de réparation d'une connexion réseau



**********DOCUMENT À L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

L'option de réparation d'une connexion réseau regroupe six des commandes de dépannage TCP/IP les plus courantes en un seul utilitaire Windows.

Exécution de l'option de réparation d'une connexion réseau

Vous pouvez exécuter l'option de réparation d'une connexion réseau de l'une des trois manières suivantes :

- Cliquez avec le bouton droit sur l'icône **Connexion au réseau local** dans le dossier **Connexions réseau** et cliquez sur **Réparer**.
- Cliquez sur l'info-bulle qui apparaît dans la barre d'état lorsque la configuration IP n'est plus active, puis cliquez sur **Réparer**.
- Dans la boîte de dialogue **État de Connexion au réseau local**, cliquez sur l'onglet **Prise en charge**, puis sur **Réparer**.

Lorsque vous sélectionnez une connexion réseau, recherchez le lien **Réparer cette connexion** dans la partie gauche de l'écran, le cas échéant.

Les tâches ci-après sont effectuées dans l'ordre de leur apparition :

Diffuser une requête DHCP pour le renouvellement du bail

La diffusion d'une requête DHCP pour le renouvellement du bail est effectuée lorsque le bail atteint 87,5 % de sa durée de vie. Il est en effet plus sûr d'effectuer un renouvellement DHCP avant d'effectuer une libération DHCP. Si un serveur DHCP n'est pas disponible pour renouveler l'adresse, le client conserve son adresse actuelle. Si un nouveau serveur DHCP se connecte, le serveur DHCP ne peut pas envoyer d'accusé de réception au client et relance le processus de bail en corrigeant éventuellement le problème d'adresse IP.

Vider le cache ARP

Il arrive qu'une entrée de cache ARP devienne obsolète et que la communication ne puisse plus être établie jusqu'à ce que l'entrée concernée expire. Il peut également arriver qu'une entrée incorrecte de cache ARP statique qui ne possède pas de date d'expiration ait été placée sur le client. Le cache ARP est normalement vidé toutes les 2 ou 10 minutes, de sorte que cette opération est considérée comme sûre.

Remarque Si votre réseau utilise des entrées de cache ARP statiques, assurez-vous qu'il existe une possibilité de réentrer les adresses de cache ARP après que cet outil est lancé.

Vider le cache de nom NetBIOS

Le cache NetBIOS peut contenir des entrées obsolètes, ce qui empêche d'établir la communication. La commande **nbtstat –R** efface le cache de nom NetBIOS et recharge n'importe quelle entrée de nom NetBIOS dans le fichier Lmhosts avec l'indicateur #PRE.

Réenregistrer le nom du client via un serveur WINS

La commande **nbtstat –RR** sert à réenregistrer le nom du client via un serveur WINS. Cette commande s'avère très utile pour identifier des problèmes liés à la conversion de nom NetBIOS.

Remarque Cette tâche planifie seulement l'actualisation du nom avec le système d'exploitation sans vérifier si elle a été réussie ou non.

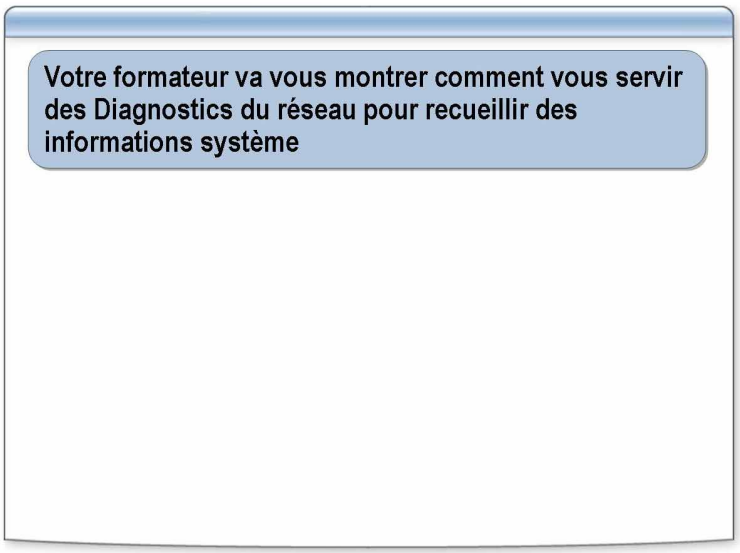
Vider le cache DNS

Cette tâche vide toutes les entrées du cache DNS non valides ou obsolètes de la mémoire. Cette commande s'avère très utile pour identifier des problèmes liés à la conversion de nom DNS.

Enregistrer un nom DNS

Cette tâche réenregistre le nom DNS du client via un serveur de mise à jour dynamique DNS.

Comment utiliser les Diagnostics du réseau pour recueillir des informations système ?



**********DOCUMENT À L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

Les diagnostics du réseau exécutent différents tests pour recueillir des informations importantes qui peuvent vous aider à identifier les causes des incidents liés au réseau. Selon les options que vous sélectionnez, les diagnostics du réseau analysent la connectivité réseau de votre système et vérifient si les programmes et les services liés au réseau fonctionnent. Ils recueillent également des informations de base concernant votre ordinateur.

Remarque La plupart des utilitaires dont vous avez besoin pour vous aider à identifier des problèmes réseau sont installés automatiquement avec Windows Server 2003. Si nécessaire, vous pouvez installer les Diagnostics du réseau et de nombreux autres outils de prise en charge Windows Server 2003 à partir du CD-ROM du système d'exploitation. Une fois ces outils installés, Netdiag.exe apparaît dans le dossier C:\Program Files\Support Tools.

Utilisation des Diagnostics du réseau

Contrairement à la plupart des utilitaires de réseau, Diagnostics du réseau est un utilitaire Windows et non un utilitaire de ligne de commande.

► **Pour analyser votre ordinateur à l'aide des Diagnostics du réseau**

1. Cliquez sur **Démarrer**, puis sur **Aide et support**.
2. Cliquez sur **Outils**.
3. Cliquez sur **Outils du Centre d'aide et de support**.
4. Cliquez sur **Diagnostics du réseau**.

5. Cliquez sur **Définir les options d'analyse**.

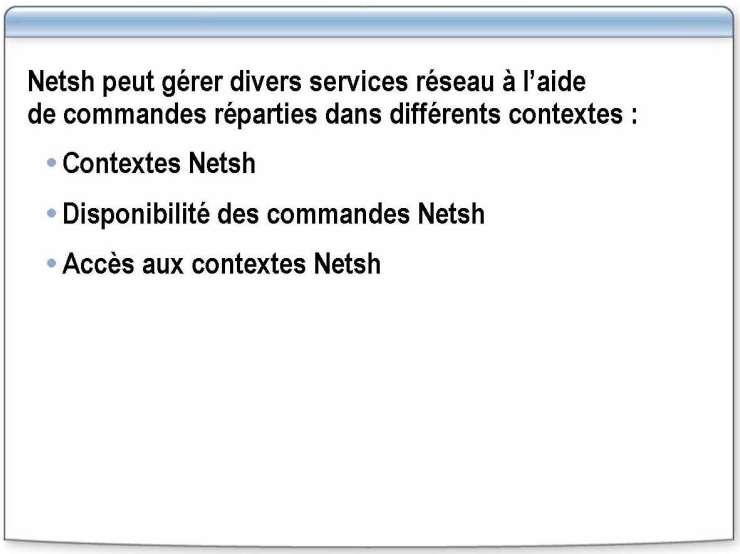
   La liste des options d'analyse s'affiche.

6. Sélectionnez toutes les options disponibles.

7. Cliquez sur **Analyser votre système**.

   Les diagnostics du réseau analysent votre système pour recueillir des informations sur vos composants matériels et logiciels, ainsi que sur vos connexions réseau, puis affichent les résultats dans la fenêtre sous forme de rapport.

Fonctionnalités de la commande Netsh



**********DOCUMENT À L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

Netsh est une interface de ligne de commande et de script s'exécutant depuis une invite de commandes, qui contient divers types de contextes et à partir de laquelle vous pouvez taper des commandes. Le contexte est indiqué par l'invite Netsh, dont la valeur par défaut est **netsh>**. Les commandes Netsh sont destinées à gérer et à analyser les services réseau, tels que DHCP, WINS, TCP/IP et IPSec.

Contextes Netsh

Chaque contexte Netsh permet de gérer un ensemble de fonctions réseau spécifiques. On appelle *contexte Netsh* l'état dans lequel Netsh accepte les commandes concernant un ensemble de fonctions spécifiques.

Disponibilité des commandes Netsh

Certaines commandes ne sont disponibles que dans un contexte particulier. D'autres sont disponibles non seulement dans le contexte affiché dans les listes de commandes, mais également dans tous les sous-contextes (le cas échéant).

Les commandes globales s'exécutent dans tous les contextes. Certaines d'entre elles, comme la commande d'aide, produisent des résultats différents selon les contextes. D'autres, telles que add helper, utilisée pour charger une nouvelle bibliothèque de liens dynamiques (DLL, *dynamic-link library*) d'application d'assistance dans Netsh, fournissent toujours le même résultat, quel que soit le contexte utilisé.

Accès aux contextes Netsh

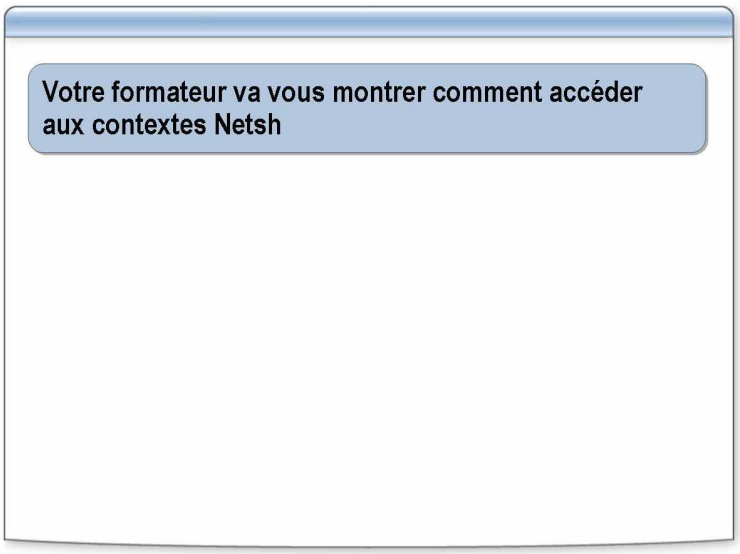
Les contextes sont organisés selon une hiérarchie. En haut de cette hiérarchie se trouve le contexte racine de Netsh. Le tableau ci-dessous regroupe, par ordre hiérarchique, les contextes et les sous-contextes, en plus de la DLL d'assistance qui fournit chaque contexte. La commande **show helper** de Netsh affiche les informations suivantes.

Contexte	Sous-contexte	Sous-contexte
aaaa		
diag		
dhcp		
	server	
		mscope
		scope
interface		
	ip	
ras		
	aaaa	
	appletalk	
	ip	
routing		
	ip	
		autodhcp
		dnsproxy
		igmp
		nat
		ospf
		relay
		rip
		routerdiscovery
wins		
	server	

Pour changer de contexte, tapez le nom du contexte désiré (par exemple, **interface**) dans l'invite **netsh>**. L'invite de commandes est modifiée pour correspondre au contexte entré. Si vous vous trouvez déjà dans un contexte, vous pouvez vous déplacer dans un sous-contexte en tapant simplement son nom (par exemple, **ip**).

Les contextes sont fournis par les DLL d'assistance. Si vous n'arrivez pas à accéder à un contexte particulier, suivez les instructions fournies par les DLL d'assistance afin de vous assurer que les fichiers correspondants au contexte sont chargés.

Comment accéder aux contextes Netsh ?



**********DOCUMENT À L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

Les commandes associées à la commande Netsh sont regroupées dans des contextes. Pour exécuter une commande Netsh, vous devez d'abord appeler cette dernière, puis indiquer le contexte qui comporte la commande désirée.

Utilisation des contextes de la commande Netsh

Pour accéder aux contextes de la commande Netsh

1. Ouvrez une fenêtre d'invite de commandes, puis entrez **netsh** comme indiqué ci-après :

   ```
   C:\>netsh
   ```

   Netsh devient l'interpréteur de la ligne de commande, encore appelé *shell*, et l'invite de commandes affiche :

   ```
   netsh>
   ```

   Vous êtes alors dans le contexte racine de Netsh et vous pouvez utiliser un nombre limité de commandes globales de Netsh.

2. Pour activer l'un des contextes Netsh, tels que le contexte IP sous le contexte Routing, entrez le chemin du contexte comme suit :

   ```
   netsh>routing ip
   ```

   Le contexte routing ip devient actif et l'invite de commandes affiche :

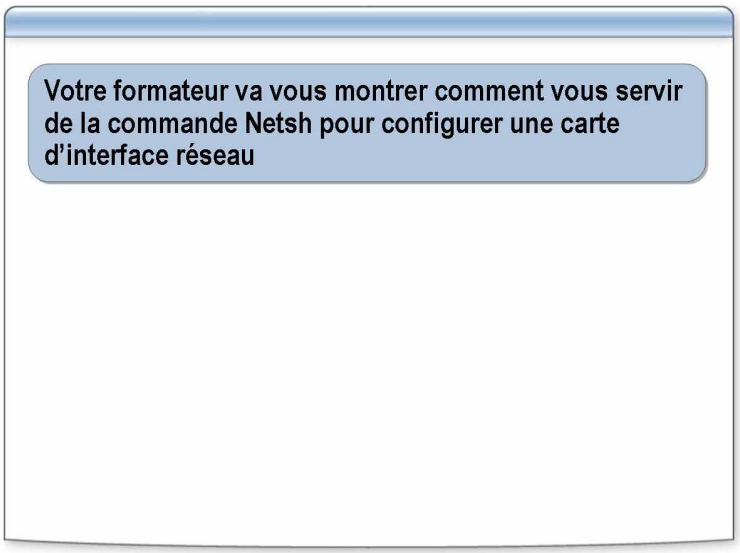
   ```
   netsh routing ip>
   ```

3. Entrez une commande disponible dans le contexte actuel (par exemple, la commande **set interface**, qui définit le mode de l'interface IP spécifiée) :

```
netsh routing ip>set interface name="Connexion au réseau
local" state=enable
```

4. Pour remonter dans la hiérarchie, tapez **..** (deux points), puis appuyez sur ENTRÉE.

Comment utiliser la commande Netsh pour configurer une carte d'interface réseau ?



**********DOCUMENT À L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

La commande Netsh vous permet de changer une adresse IP statique en une adresse IP dynamique sur une carte d'interface réseau.

Utilisation de Netsh pour configurer une carte d'interface réseau avec une IP statique

Pour que la carte d'interface réseau utilise une adresse IP statique

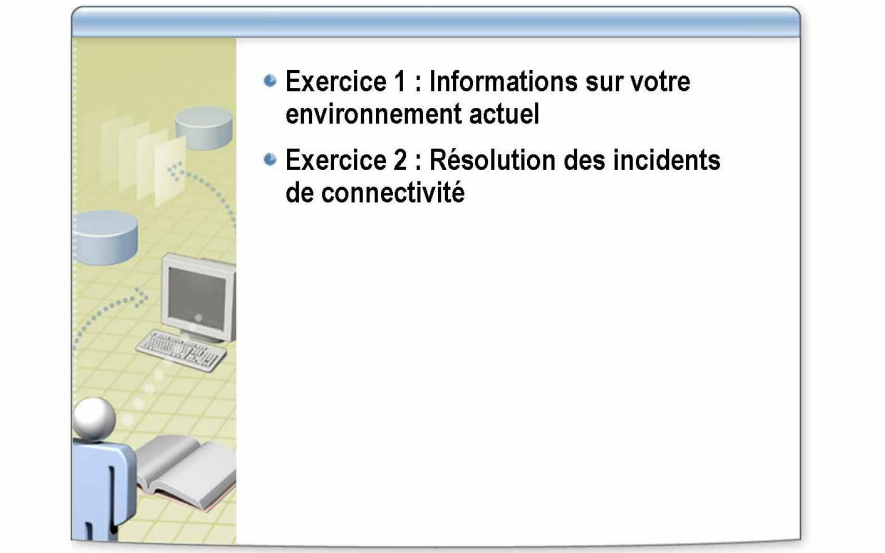
1. Ouvrez une invite de commandes.
2. Vérifiez que vous utilisez le protocole DHCP sur votre ordinateur en tapant **ipconfig /all**, puis appuyez sur ENTRÉE. Le message DHCP activé=Oui apparaît.
3. À l'invite, tapez la commande **netsh interface ip set address name="***nom_interface***" source=static addr=192.168.***x.y* **mask=255.255.255.0** (dans laquelle *nom_interface* représente le nom de la connexion au réseau local, *x* représente le numéro du réseau et *y* le numéro du stagiaire fourni par le formateur), puis appuyez sur ENTRÉE.

Utilisation de Netsh pour configurer une carte d'interface réseau avec une IP dynamique

Pour que la carte d'interface réseau utilise une adresse IP dynamique

1. Ouvrez une invite de commandes.
2. Vérifiez que vous utilisez une adresse IP statique sur votre ordinateur en tapant **ipconfig /all**, puis appuyez sur ENTRÉE. Le message DHCP activé=Non apparaît.
3. À l'invite, tapez la commande **netsh interface ip set address name="***nom_interface***" source=dhcp** et appuyez sur ENTRÉE.
4. Vérifiez que votre interface réseau est configurée de manière à obtenir automatiquement une adresse IP en tapant **ipconfig /all** et en appuyant sur ENTRÉE. Le message DHCP activé=Oui apparaît.

Atelier A : Identification des incidents courants de connectivité



**********DOCUMENT À L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Objectifs

À la fin de cet atelier, vous saurez utiliser le Diagramme d'identification d'incidents afin d'identifier les incidents de connectivité couramment rencontrés.

Connaissances préalables

Pour effectuer cet atelier, vous devez posséder des connaissances préalables en matière de configuration TCP/IP sur un ordinateur client fonctionnant sous Windows.

Scénario

Cet atelier propose quatre scénarios qui renferment chacun un incident de connectivité que vous devrez résoudre. Vous vous servirez du Diagramme d'identification d'incidents pour identifier les incidents de connectivité sur le client. Pour chaque scénario, vous exécuterez un fichier de commandes qui introduit un incident dans le système. Vous devrez ensuite réaliser une série d'étapes visant à isoler le problème et à le résoudre.

Remarque Pour afficher le Diagramme d'identification d'incidents, consultez l'annexe C.

Réponses de l'atelier

La procédure détaillée, ainsi que les réponses aux questions, se trouvent à la fin de l'atelier.

Durée approximative de cet atelier : 60 minutes

Exercice 0
Mise en place de l'atelier

Pour réaliser pleinement cet atelier, vous devez ajouter deux variables d'environnement à votre ordinateur et renommer l'icône de la carte réseau en connexions réseau. Les variables d'environnement sont utilisées dans les fichiers de commandes pour créer et supprimer les scénarios. Par exemple, pour réinitialiser votre adresse IP, un fichier de commandes comportant votre adresse IP comme commande est exécuté. Les variables d'environnement fournissent l'ID réseau et l'ID hôte pour le fichier de commandes.

Tâches	Procédure détaillée
1. Définir des variables d'environnement.	**a.** Ouvrez une session en tant qu'**Administrateur** avec le mot de passe **P@ssw0rd**. **b.** Cliquez sur **Démarrer**, pointez sur **Panneau de configuration**, puis cliquez sur **Système**. **c.** Cliquez sur l'onglet **Avancé**, puis sur le bouton **Variables d'environnement**. **d.** Dans la zone **Variables système**, cliquez sur **Nouveau**. **e.** Dans le champ **Nom de la variable,** tapez **mochost**, puis dans le champ **Valeur de la variable**, tapez le numéro de votre adresse hôte conformément au tableau ci-après. **f.** Cliquez sur **OK**. **g.** Répétez les étapes d à f, en utilisant **mocnet** comme nom de variable et le numéro de réseau *x* (où *x* représente le numéro de la classe) comme valeur de la variable.
Remarque les variables d'environnement sont des nombres entiers uniques et non des adresses IP. La variable d'environnement mochost est un nombre entier compris entre 11 et 34 (voir tableau ci-après). La variable mocnet est aussi un nombre entier unique qui correspond au numéro de la classe, par exemple 5.	
1. (*suite*)	**h.** Pour fermer la boîte de dialogue **Variables d'environnement**, cliquez sur **OK**. **i.** Pour fermer la boîte de dialogue **Propriétés système**, cliquez sur **OK**.
2. Nommer votre connexion par réseau local MOCLAN.	**a.** Cliquez sur **Démarrer**, pointez sur **Panneau de configuration**, cliquez avec le bouton droit sur **Connexions réseau**, puis cliquez sur **Ouvrir**. **b.** Cliquez avec le bouton droit sur votre connexion réseau principale, puis cliquez sur **Renommer**. **c.** Tapez **MOCLAN** et appuyez sur ENTRÉE.

(suite)

Tâches	Procédure détaillée
3. Activer DHCP.	**a.** Cliquez sur **Démarrer**, pointez sur **Panneau de configuration** et **Connexions réseau**, puis cliquez sur **MOCLAN**. La boîte de dialogue **État de MOCLAN** apparaît. **b.** Cliquez sur **Propriétés**. La boîte de dialogue **Propriétés de MOCLAN** apparaît. **c.** Activez la case à cocher **Protocole Internet (TCP/IP)**, puis cliquez sur **Propriétés**. La boîte de dialogue **Propriétés de Protocole Internet (TCP/IP)** s'affiche. **d.** Cliquez sur **Obtenir une adresse IP automatiquement**. **e.** Cliquez sur **Obtenir les adresses des serveurs DNS automatiquement**, puis sur **OK**. **f.** Pour fermer la boîte de dialogue **Propriétés de MOCLAN**, cliquez sur **OK**. **g.** Pour fermer la boîte de dialogue **État de MOCLAN**, cliquez sur **Fermer**.
4. Fermer toutes les fenêtres.	▪ Fermez toutes les fenêtres et fermez la session.
5. Ouvrir une session avec le compte *Ordinateur*User.	▪ Ouvrez une session en tant que **NWTRADERS***Ordinateur***User** (où *Ordinateur* est le nom de votre poste).

Nom de l'ordinateur	Valeur MOCHOST
Vancouver	11
Denver	12
Perth	13
Brisbane	14
Lisbon	15
Bonn	16
Lima	17
Santiago	18
Bangalore	19
Singapore	20
Casablanca	21
Tunis	22
Acapulco	23
Miami	24
Auckland	25

(suite)

Nom de l'ordinateur	Valeur MOCHOST
Suva	26
Stockholm	27
Moscow	28
Caracas	29
Montevideo	30
Manila	31
Tokyo	32
Khartoum	33
Nairobi	34

Exercice 1
Informations sur votre environnement actuel

Lors de l'exécution des scripts servant à introduire les scénarios, il se peut que les paramètres de configuration de votre ordinateur soient modifiés. À la fin de chaque scénario, vous devrez donc les réinitialiser. Notez les paramètres de configuration dans le tableau ci-dessous, puis consultez-les pour vérifier s'ils sont corrects après la réinitialisation de l'ordinateur.

Élément	Configuration
Votre numéro de réseau	
L'adresse IP de votre ordinateur	
Votre passerelle par défaut	
Votre serveur DNS principal	
Votre serveur DNS secondaire	
Votre serveur WINS	
Le type de nœud NetBT de votre ordinateur	
L'adresse distante (adresse en dehors de votre réseau local)	

Exercice 2
Résolution des incidents de connectivité

Cet atelier propose quatre scénarios qui renferment chacun un incident de connectivité que vous devrez résoudre. Vous vous servirez du Diagramme d'identification d'incidents, joint en annexe C, pour identifier les incidents de connectivité sur le client. Pour chaque scénario, vous exécuterez un fichier de commandes qui introduit un incident dans le système. Vous devrez ensuite réaliser une série d'étapes visant à isoler le problème et à le résoudre.

Scénario 1 : Résolution d'un incident de connectivité lié à un dépassement de délai

Un utilisateur fait parvenir une requête au support technique car il ne peut accéder à aucune ressource du réseau. Il reçoit à chaque fois le message « Délai d'attente de la demande dépassé ». Vous travaillez sur le poste de cet utilisateur pour identifier l'incident de connectivité, le résoudre par vous-même ou le transmettre à un ingénieur système plus qualifié.

Tâches	Instructions spécifiques
1. Présenter le problème.	▪ À l'aide de l'identité administrateur, exécutez **C:\MOC\2177\Labfiles\s1.bat**.
2. Identifier l'incident.	**a.** Utilisez la commande **Ping** pour envoyer une demande d'écho à localhost. **b.** Exécutez la commande **Ping** sur London. **c.** Vérifiez votre propre configuration IP.
? Après avoir exécuté la commande **Ping** sur localhost, la pile TCP/IP fonctionnait-elle normalement ?	
? Après avoir exécuté la commande **Ping** sur London, avez-vous reçu une réponse positive ?	
? Lorsque vous avez vérifié votre configuration IP, était-elle correcte ? Si tel n'était pas le cas, quel était le problème ?	
3. Corriger le problème.	▪ Accédez à **Connexions réseau** depuis le Panneau de configuration, utilisez **MOCLAN** et corrigez le problème.
4. Réinitialiser la configuration de l'ordinateur.	▪ À l'aide de l'identité administrateur, exécutez **C:\MOC\2177\Labfiles\r1.bat**.

Scénario 2 : L'utilisateur ne peut accéder à aucune ressource réseau

Un utilisateur se plaint de n'avoir accès à aucune ressource réseau. Il indique qu'une boîte de dialogue concernant la duplication d'une adresse IP sur le réseau s'est affichée.

Tâches	Instructions spécifiques
1. Présenter le problème.	▪ À l'aide de l'identité administrateur, exécutez **C:\MOC\2177\Labfiles\s2.bat**.
2. Identifier les problèmes associés au scénario.	**a.** Consultez les informations concernant la configuration IP en utilisant la commande **ipconfig /all**. **b.** Déterminez si DHCP est activé. **c.** Assurez-vous que le cache ARP contient une carte d'interface réseau. **d.** Identifiez l'incident.
? La carte est-elle configurée pour fonctionner avec DHCP ?	
? Quelles sont les valeurs de l'adresse IP et du masque de sous-réseau ?	
? Lorsque vous analysez ARP, quelle est la réponse ?	
? Quel est le problème ?	
3. Corriger le problème.	▪ Corrigez le problème à l'aide de **MOCLAN**.
4. Réinitialiser la configuration de l'ordinateur.	▪ À l'aide de l'identité administrateur, exécutez **C:\MOC\2177\Labfiles\r2.bat**.

Scénario 3 : Accès partiel aux ressources réseau

Une utilisatrice située dans un bureau distant ne dispose que d'un accès limité au réseau. En effet, elle peut accéder aux fichiers d'un dossier partagé de l'un de ses collaborateurs mais ne peut pas accéder à l'ordinateur London. Vous travaillez sur le poste de cette utilisatrice pour identifier l'incident de connectivité, le résoudre par vous-même ou le transmettre à un ingénieur système plus qualifié. Dans ce scénario, vous êtes chargé de rétablir la connectivité à l'ordinateur London.

Tâches	Instructions spécifiques
1. Présenter le problème.	▪ À l'aide de l'identité administrateur, exécutez **C:\MOC\2177\Labfiles\s3.bat**.
2. Identifier les problèmes associés au scénario.	**a.** Exécutez la commande **Ping** sur localhost. **b.** Exécutez la commande **Ping** sur London. **c.** Lancez Nslookup pour interroger l'ordinateur London.
? Pouvez-vous exécuter la commande **Ping** sur localhost ? Avez-vous reçu une réponse ?	
? Pouvez-vous exécuter la commande **Ping** sur London ? Quelle a été la réponse ? Quelle est l'adresse de London ?	
? La recherche **nslookup** lancée sur l'ordinateur London a-t-elle été fructueuse ?	
? Selon vous, de quel type de problème peut-il s'agir ?	
3. Corriger le problème.	
4. Réinitialiser la configuration de l'ordinateur.	▪ À l'aide de l'identité administrateur, exécutez **C:\MOC\2177\Labfiles\r3.bat**.

Scénario 4 : Impossible d'accéder à l'hôte via l'adresse IP

Un utilisateur situé dans le bureau local rencontre des difficultés pour accéder à l'ordinateur London. Il ne peut pas imprimer sur l'imprimante connectée à l'ordinateur London et ne peut pas accéder aux fichiers enregistrés dans les dossiers partagés de l'ordinateur London. Dans ce scénario, vous êtes chargé de rétablir la connectivité à l'ordinateur London.

Tâches	Instructions spécifiques
1. Présenter le problème.	▪ À l'aide de l'identité administrateur, exécutez **C:\MOC\2177\Labfiles\s4.bat**.
2. Identifier les problèmes associés au scénario.	**a.** Exécutez la commande **Ping** sur localhost. **b.** Exécutez la commande **Ping** sur London. **c.** Exécutez la commande **Ping** sur 192.168.*x*.200.
Pouvez-vous exécuter la commande **Ping** sur localhost ? Le protocole TCP/IP fonctionne-t-il correctement ?	
Pouvez-vous exécuter la commande **Ping** sur London ? Indiquez le résultat.	
Pouvez-vous exécuter la commande **Ping** sur 192.168.*x*.200 ? Quelle est la réponse ?	
Indiquez le problème.	
3. Corriger le problème.	
4. Réinitialiser la configuration de l'ordinateur.	▪ À l'aide de l'identité administrateur, exécutez **C:\MOC\2177\Labfiles\r4.bat**.