Exemple de configuration d'un commutateur Catalyst de couche 3 pour la prise en charge de Wake-On-LAN sur des réseaux VLAN

Contenu

Introduction

Ce document fournit un exemple de configuration pour la prise en charge de Wake-On-LAN (WOL) sur des VLAN avec un commutateur Catalyst de couche 3.

Conditions préalables

Conditions requises

Cisco recommande de posséder des connaissances sur les sujets suivants avant de tenter cette configuration :

- **Création de réseaux VLAN Ethernet sur des commutateurs Catalyst**
- Présentation du protocole VTP (VLAN Trunk Protocol)
- Comment configurer le routage entre réseaux locaux virtuels (InterVLAN) sur les commutateurs de couche 3
- >Utilisation de PortFast et d'autres commandes pour remédier aux délais de connectivité lors

du démarrage de la station de travail
- Présentation et dépannage du protocole DHCP dans les commutateurs Catalyst ou les réseaux d'entreprise

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Commutateur de la gamme Catalyst 3750 qui exécute le logiciel du système Cisco IOS® Version 12.2(25r)SEC
- Commutateurs de la gamme Catalyst 2950 qui exécutent le logiciel du système Cisco IOS Version 12.1(19)EA1a
- PC qui exécutent le système d'exploitation Microsoft Windows 2000
- Utilitaire gratuit Wake-On-LAN de SolarWinds**Remarque:** Cisco ne recommande aucun utilitaire Wake-On-LAN.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

Wake-On-LAN

Wake-On-LAN (WOL) est une combinaison de technologies matérielles et logicielles pour faire sortir de veille des systèmes en état de veille. WOL envoie les paquets réseau spécialement codés, appelés « paquets magiques », aux systèmes équipés et activés pour répondre à ces paquets. Cette fonctionnalité supplémentaire permet aux administrateurs d'effectuer la maintenance sur les systèmes même si l'utilisateur les a mis hors tension. La fonctionnalité WOL permet à l'administrateur de mettre sous tension à distance toutes les machines en veille afin qu'elles puissent recevoir des mises à jour. WOL est basé sur le principe suivant lequel, quand le PC s'arrête, la carte NIC est toujours alimentée et continue à écouter, sur le réseau, l'arrivée du paquet magique. Ce paquet magique peut être envoyé sur un grand nombre de protocoles sans connexion (UDP, IPX), mais UDP est le plus couramment utilisé.

Si vous envoyez des paquets WOL à partir de réseaux distants, les routeurs doivent être configurés pour autoriser les diffusions dirigées. Cela doit être fait pour les deux raisons suivantes :

- Étant donné que le PC est en veille, il n'aura pas d'adresse IP et ne répondra pas aux protocoles de résolution d'adresse (ARP) en provenance du routeur. Par conséquent, seul un paquet de diffusion IP de sous-réseau local est transmis sur le segment sans ARP.
- S'il y a un commutateur de couche 2 entre le routeur et le PC, ce qui est vrai pour la plupart

des réseaux aujourd'hui, le commutateur ne sait pas à quel port le PC est physiquement connecté. Seule une diffusion de couche 2 diffusée ou une trame de monodiffusion inconnue est envoyée à tous les ports de commutateur. Tous les paquets de diffusion IP sont adressés à l'adresse MAC de diffusion.

Obstacle - Diffusions dirigées

Les diffusions dirigées par IP sont utilisées dans l'attaque de déni de service par rebond (« smurf ») courante et classique, et peuvent également être utilisées dans des attaques associées.

Une diffusion dirigée par IP est un datagramme qui est envoyé à l'adresse de diffusion d'un sous-réseau auquel l'ordinateur expéditeur n'est pas directement attaché. La diffusion dirigée est routée à travers le réseau sous la forme d'un paquet de monodiffusion jusqu'à ce qu'elle arrive au sous-réseau cible, où elle est convertie en diffusion de couche de liaison. En raison de la nature de l'architecture d'adressage IP, seul le dernier routeur dans la chaîne, celui qui est connecté directement au sous-réseau cible, peut, de façon certaine, identifier une diffusion dirigée. Les diffusions dirigées sont parfois utilisées pour des raisons légitimes, mais une telle utilisation n'est pas courante en dehors du secteur des services financiers.

Dans une attaque par rebond (« smurf »), l'attaquant envoie des demandes d'écho ICMP à partir d'une adresse source falsifiée à une adresse de diffusion dirigée. Cela entraîne l'envoi, par tous les hôtes sur le sous-réseau cible, de réponses à la source falsifiée. En envoyant un flux continu de telles demandes, l'attaquant peut créer un flux de réponses beaucoup plus important. Cela peut complètement inonder l'hôte, dont l'adresse est falsifiée.

Si une interface Cisco est configurée avec la commande no ip directed-broadcast, les diffusions dirigées sont supprimées au lieu d'être éclatées dans des diffusions de couche de liaison sur cette interface. Cela signifie que la commande **no ip directed-broadcast** doit être configurée sur chaque interface de chaque routeur qui est connecté à un sous-réseau cible. Effectuer la configuration uniquement sur les routeurs de pare-feu ne suffit pas. La commande **no ip directed-broadcast** est la configuration par défaut dans le logiciel Cisco IOS Version 12.0 et ultérieures. Dans les versions antérieures, la commande devrait être appliquée à chaque interface LAN qui n'est pas connue pour transférer des diffusions dirigées légitimes.

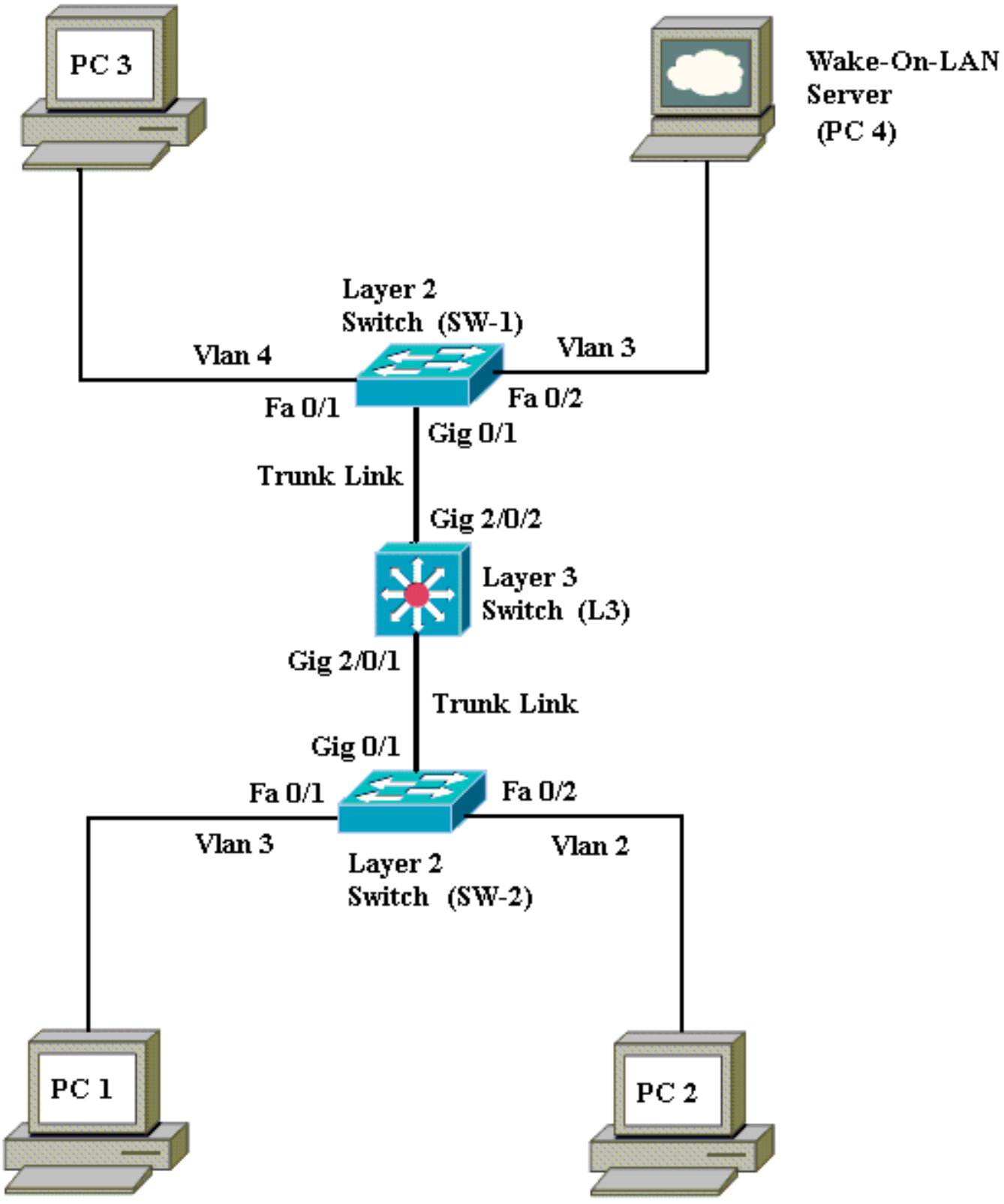
Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Voici les détails de cette configuration réseau :

- Les PC 1, 2 et 3 sont les PC clients qui doivent être sortis de veille.
- PC 4 est le serveur WOL ainsi que le serveur DHCP.
- PC 4 est configuré avec l'adresse IP statique 172.16.3.2/24.
- Les PC clients sont configurés pour obtenir l'adresse IP d'un serveur DHCP.
- Le serveur DHCP (PC 4) est configuré avec trois portées IP pour les clients qui se connectent aux VLAN 2, 3 et 4.

- SW-1 et SW-2 (Catalyst 2950) sont utilisés comme commutateurs de couche 2 et L3 (Catalyst 3750) est utilisé comme commutateur de couche 3.
- Les PC 1 et 4 sont connectés dans le même VLAN (VLAN 3).
- Les PC 2 et 3 sont connectés dans le VLAN 2 et le VLAN 4, respectivement.

Configurations de commutateurs

Ce document utilise les configurations de commutateurs suivantes :

- Commutateur de couche 3 - L3
- Commutateurs de couche 2 - SW-1 et SW-2

L3

```
Switch>en
Switch#configure terminal
Enter configuration commands, one per line.  End with
CNTL/Z.
Switch(config)#hostname L3
L3(config)#ip routing
L3(config)#vtp mode server
Device mode already VTP SERVER.
L3(config)#vtp domain cisco
Changing VTP domain name from NULL to cisco
L3(config)#vlan 2
L3(config-vlan)#vlan 3
L3(config-vlan)#vlan 4
L3(config)#interface gigabitEthernet 2/0/1
L3(config-if)#switchport trunk encapsulation dot1q
L3(config-if)#switchport mode trunk
L3(config-if)#interface gigabitEthernet 2/0/2
L3(config-if)#switchport trunk encapsulation dot1q
L3(config-if)#switchport mode trunk
L3(config-if)#exit
L3(config)#access-list 101 permit udp host 172.16.3.2
any eq 7
!--- This accepts directed broadcasts only from PC 4.
L3(config)#ip forward-protocol udp 7
!--- Specifies the protocol and port to be forwarded. !-
-- Capture the WOL packet with any network sniffer to
determine the UDP port !--- to use in this command. The
port number varies with the WOL utility used. L3(config-
if)#interface vlan 2
L3(config-if)#ip address 172.16.2.1 255.255.255.0
L3(config-if)#ip helper-address 172.16.3.2
!--- Enables BOOTP broadcast forwarding to the DHCP
server. L3(config-if)#ip directed-broadcast 101
!--- Enables the translation of a directed broadcast to
physical broadcasts. L3(config-if)#interface vlan 3
L3(config-if)#ip address 172.16.3.1 255.255.255.0
L3(config-if)#ip helper-address 172.16.2.255
L3(config-if)#ip helper-address 172.16.4.255
!-- Enables forwarding of WoL packets to clients. !--
Works in conjunction with the ip forward-protocol
command.
L3(config-if)#interface vlan 4
L3(config-if)#ip address 172.16.4.1 255.255.255.0
L3(config-if)#ip helper-address 172.16.3.2
!--- Enables BOOTP broadcast forwarding to the DHCP
server. L3(config-if)#ip directed-broadcast 101
```

```
!--- Enables the translation of a directed broadcast to
physical broadcasts. L3(config)#^Z
L3#wr
Building configuration...
[OK]
L3#
```

SW-1

```
Switch>en
Switch#configure terminal
Enter configuration commands, one per line.  End with
CNTL/Z.
Switch(config)#hostname SW-1
SW-1(config)#vtp mode client
Setting device to VTP CLIENT mode.
SW-1(config)#vtp domain cisco
Changing VTP domain name from NULL to cisco
SW-1(config)#interface fastEthernet 0/1
SW-1(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports
connected to a single
 host. Connecting hubs, concentrators, switches,
bridges, etc... to this
 interface  when portfast is enabled, can cause
temporary bridging loops.
 Use with CAUTION

%Portfast has been configured on FastEthernet0/1 but
will only
 have effect when the interface is in a non-trunking
mode.
SW-1(config-if)#switchport mode access
SW-1(config-if)#switchport access vlan 4
SW-1(config-if)#interface fastEthernet 0/2
SW-1(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports
connected to a single
 host. Connecting hubs, concentrators, switches,
bridges, etc... to this
 interface  when portfast is enabled, can cause
temporary bridging loops.
 Use with CAUTION

%Portfast has been configured on FastEthernet0/2 but
will only
 have effect when the interface is in a non-trunking
mode.
SW-1(config-if)#switchport mode access
SW-1(config-if)#switchport access vlan 3
SW-1(config-if)#interface gigabitethernet 0/1
SW-1(config-if)#switchport mode trunk
SW-1(config-if)#^Z
SW-1#wr
Building configuration...
[OK]
SW-1#
```

SW-2

```
Switch>en
Switch#configure terminal
Enter configuration commands, one per line.  End with
CNTL/Z.
Switch(config)#hostname SW-2
SW-2(config)#vtp mode client
```

```
Setting device to VTP CLIENT mode.
SW-2(config)#vtp domain cisco
Changing VTP domain name from NULL to cisco
SW-2(config)#interface fastEthernet 0/1
SW-2(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports
connected to a single
 host. Connecting hubs, concentrators, switches,
bridges, etc... to this
 interface  when portfast is enabled, can cause
temporary bridging loops.
 Use with CAUTION

%Portfast has been configured on FastEthernet0/1 but
will only
 have effect when the interface is in a non-trunking
mode.
SW-2(config-if)#switchport mode access
SW-2(config-if)#switchport access vlan 3
SW-2(config-if)#interface fastEthernet 0/2
SW-2(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports
connected to a single
 host. Connecting hubs, concentrators, switches,
bridges, etc... to this
 interface  when portfast is enabled, can cause
temporary bridging loops.
 Use with CAUTION

%Portfast has been configured on FastEthernet0/2 but
will only
 have effect when the interface is in a non-trunking
mode.
SW-2(config-if)#switchport mode access
SW-2(config-if)#switchport access vlan 2
SW-2(config)#interface gigabitethernet 0/1
SW-2(config-if)#switchport mode trunk
SW-2(config-if)#^Z
SW-2#wr
Building configuration...
[OK]
SW-2#
```

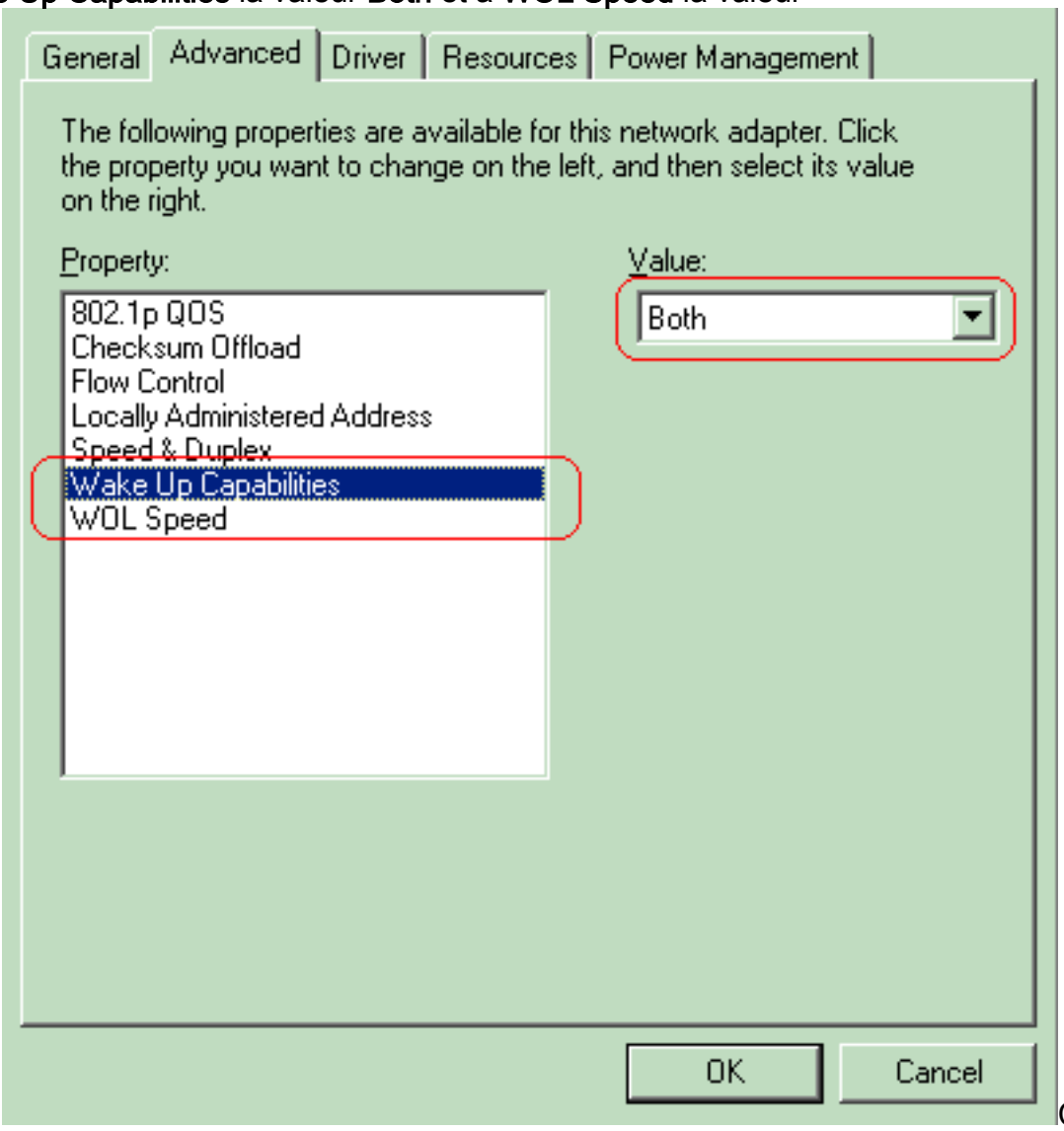
Configuration d'un PC client

Aujourd'hui, la plupart des cartes mères ont une carte NIC intégrée et prennent en charge la fonctionnalité WOL. WOL est désactivé par défaut sur certains ordinateurs. Vous devez accéder aux options du BIOS (Basic Input/Output System) pour activer WOL. Voici la procédure permettant d'activer WOL sur un PC client :

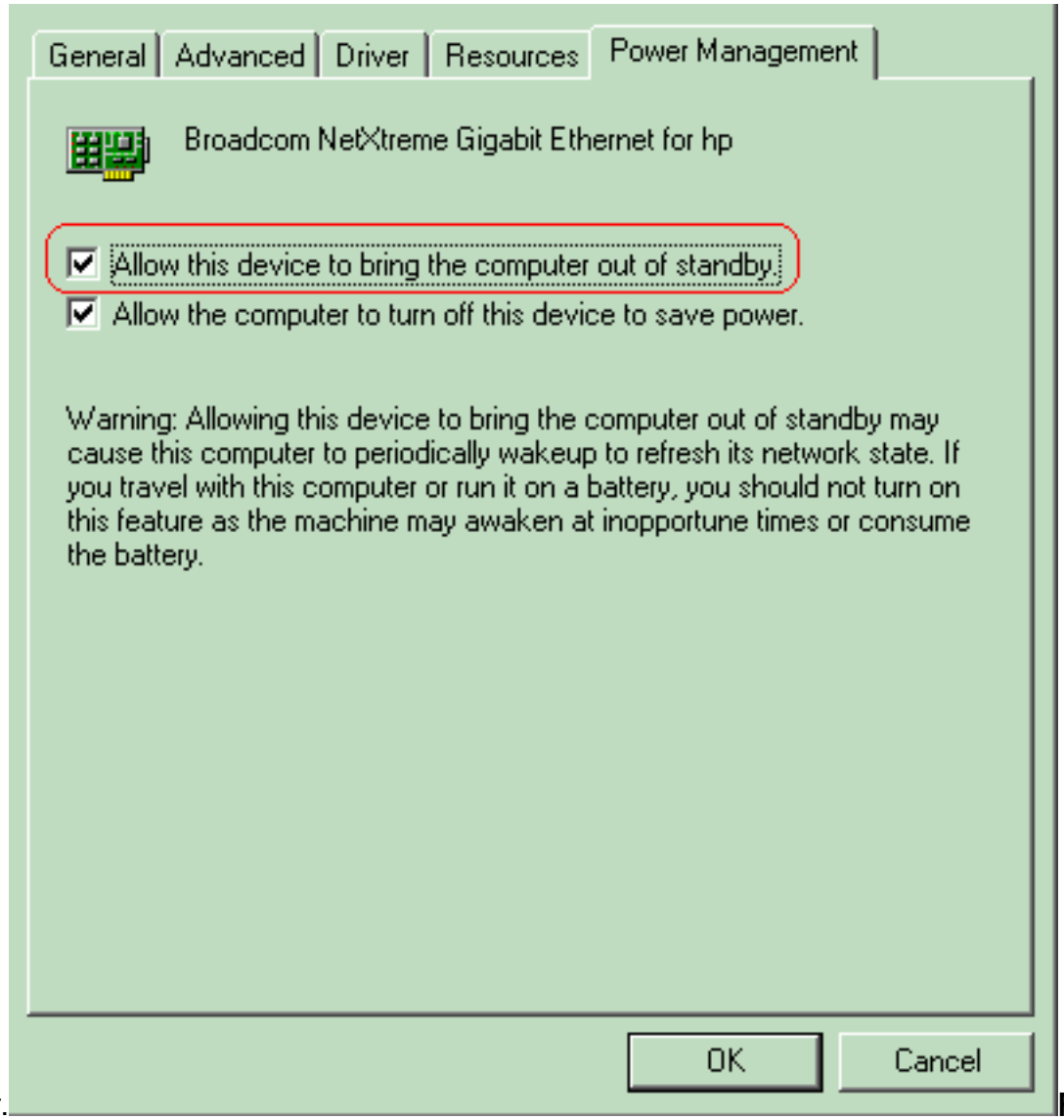
1. Entrez dans l'écran des paramètres du BIOS pendant l'autotest de mise sous tension (POST) de l'ordinateur.**Remarque:** Généralement, le fait d'appuyer sur **F10** ou sur la **touche Delete** permet d'entrer dans les paramètres du BIOS.
2. Dans l'écran du BIOS, accédez à **Advanced settings**, puis à **Device Options**.
3. Dans cet écran, recherchez le paramètre relatif à **Wake-On-LAN** et activez-le.
4. Enregistrez et quittez les paramètres du BIOS.**Remarque:** La procédure précise et les options disponibles dans le BIOS pour activer WOL sont différentes avec chaque constructeur d'ordinateurs. Consultez le manuel de la carte mère fournie avec chaque

ordinateur pour plus d'informations sur les paramètres du BIOS.

5. Vérifiez les propriétés avancées de votre carte réseau afin de vous assurer que la fonctionnalité WOL est activée.Choisissez **Start > Settings > Network and Dial-up Connections**, puis cliquez avec le bouton droit sur **Local Area Connection**.Cliquez sur **Properties** et choisissez **Configure**.Accédez à l'onglet **Advanced**. Affectez à la propriété **Wake Up Capabilities** la valeur **Both** et à **WOL Speed** la valeur



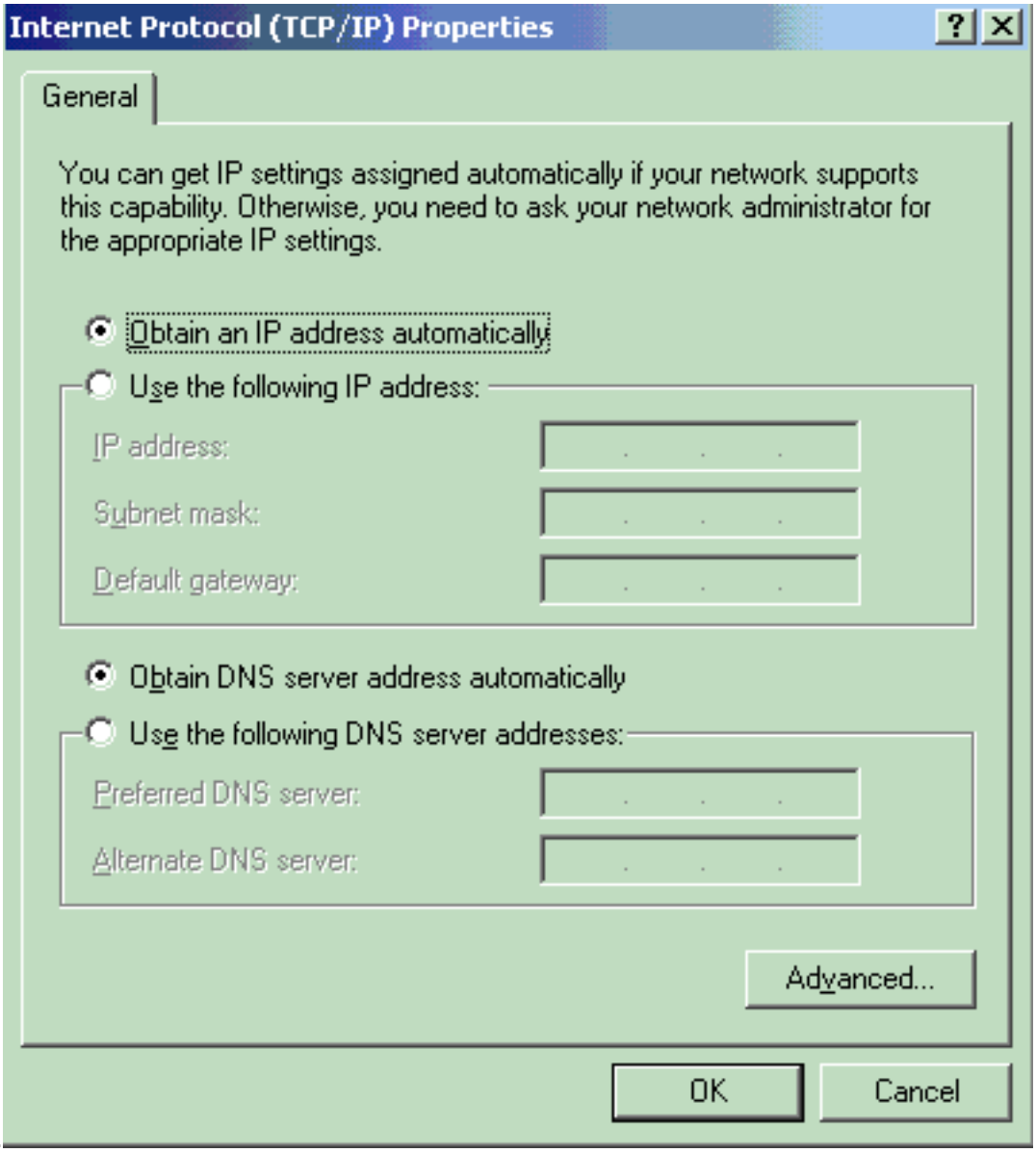
Auto.Cliquez sur l'onglet **Power Management** et activez la case qui indique **Allow this device to bring the computer out of**



standby.**Remarque:** Sur les ordinateurs Microsoft Windows XP, il y a une option supplémentaire : **N'autoriser que les stations de gestion à faire sortir l'ordinateur du mode veille**. Cette dernière option met l'ordinateur sous tension seulement si un paquet magique WOL est reçu. Si cette option n'est pas activée, tout trafic envoyé à l'adaptateur réseau met le PC sous tension.

Exécutez les étapes suivantes pour que le client obtienne une adresse IP à partir du serveur DHCP :

1. Choisissez **Start > Settings > Network and Dial-up Connections**, puis cliquez avec le bouton droit sur **Local Area Connection** et choisissez **Properties**.
2. Sous l'onglet **General**, cliquez sur **Internet Protocol (TCP/IP)**, puis sur **Properties**.
3. Choisissez **Obtain an IP address**

automatically. 

Configuration d'un PC serveur

Exécutez les étapes suivantes pour configurer le serveur WOL :

1. Téléchargez et installez l'utilitaire Wake-On-LAN.
2. Configurez le PC avec l'adresse IP statique 172.16.3.2/24.
3. Configurez le PC comme serveur DHCP.
4. Créez trois portées avec les détails suivants :Consultez Comment installer et configurer un serveur DHCP dans un groupe de travail dans Windows Server 2003 pour plus d'informations sur la configuration du serveur DHCP.

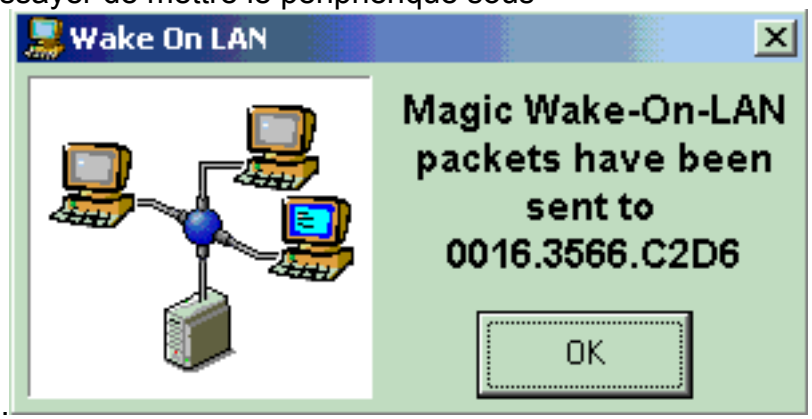
Vérifiez

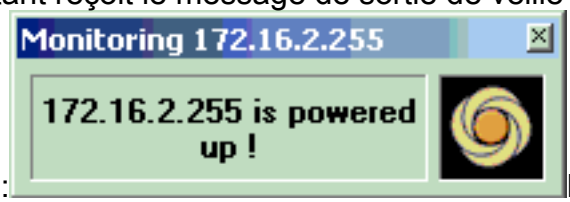
Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Procédez comme suit :

1. Mettez les PC sous tension et connectez-les aux commutateurs respectifs, comme indiqué dans le diagramme du réseau.

2. Connectez-vous à chaque PC et notez les adresses MAC et les adresses IP.**Remarque:** Ouvrez une invite de commandes et entrez la commande **ipconfig /all** afin de déterminer l'adresse MAC et l'adresse IP.
3. Utilisez un test Ping afin de vérifier la connectivité entre les PC.
4. Mettez hors tension tous les PC clients (PC 1, PC 2 et PC 3) après avoir vérifié que la connectivité est correcte.
5. Lancez l'utilitaire WOL sur le PC serveur (PC 4).
6. Entrez l'adresse MAC et l'adresse IP du PC que vous voulez sortir de veille, comme indiqué ici : 

Remarque: L'adresse IP peut être n'importe quelle adresse (même de diffusion de sous-réseau) dans cette plage de sous-réseau VLAN à laquelle le PC client est connecté. Seule l'adresse MAC du PC client doit correspondre.
7. Cliquez sur l'icône **Wake UP PC** afin d'envoyer une série de paquets magiques au PC cible afin d'essayer de mettre le périphérique sous tension. 

8. Quand le périphérique distant reçoit le message de sortie de veille et se met sous tension, le message suivant s'affiche : 

Le PC client est maintenant sous tension.

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Support pour les produits LAN
- Prise en charge de la technologie de commutation LAN
- Support et documentation techniques - Cisco Systems