Ejemplo de Configuración del Switch Catalyst de Capa 3 para Soporte Wake-On-LAN a través de VLAN

Contenido

Introducción

Este documento proporciona una configuración de ejemplo del soporte de WOL (Wake-On-LAN) en las VLAN con un switch Catalyst Layer 3.

Prerequisites

Requirements

Cisco recomienda tener conocimientos sobre estos temas antes de intentar esta configuración:

- Creación de VLAN de Ethernet en Switches Catalyst
- Cómo Comprender VLAN Trunk Protocol (VTP)
- Cómo configurar el ruteo entre VLAN en los switches de Capa 3.
- Uso de Portfast y otros comandos para solucionar retrasos al iniciar la conectividad de la estación de trabajo
- Resolución de problemas de DHCP en el switch Catalyst o en las redes corporativas e

introducción.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Catalyst 3750 Series Switch que ejecuta Cisco IOS® system Software Release 12.2(25r)SEC
- Catalyst 2950 Series Switches que ejecutan Cisco IOS system Software Release 12.1(19)EA1a
- PC que ejecutan el sistema operativo Microsoft Windows 2000
- Utilidad Freeware Wake-On-LAN de SolarWindsNota: Cisco no recomienda ninguna utilidad Wake-On-LAN.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Antecedentes

Wake-On-LAN

Wake-On-LAN (WOL) es una combinación de tecnologías de hardware y software para activar sistemas de suspensión. WOL envía paquetes de red especialmente codificados, llamados paquetes mágicos, a los sistemas equipados y habilitados para responder a estos paquetes. Esta funcionalidad adicional permite a los administradores realizar el mantenimiento de los sistemas incluso si el usuario los ha apagado. La función WOL permite que el administrador encienda de forma remota todos los equipos en espera para que puedan recibir actualizaciones. WOL se basa en el principio de que cuando el PC se apaga, el NIC todavía recibe energía y sigue escuchando en la red para que llegue el paquete mágico. Este paquete mágico se puede enviar a través de una variedad de protocolos sin conexión (UDP, IPX), pero UDP se utiliza con más frecuencia.

Si envía paquetes WOL desde redes remotas, los routers se deben configurar para permitir broadcasts dirigidos. Esto debe hacerse por estas dos razones:

- Como el PC está dormido, no tendrá una dirección IP y no responderá a los protocolos de resolución de direcciones (ARP) del router. Por lo tanto, sólo se transmite un paquete de broadcast IP de subred local en el segmento sin un ARP.
- Si hay un switch de Capa 2 entre el router y la PC, lo cual es cierto para la mayoría de las redes actuales, el switch no sabe a qué puerto está conectado físicamente la PC. Sólo se envía un broadcast de Capa 2 o una trama de unidifusión desconocida a todos los puertos del switch. Todos los paquetes de broadcast IP se dirigen a la dirección MAC de difusión.

Advertencias - Broadcasts Dirigidos

Las difusiones IP dirigidas se utilizan en el ataque de denegación de servicio smurf común y popular, y también se pueden utilizar en ataques relacionados.

Las transmisiones directas por IP son datagramas enviados a la dirección de difusión de una subred a la que el equipo de envío no está directamente conectado. La difusión directa se enruta a través de la red como un paquete de unidifusión hasta que llega a la subred de destino, donde se convierte en una difusión de capa de link. Debido a la naturaleza de la arquitectura de direccionamiento IP, sólo el último router de la cadena, el que se encuentra conectado directamente con la subred de destino, puede identificar en forma definitiva una transmisión dirigida. Algunas veces las difusiones directas se utilizan con objetivos legítimos, pero tal uso no es habitual fuera de la industria de servicios financieros.

En un ataque smurf, el atacante envía solicitudes de eco ICMP desde una dirección de origen falsificada a una dirección de broadcast dirigida. Esto hace que todos los hosts en la subred de destino envíen respuestas al origen falsificado. Al enviar un flujo continuo de tales solicitudes, el atacante puede crear un flujo mucho mayor de respuestas. Esto puede inundar completamente al host, cuya dirección es falsificada.

Si una interfaz de Cisco se configura con el comando no ip directed-broadcast, las broadcasts dirigidos que de otra manera se explotan en broadcasts de capa de link en esa interfaz se descartan en su lugar. Esto significa que el comando **no ip directed-broadcast** debe configurarse en cada interfaz de cada router que esté conectado a una subred de destino. No basta con configurar solamente en los routers de firewall. El comando **no ip directed-broadcast** es el valor predeterminado en Cisco IOS Software Release 12.0 y posteriores. En las versiones anteriores, el comando se debe aplicar a cada interfaz LAN que no se sabe que reenvía broadcasts dirigidos legítimos.

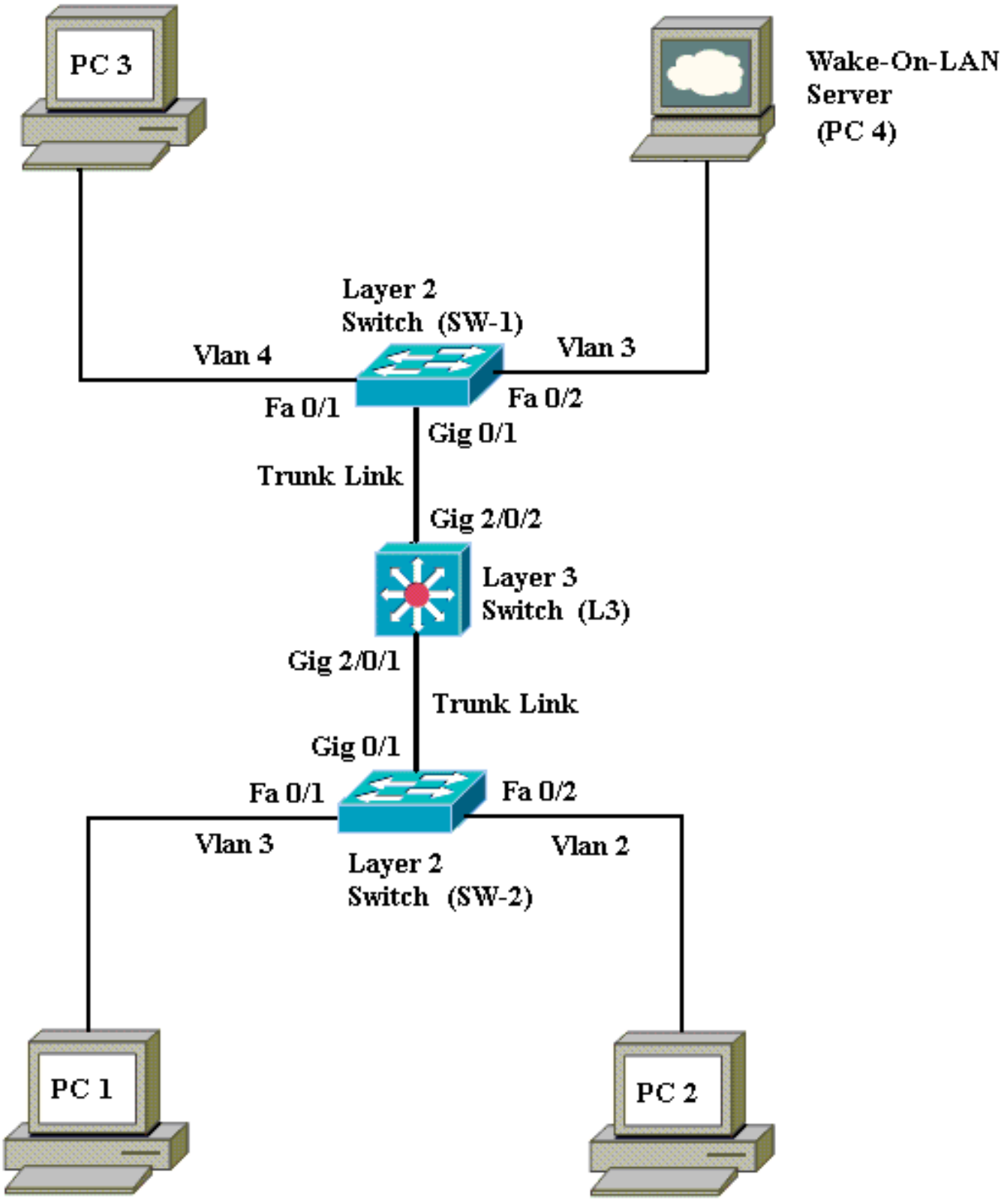
Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Use el Command Lookup Tool (únicamente clientes registrados) para obtener más información sobre los comandos que se utilizan en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Estos son los detalles de esta configuración de red:

- Los PC 1, 2 y 3 son los PC cliente que deben activarse.
- PC 4 es el servidor WOL así como el servidor DHCP.
- PC 4 está configurado con una dirección IP estática de 172.16.3.2/24.
- Los PC cliente se configuran para obtener la dirección IP de un servidor DHCP.
- El servidor DHCP (PC 4) se configura con tres ámbitos IP para los clientes que se conectan a las VLAN 2, 3 y 4.

- SW-1 y SW-2 (Catalyst 2950) se utilizan como switches de Capa 2 y L3 (Catalyst 3750) como switch de Capa 3.
- Los PC 1 y 4 están conectados en la misma VLAN (VLAN 3).
- Los PC 2 y 3 están conectados en VLAN 2 y 4 respectivamente.

Configuraciones de switches

Este documento utiliza estas configuraciones de switch:

- Switch de Capa 3 - L3
- Switches de Capa 2 - SW-1 y 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
```

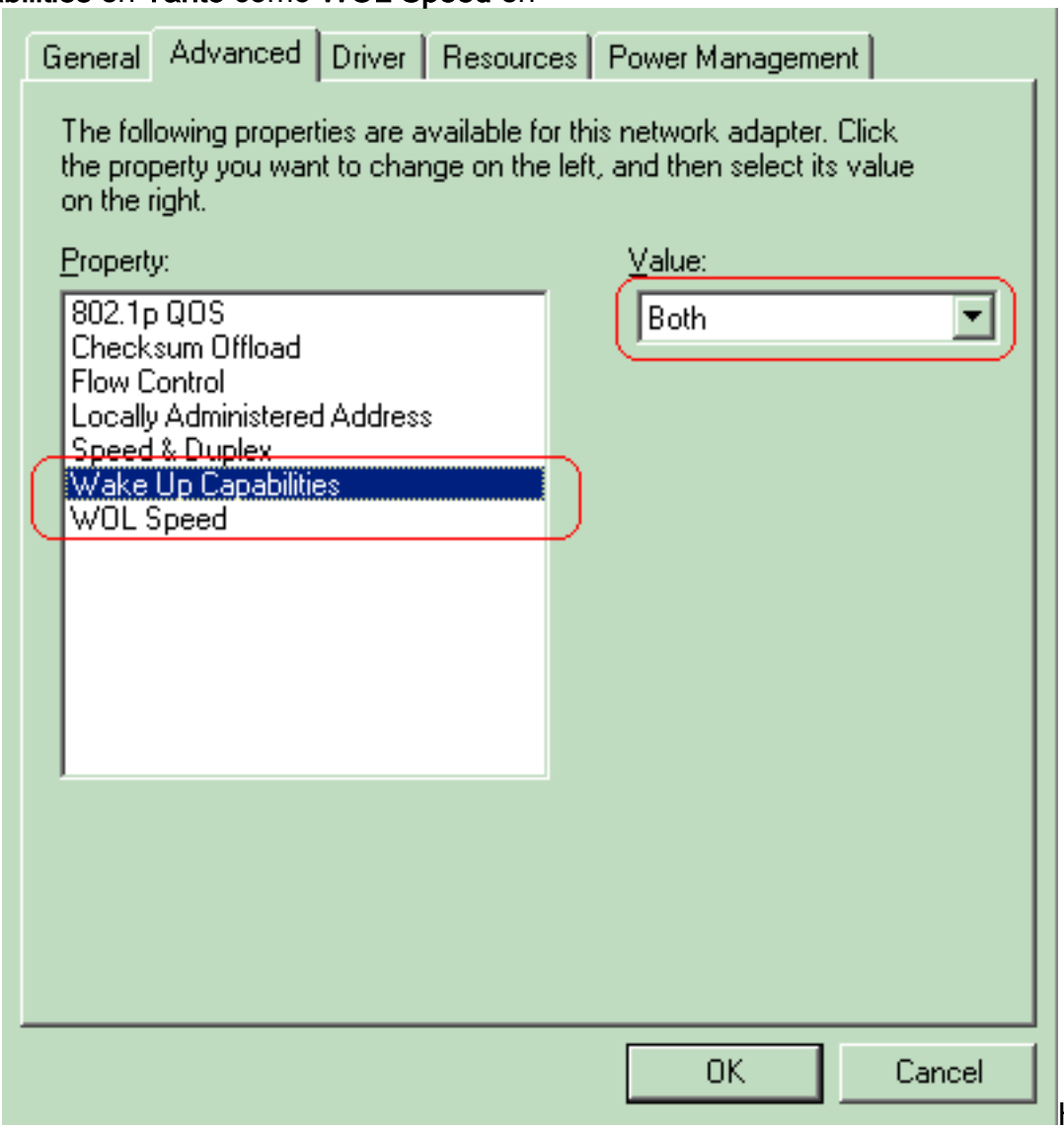
```
Enter configuration commands, one per line.  End with
CNTL/Z.
Switch(config)#hostname SW-2
SW-2(config)#vtp mode client
Setting device to VTP CLIENT mode.
SW-2(config)#vtp domain cisco
Changing VTP domain name from NULL to cisco
SW-2(config)#interface fastEthernet 0/1
SW-2(config-if)#spanning-tree 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#
```

Configuración del PC del cliente

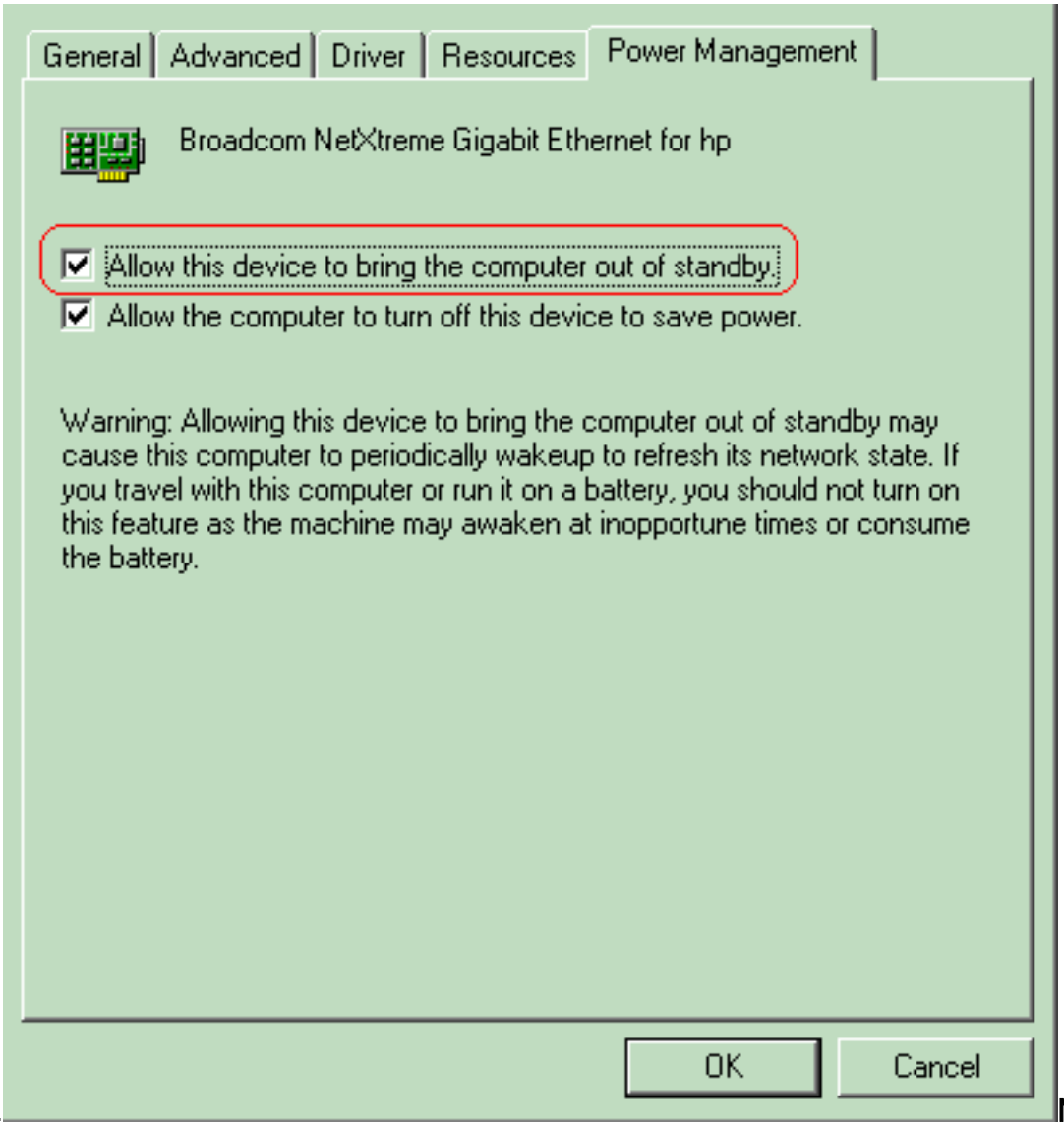
Hoy en día, la mayoría de las placas madre tienen una NIC integrada y admiten la funcionalidad WOL. Algunos ordenadores tienen WOL desactivado de forma predeterminada. Debe ingresar en las opciones del Sistema de salida de entrada básico (BIOS) para activar WOL. Este es el procedimiento para habilitar WOL en un equipo cliente:

1. Introduzca la pantalla de configuración del BIOS durante la autoprueba de encendido (POST) del ordenador.**Nota:** Normalmente, se presiona la tecla **F10** o **Delete** para ingresar la configuración del BIOS.
2. En la pantalla BIOS, navegue hasta los parámetros **avanzados** y luego **Opciones de dispositivo**.

3. En esta pantalla, busque los ajustes relacionados con **Wake-On-LAN** y habilite el .
4. Guarde y salga de la configuración del BIOS.**Nota:** El procedimiento exacto y las opciones disponibles en el BIOS para habilitar WOL son diferentes con cada fabricante de equipo. Consulte el manual de la placa base proporcionado con cada ordenador para obtener más información sobre los parámetros del BIOS.
5. Verifique las propiedades avanzadas de su tarjeta de red para asegurarse de que la funcionalidad WOL esté habilitada.Elija **Start > Settings > Network and Dial-up Connections** y luego haga clic con el botón derecho en su **Local Area Connection**.Haga clic en **Properties** y elija **Configure**.Vaya a la pestaña **Avanzadas**. Establezca la propiedad **Wake Up Capabilities** en **Tanto** como **WOL Speed** en



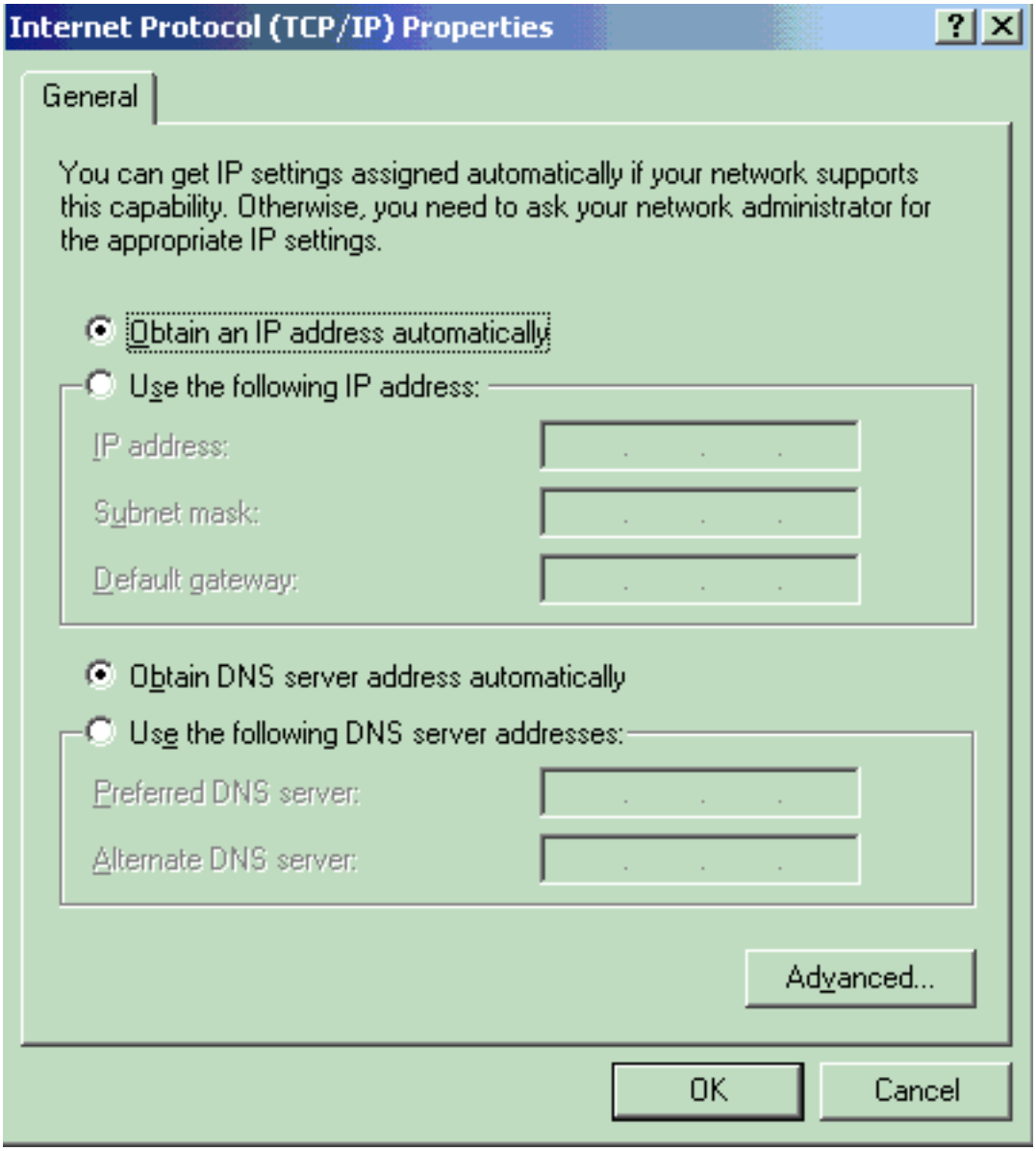
Auto. Haga clic en la ficha **Administración de energía** y marque la casilla que indica **Permitir que este dispositivo deje el equipo en**



espera.**Nota:** En los equipos con Microsoft Windows XP, hay una opción más: **Permitir solamente que las estaciones de administración saquen el equipo de modo en espera**. Esta última opción activa el equipo sólo si se recibe un paquete mágico WOL. Sin esta opción marcada, cualquier tráfico enviado al adaptador de red enciende el PC.

Complete estos pasos para que el cliente obtenga una dirección IP del servidor DHCP:

1. Elija **Start > Settings > Network and Dial-up Connections**, luego haga clic con el botón derecho en su **Local Area Connection** y elija **Properties**.
2. En la ficha **General**, haga clic en **Internet Protocol (TCP/IP)** y, a continuación, en **Properties**.
3. Elija **Obtener una dirección IP automáticamente**.



Configuración del PC del servidor

Complete estos pasos para configurar el servidor WOL:

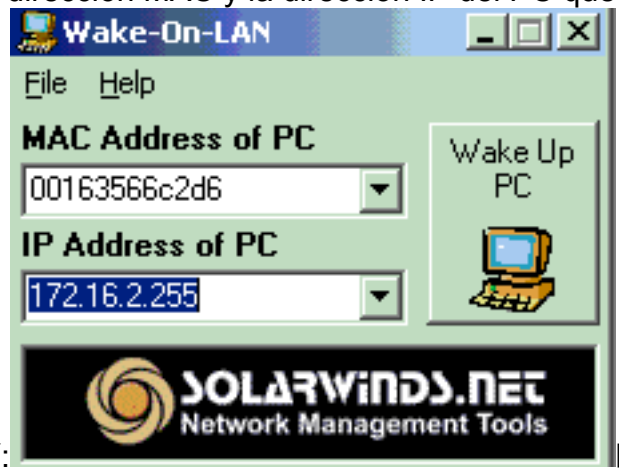
1. Descargue e instale la utilidad Wake-On-LAN.
2. Configure el PC con una dirección IP estática de 172.16.3.2/24.
3. Configure el PC como servidor DHCP.
4. Cree tres ámbitos con estos detalles:Refiérase a Cómo Instalar y Configurar un Servidor DHCP en un Grupo de Trabajo en Windows Server 2003 para obtener más información sobre la configuración del servidor DHCP.

Verificación

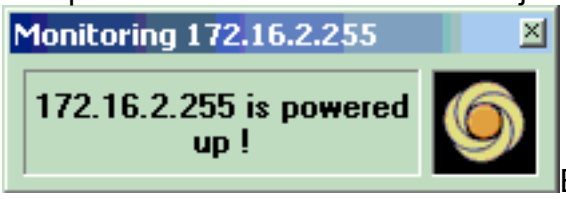
Utilize esta sección para confirmar que su configuración funcione correctamente.

Complete estos pasos:

1. Encienda los PC y conéctelos a los respectivos switches como se muestra en el Diagrama de red.

2. Inicie sesión en cada PC y tome nota de las direcciones MAC e IP.**Nota:** Abra un símbolo del sistema e ingrese el comando **ipconfig /all** para determinar la dirección MAC y la dirección IP.
3. Utilice Ping para verificar la conectividad entre los PC.
4. Apague todos los PC cliente (PC 1, PC 2 y PC 3) después de verificar que la conectividad es correcta.
5. Inicie la utilidad WOL en el PC servidor (PC 4).
6. Introduzca la dirección MAC y la dirección IP del PC que desea "Despertar", como se muestra aquí: 

Nota: La dirección IP puede ser cualquier dirección (incluso difusión de subred) en ese rango de subred VLAN al que esté conectada la PC cliente. Sólo la dirección MAC del PC cliente debe coincidir.
7. Haga clic en el icono **Wake UP PC** para enviar una serie de paquetes Magic al equipo de destino en un intento de encender el dispositivo. 

8. Cuando el dispositivo remoto recibe el mensaje de activación y se enciende, se muestra este mensaje: 

El PC cliente ya está encendido.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Soporte de Producto de LAN

- Soporte de Tecnología de LAN Switching
- Soporte Técnico y Documentación - Cisco Systems