# Konfigurationsbeispiel: Catalyst Layer-3-Switch für Wake-On-LAN-Unterstützung über VLANs hinweg

## Inhalt



## Einführung

Dieses Dokument enthält eine Beispielkonfiguration für die WOL-Unterstützung (Wake-On-LAN) in VLANs mit einem Catalyst Layer-3-Switch.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, vor dem Versuch dieser Konfiguration über Kenntnisse dieser Themen zu verfügen:

- Erstellen von Ethernet-VLANs auf Catalyst-Switches
- VLAN Trunk Protocol (VTP)
- Konfigurieren von Inter-VLAN-Routing auf Layer-3-Switches
- Verwenden von PortFast und anderen Befehlen zum Beheben von Verzögerungen bei der Workstation-Startverbindung

- Verständnis und Fehlerbehebung von DHCP in Catalyst Switch oder Enterprise Networks

## Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Catalyst Switch der Serie 3750 mit Cisco IOS® Systemsoftware-Version 12.2(25r)SEC
- Catalyst Switches der Serie 2950 mit Cisco IOS-Systemsoftware, Version 12.1(19)EA1a
- PCs mit Microsoft Windows 2000-Betriebssystem
- Freeware Wake-On-LAN-Utility von SolarWinds**Hinweis:** Cisco empfiehlt kein Wake-On-LAN-Dienstprogramm.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

## Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

# Hintergrundinformationen

## Wake-On-LAN

Wake-On-LAN (WOL) ist eine Kombination aus Hardware- und Softwaretechnologien zum Aufwachen schlafender Systeme. WOL sendet speziell codierte Netzwerkpakete, so genannte magische Pakete, an Systeme, die ausgestattet sind und in der Lage sind, auf diese Pakete zu reagieren. Diese zusätzliche Funktion ermöglicht Administratoren die Durchführung von Wartungsarbeiten an Systemen, selbst wenn der Benutzer diese heruntergefahren hat. Mit der WOL-Funktion können Administratoren alle schlafenden Systeme remote hochfahren, sodass sie Updates erhalten können. WOL basiert auf dem Prinzip, dass die Netzwerkkarte beim Herunterfahren des PCs immer noch mit Strom versorgt wird und im Netzwerk ständig wartet, bis das magische Paket eintrifft. Dieses Magic-Paket kann über verschiedene verbindungslose Protokolle (UDP, IPX) gesendet werden, aber UDP wird am häufigsten verwendet.

Wenn Sie WOL-Pakete von Remote-Netzwerken senden, müssen die Router so konfiguriert werden, dass gezielte Übertragungen zugelassen werden. Dies muss aus den folgenden beiden Gründen geschehen:

- Da der PC eingeschlafen ist, hat er keine IP-Adresse und reagiert nicht auf die Address Resolution Protocols (ARPs) des Routers. Daher wird nur ein lokales Subnetz-IP-Broadcast-Paket ohne ARP auf das Segment übertragen.
- Wenn zwischen dem Router und dem PC ein Layer-2-Switch vorhanden ist, was für die meisten heutigen Netzwerke gilt, weiß der Switch nicht, mit welchem Port der PC physisch verbunden ist. An alle Switch-Ports werden nur ein Layer-2-Broadcast oder ein unbekannter Unicast-Frame gesendet. Alle IP-Broadcast-Pakete werden an die Broadcast-MAC-Adresse adressiert.

## Caveat - Directed Broadcasts

IP-gesteuerte Broadcasts werden im häufig verwendeten und häufig verwendeten "smurf Denial of Service"-Angriff verwendet und können auch bei damit verbundenen Angriffen eingesetzt werden.

Eine IP-gerichtete Sendung ist ein Datagramm, das an die Broadcast-Adresse eines Subnetzes gesendet wird, an das der Sendercomputer nicht direkt angeschlossen ist. Der gezielte Broadcast wird als Unicast-Paket über das Netzwerk geroutet, bis er am Ziel-Subnetz ankommt, wo er in einen Link-Layer-Broadcast umgewandelt wird. Aufgrund der Beschaffenheit der IP-Adressierungsarchitektur kann nur der letzte Router in der Kette, der direkt mit dem Ziel-Subnetz verbunden ist, eine gezielte Übertragung eindeutig identifizieren. Direkte Sendungen werden gelegentlich für rechtmäßige Zwecke verwendet, doch diese Nutzung ist außerhalb der Finanzdienstleistungsbranche nicht üblich.

Bei einem SMURF-Angriff sendet der Angreifer ICMP-Echoanfragen von einer gefälschten Quelladresse an eine gezielte Broadcast-Adresse. Dadurch senden alle Hosts im Ziel-Subnetz Antworten an die gefälschte Quelle. Wenn der Angreifer einen kontinuierlichen Strom solcher Anfragen sendet, kann er einen wesentlich größeren Strom an Antworten erstellen. Dadurch kann der Host, dessen Adresse gefälscht ist, vollständig überschwemmt werden.

Wenn eine Cisco Schnittstelle mit dem **Befehl no** ip directed-broadcast konfiguriert ist**,** werden stattdessen gezielte Broadcasts verworfen, die ansonsten in Link-Layer-Broadcasts an dieser Schnittstelle explodiert sind. Das bedeutet, dass der Befehl **no ip directed-broadcast** auf jeder Schnittstelle jedes Routers konfiguriert werden muss, der mit einem Ziel-Subnetz verbunden ist. Es reicht nicht aus, nur Firewall-Router zu konfigurieren. Der Befehl **no ip directed-broadcast** ist der Standardwert in Cisco IOS Software Release 12.0 und höher. In früheren Versionen sollte der Befehl auf alle LAN-Schnittstellen angewendet werden, von denen nicht bekannt ist, dass sie legitime gezielte Broadcasts weiterleiten.

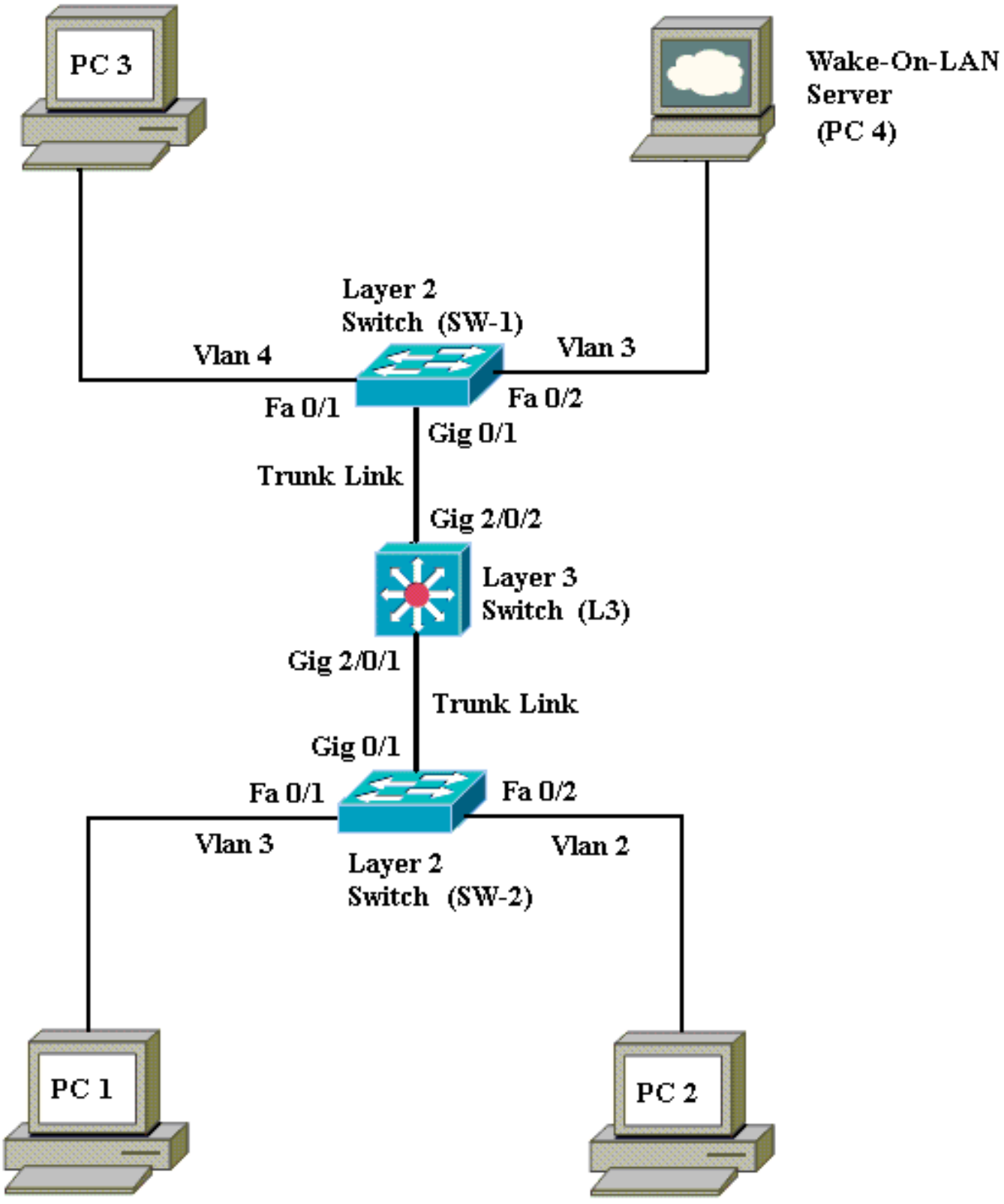
# Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

**Hinweis:** Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

## Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:




Diese Netzwerkeinrichtung umfasst folgende Details:

- PCs 1, 2 und 3 sind die Client-PCs, die aufgeweckt werden müssen.
- PC 4 ist der WOL-Server und der DHCP-Server.
- PC 4 ist mit der statischen IP-Adresse 172.16.3.2/24 konfiguriert.
- Client-PCs sind so konfiguriert, dass sie die IP-Adresse von einem DHCP-Server beziehen.
- Der DHCP-Server (PC 4) ist mit drei IP-Bereichen für Clients konfiguriert, die mit den VLANs 2, 3 und 4 verbunden sind.

- Als Layer-2-Switches werden SW-1 und SW-2 (Catalyst 2950) und L3 (Catalyst 3750) als Layer-3-Switch verwendet.
- PCs 1 und 4 sind im gleichen VLAN (VLAN 3) verbunden.
- Die PCs 2 und 3 sind jeweils in VLAN 2 bzw. 4 angeschlossen.

## Switch-Konfigurationen

In diesem Dokument werden folgende Switch-Konfigurationen verwendet:

- Layer-3-Switch - L3
- Layer-2-Switches - SW-1 und 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#
```

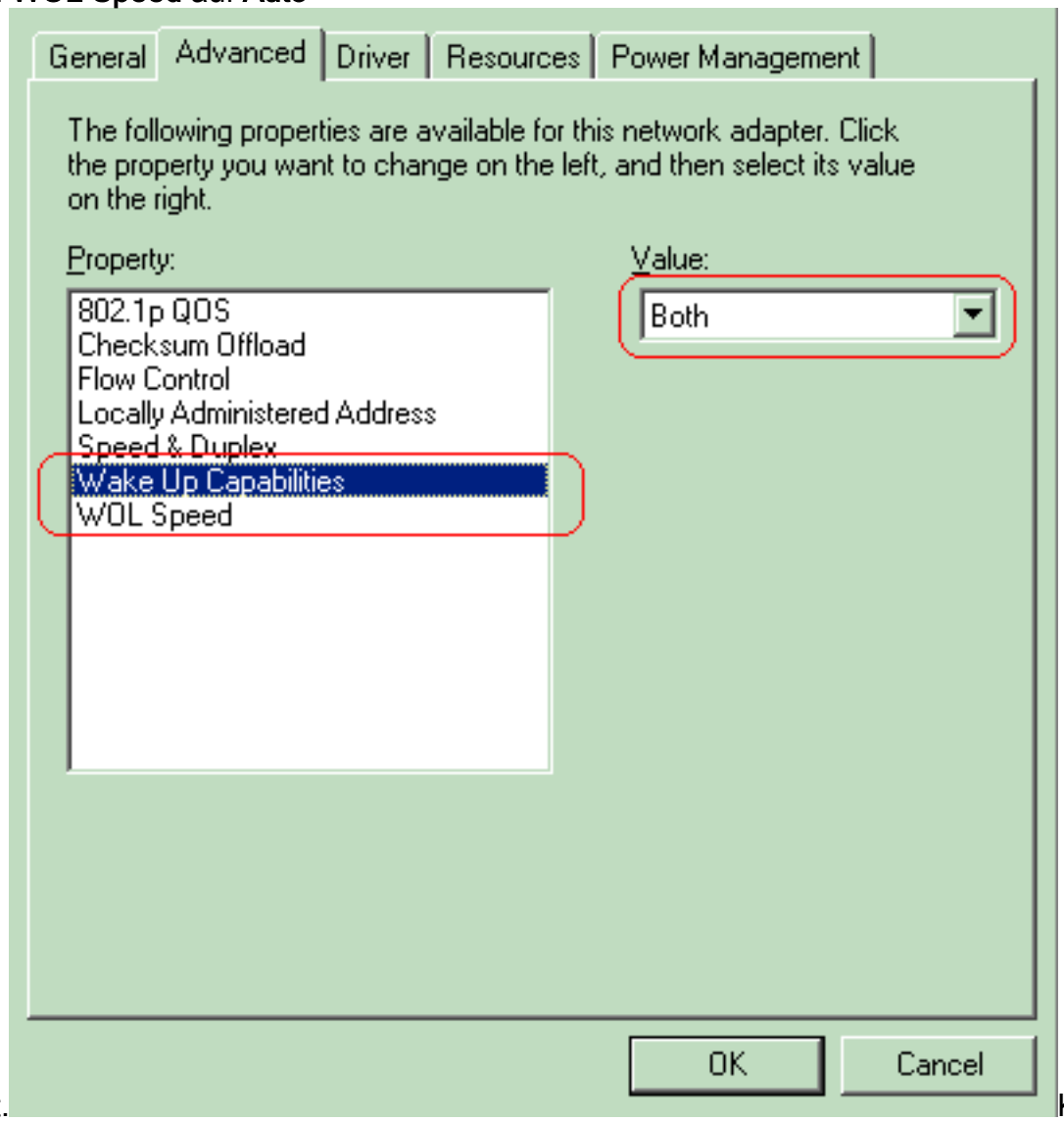
## Client-PC-Konfiguration

Die meisten Motherboards verfügen heute über eine integrierte Netzwerkkarte und unterstützen WOL-Funktionen. Auf einigen Computern ist WOL standardmäßig deaktiviert. Sie müssen die Optionen Basic Input Output System (BIOS) aufrufen, um WOL zu aktivieren. Dies ist die Vorgehensweise zum Aktivieren von WOL auf einem Client-PC:

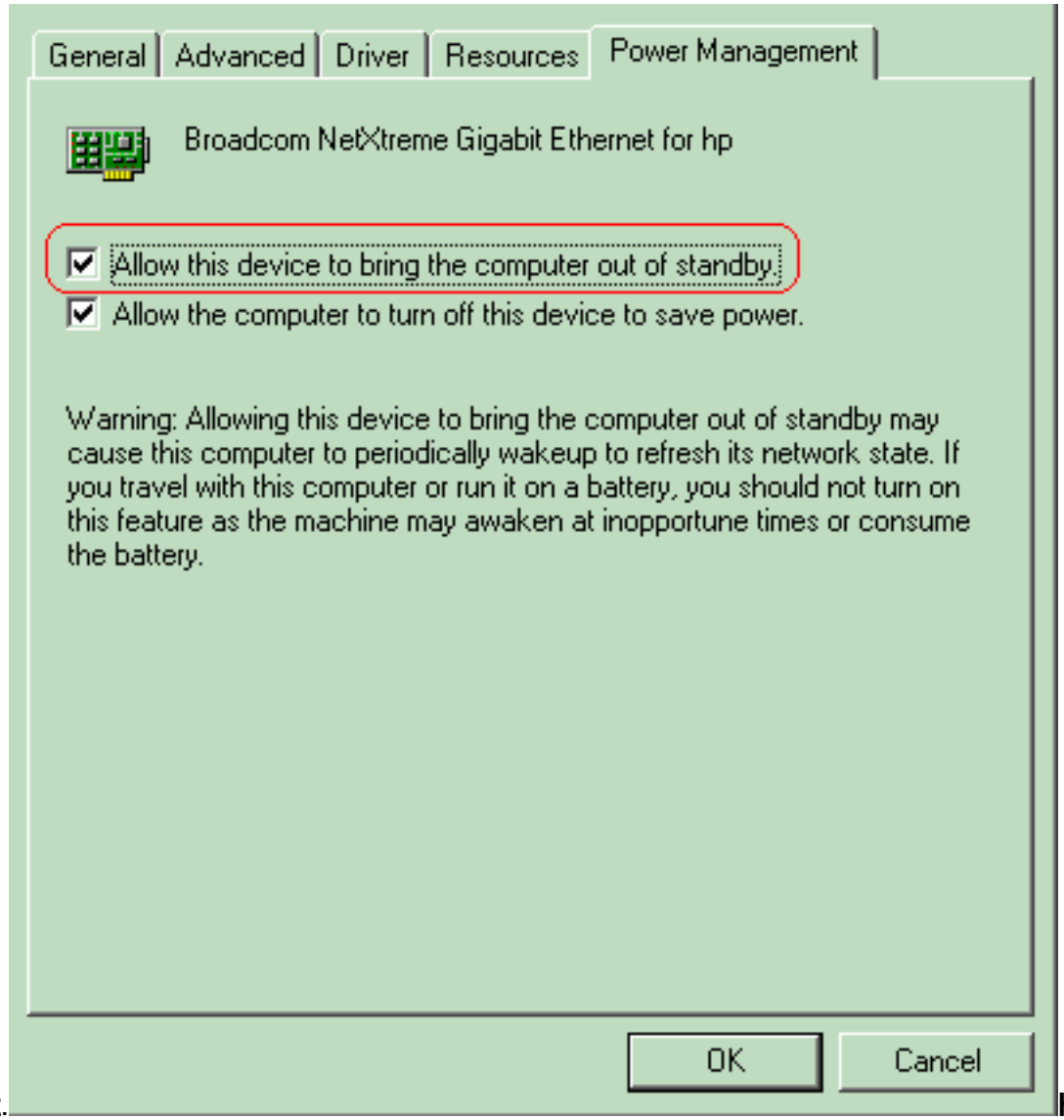
1. Rufen Sie den BIOS-Einstellungsbildschirm während des Einschalt-Selbsttests (POST) des Computers auf.**Hinweis:** Normalerweise wird die **F10**- oder **Delete-**Taste gedrückt, um die BIOS-Einstellungen aufzurufen.
2. Navigieren Sie im BIOS-Bildschirm zu **Erweiterte** Einstellungen und dann zu **Geräteoptionen**.
3. Suchen Sie in diesem Bildschirm nach Einstellungen für **Wake-On-LAN**, und aktivieren Sie

sie.

4. Speichern und beenden Sie die BIOS-Einstellungen.**Hinweis:** Die genauen Verfahren und Optionen, die im BIOS zur Aktivierung von WOL verfügbar sind, unterscheiden sich je nach Computerhersteller. Weitere Informationen zu den BIOS-Einstellungen finden Sie im Motherboard-Handbuch, das mit jedem Computer geliefert wurde.
5. Überprüfen Sie die erweiterten Eigenschaften Ihrer Netzwerkkarte, um sicherzustellen, dass die WOL-Funktion aktiviert ist.Wählen Sie **Start > Einstellungen > Netzwerk- und DFÜ-Verbindungen**, und klicken Sie dann mit der rechten Maustaste auf Ihre **LAN-Verbindung**.Klicken Sie auf **Eigenschaften** und wählen Sie **Konfigurieren**.Navigieren Sie zur Registerkarte **Erweitert**. Legen Sie die **Wake Up Capabilities-**Eigenschaft auf **Wake** Speed und **WOL Speed** auf **Auto**




fest.Klicken Sie auf die Registerkarte **Energiemanagement**, und aktivieren Sie das Kontrollkästchen **Zulassen, dass dieses Gerät den Computer aus dem Standby-Modus**

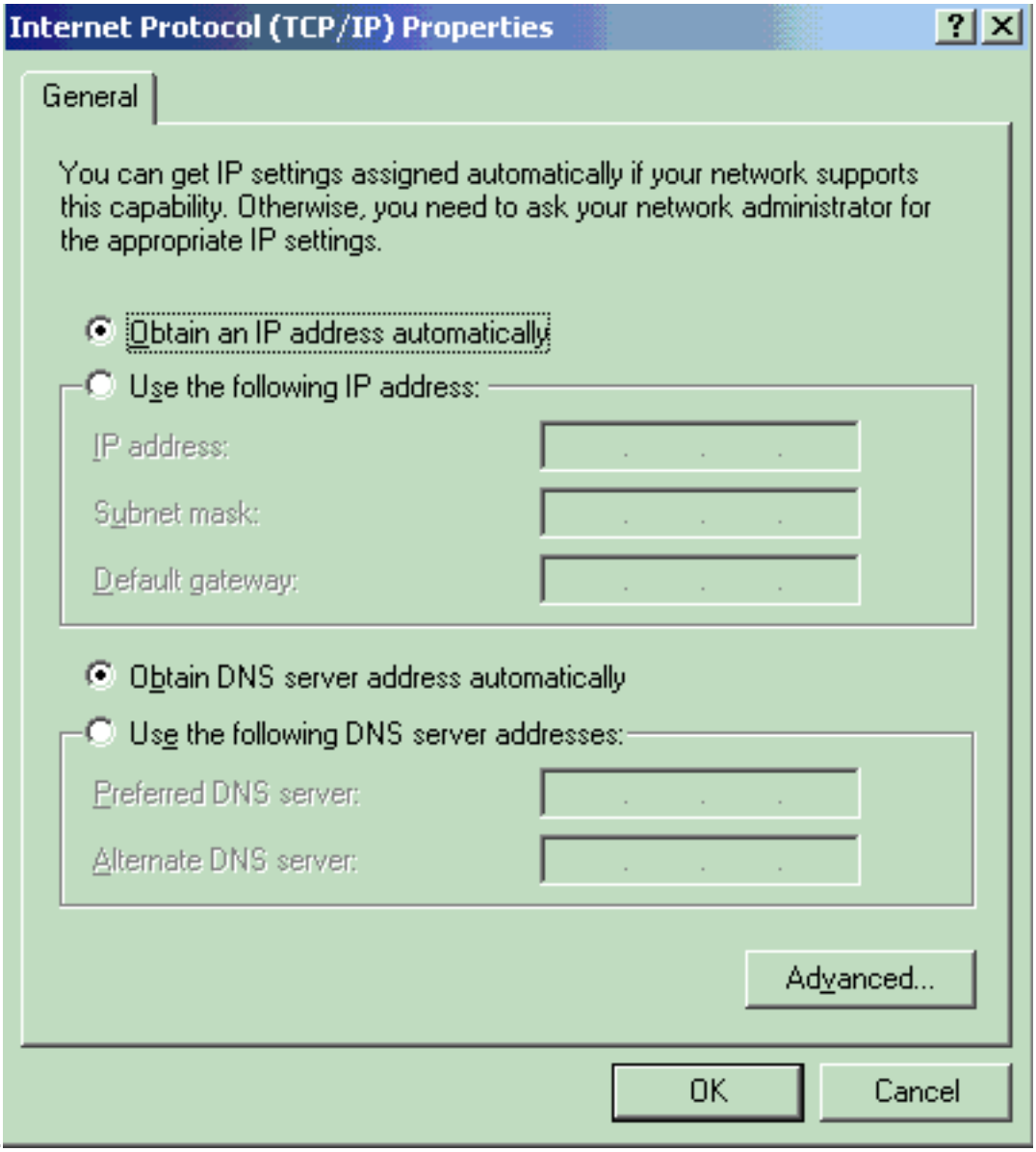



**bringt.** **Hinweis:** Auf Computern mit Microsoft Windows XP gibt es eine weitere Option: **Lassen Sie nur Managementkonsolen den Computer aus dem Standby-Modus holen**. Diese letzte Option aktiviert den Computer nur, wenn ein WOL-Magic-Paket empfangen wird. Wenn diese Option nicht aktiviert ist, schaltet der an den Netzwerkadapter gesendete Datenverkehr den PC ein.

Gehen Sie wie folgt vor, damit der Client vom DHCP-Server eine IP-Adresse erhält:

1. Wählen Sie **Start > Einstellungen > Netzwerk- und DFÜ-Verbindungen**, klicken Sie dann mit der rechten Maustaste auf Ihre **LAN-Verbindung** und wählen Sie **Eigenschaften aus**.
2. Klicken Sie auf der Registerkarte **Allgemein** auf **Internetprotokoll (TCP/IP)** und anschließend auf **Eigenschaften**.
3. Wählen Sie **IP-Adresse automatisch beziehen**

aus.




## Server-PC-Konfiguration

Gehen Sie wie folgt vor, um den WOL-Server zu konfigurieren:

1. Laden Sie das Dienstprogramm Wake-On-LAN herunter, und installieren Sie es.
2. Konfigurieren Sie für den PC die statische IP-Adresse 172.16.3.2/24.
3. Konfigurieren Sie den PC als DHCP-Server.
4. Erstellen Sie drei Bereiche mit den folgenden Details:Weitere Informationen zur DHCP-Serverkonfiguration finden Sie unter So installieren und konfigurieren Sie einen DHCP-Server in einer Arbeitsgruppe in Windows Server 2003 .

# Überprüfen

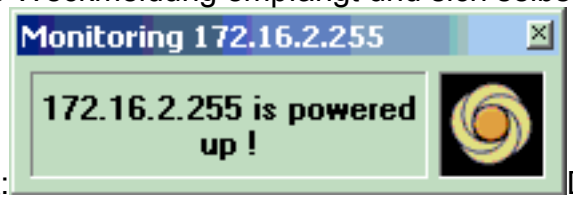
In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Gehen Sie wie folgt vor:

1. Schalten Sie die PCs ein, und schließen Sie sie an die entsprechenden Switches an, wie im Netzwerkdiagramm gezeigt.

2. Melden Sie sich bei jedem PC an, und notieren Sie sich die MAC-Adressen und IP-Adressen.**Hinweis:** Öffnen Sie eine Eingabeaufforderung, und geben Sie den Befehl **ipconfig /all** ein, um die MAC-Adresse und die IP-Adresse zu bestimmen.
3. Verwenden Sie Ping, um die Verbindung zwischen den PCs zu überprüfen.
4. Schalten Sie alle Client-PCs (PC 1, PC 2 und PC 3) nach der Überprüfung einer erfolgreichen Verbindung aus.
5. Starten Sie das WOL-Dienstprogramm auf dem Server-PC (PC 4).
6. Geben Sie die MAC-Adresse und die IP-Adresse des PCs ein, den Sie "Wake Up" (Einschalten) wie hier gezeigt aktivieren möchten: 

**Hinweis:** Bei der IP-Adresse kann es sich um eine beliebige Adresse (auch Subnetz-Broadcast) in dem VLAN-Subnetzbereich handeln, mit dem der Client-PC verbunden ist. Nur die MAC-Adresse des Client-PCs muss übereinstimmen.
7. Klicken Sie auf das Symbol **Wake UP PC**, um eine Reihe von Magic-Paketen an den Ziel-PC zu senden, um das Gerät einzuschalten. 

8. Wenn das Remote-Gerät die Weckmeldung empfängt und sich selbst einschaltet, wird folgende Meldung angezeigt: 

Der Client-PC ist jetzt eingeschaltet.

## Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

# Zugehörige Informationen

- LAN-Produktunterstützung
- Unterstützung der LAN Switching-Technologie
- Technischer Support und Dokumentation - Cisco Systems