Índice

Introdução

Este documento fornece uma configuração de exemplo para suporte a Wake-On-LAN (WOL) um switch Catalyst de Camada 3.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento destes assuntos antes que você tente esta configuração:

- Criando VLANs de Ethernet em Switches Catalyst
- **Como Entender O VLAN Trunk Protocol (VTP)**
- Como configurar o roteamento InterVLAN nos Switches de camada 3
- **Utilização de Portfast e outros comandos para reparar retardos de conectividade da inicialização de estação de trabalho**
- Compreensão e Troubleshooting DHCP no Catalyst Switch ou em Redes Corporativas

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Catalyst 3750 Series Switch que executa o system software release 12.2(25r)SEC de Cisco IOS®

- Catalyst 2950 Series Switch que executam o system software release 12.1(19)EA1a do Cisco IOS
- PC que executam o sistema operacional do Microsoft Windows 2000
- Utilidade do freeware Vigília-Em-LAN de SolarWinds **Nota:** Cisco não recomenda nenhuma utilidade Vigília-Em-LAN.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

Vigília-Em-LAN

O Vigília-Em-LAN (WOL) é uma combinação de Tecnologias de hardware e software para acordar sistemas do sono. WOL envia os pacotes de rede especialmente codificados, chamados pacotes mágicos, aos sistemas equipados e permitidos de responder a estes pacotes. Esta funcionalidade adicional permite que os administradores executem a manutenção em sistemas mesmo se o usuário os pôs para baixo. A característica de WOL permite que o administrador ponha remotamente acima todas as máquinas do sono de modo que possam receber atualizações. WOL é baseado no princípio que quando o PC fechou, o NIC ainda recebe a potência, e mantém-se escutar na rede o pacote mágico para chegar. Este pacote mágico pode ser enviado sobre uma variedade de protocolos sem conexão (UDP, IPX), mas o UDP é o mais de uso geral.

Se você envia pacotes de WOL das redes remotas, o Roteadores deve ser configurado para permitir transmissões direcionada. Isto deve ser feito para estas duas razões:

- Porque o PC está adormecido, não terá um endereço IP de Um ou Mais Servidores Cisco ICM NT e não responderá aos protocolos Protocolo de resolución de la dirección (ARP) (ARP) do roteador. Consequentemente, somente um pacote da transmissão IP da sub-rede local é transmitido no segmento sem um ARP.
- Se há um switch de Camada 2 entre o roteador e o PC, que é verdadeiro para a maioria de redes hoje, o interruptor não sabe a que porta o PC é conectado fisicamente. Somente uma transmissão da camada 2 ou um quadro do unicast desconhecido são mandados a todas as portas de switch. Todos os pacotes da transmissão IP são endereçados ao MAC address da transmissão.

Advertência - Transmissões direcionada

Os broadcasts direto de IP são usados no ataque de recusa de serviço comum e popular do smurf, e podem igualmente ser usados em ataques relacionados.

Uma transmissão direcionada de IP é um datagrama enviado ao endereço de transmissão de uma sub-rede à qual a máquina emissora não está diretamente conectada. A transmissão

direcionada é roteada pela rede como um pacote unicast até que chegue à sub-rede de destino, onde será convertida em uma transmissão de camada de enlace. Devido à natureza da arquitetura de endereçamento IP, apenas o último roteador da cadeia, o que está diretamente conectado à sub-rede de destino, pode identificar conclusivamente uma transmissão direcionada. As transmissões direcionadas são utilizadas ocasionalmente para finalidades legitimas, mas tal uso não é comum fora do setor de serviços financeiros.

Em um ataque de smurf, o atacante envia requisições de eco ICMP de um endereço de origem falsificado a um endereço de broadcast direcionado. Isto faz com que todos os anfitriões na sub-rede de destino enviem respostas ao origem falsificada. Enviando um fluxo contínuo de tal requisição, o atacante pode criar um fluxo de resposta muito maior. Isto pode completamente inundar o host, cujo o endereço é falsificado.

Se uma interface Cisco é configurada com o comando no ip directed-broadcast, as transmissões direcionada que são explodidas de outra maneira em broadcasts de camada de enlace nessa relação estão deixadas cair pelo contrário. Isto significa que o **comando no ip directed-broadcast** deve ser configurado em cada relação de cada roteador que é conectado a uma sub-rede de destino. Não é suficiente configurar somente em roteadores de firewall. **O comando no ip directed-broadcast** é o padrão no Cisco IOS Software Release 12.0 e Mais Recente. Nas versões anterior, o comando deve ser aplicado a cada interface de LAN que não é sabida para enviar transmissões direcionada legítimas.

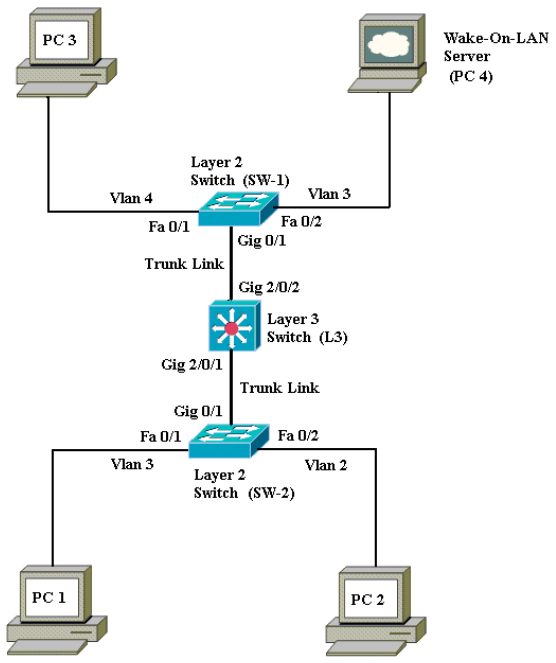
Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Estes são os detalhes desta instalação de rede:

- Os PC 1, 2 e 3 são o cliente PC que precisam de ser acordados.
- O PC 4 é o server de WOL assim como o servidor DHCP.
- O PC 4 é configurado com um endereço IP estático de 172.16.3.2/24.
- O cliente PC é configurado para obter o endereço IP de Um ou Mais Servidores Cisco ICM NT de um servidor DHCP.
- O servidor DHCP (PC 4) é configurado com três espaços IP para os clientes que conectam a VLAN 2,3 e 4.
- SW-1 e SW-2 (Catalyst 2950) estão usados enquanto os switch de Camada 2 e o L3 (catalizador 3750) são usados como o switch de camada 3.
- Os PC 1 e 4 são conectados no mesmo VLAN (VLAN3).
- Os PC 2 e 3 são conectados no VLAN2 e 4 respectivamente.

Configurações de switch

Este documento usa estas configurações de switch:

- Switch de camada 3 - L3
- Switch de Camada 2 - SW-1 e SW-2

L3

```
Switch>enSwitch#configure terminalEnter configuration
commands, one per line.  End with
CNTL/Z.Switch(config)#hostname L3L3(config)#ip
routingL3(config)#vtp mode serverDevice mode already VTP
SERVER.L3(config)#vtp domain ciscoChanging VTP domain
name from NULL to ciscoL3(config)#vlan 2L3(config-
vlan)#vlan 3L3(config-vlan)#vlan 4L3(config)#interface
gigabitEthernet 2/0/1L3(config-if)#switchport trunk
encapsulation dot1qL3(config-if)#switchport mode
trunkL3(config-if)#interface gigabitEthernet
2/0/2L3(config-if)#switchport trunk encapsulation
dot1qL3(config-if)#switchport mode trunkL3(config-
if)#exitL3(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 2L3(config-if)#ip address 172.16.2.1
255.255.255.0L3(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
3L3(config-if)#ip address 172.16.3.1
255.255.255.0L3(config-if)#ip helper-address
172.16.2.255L3(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
4L3(config-if)#ip address 172.16.4.1
255.255.255.0L3(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)#^ZL3#wrBuilding
configuration...[OK]L3#
```

SW-1

```
Switch>enSwitch#configure terminalEnter configuration
commands, one per line.  End with
CNTL/Z.Switch(config)#hostname SW-1SW-1(config)#vtp mode
clientSetting device to VTP CLIENT mode.SW-1(config)#vtp
domain ciscoChanging VTP domain name from NULL to
ciscoSW-1(config)#interface fastEthernet 0/1SW-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
accessSW-1(config-if)#switchport access vlan 4SW-
1(config-if)#interface fastEthernet 0/2SW-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
accessSW-1(config-if)#switchport access vlan 3SW-
1(config-if)#interface gigabitethernet 0/1SW-1(config-
if)#switchport mode trunkSW-1(config-if)#^ZSW-
1#wrBuilding configuration...[OK]SW-1#
```

SW-2

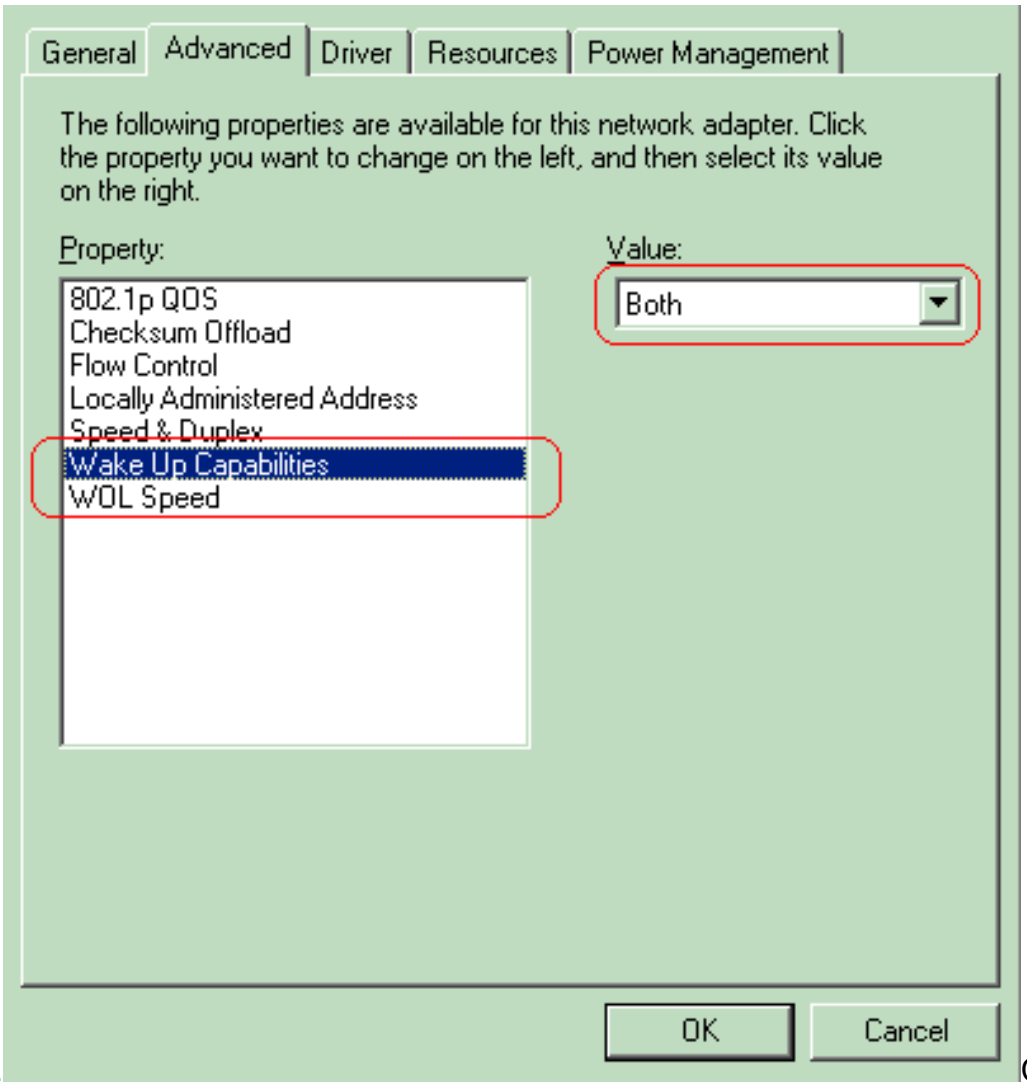
```
Switch>enSwitch#configure terminalEnter configuration
commands, one per line.  End with
CNTL/Z.Switch(config)#hostname SW-2SW-2(config)#vtp mode
clientSetting device to VTP CLIENT mode.SW-2(config)#vtp
domain ciscoChanging VTP domain name from NULL to
ciscoSW-2(config)#interface fastEthernet 0/1SW-2(config-
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
accessSW-2(config-if)#switchport access vlan 3SW-
2(config-if)#interface fastEthernet 0/2SW-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
accessSW-2(config-if)#switchport access vlan 2SW-
2(config)#interface gigabitethernet 0/1SW-2(config-
if)#switchport mode trunkSW-2(config-if)#^ZSW-
```

```
2#wrBuilding configuration...[OK]SW-2#
```

Configuração do PC cliente

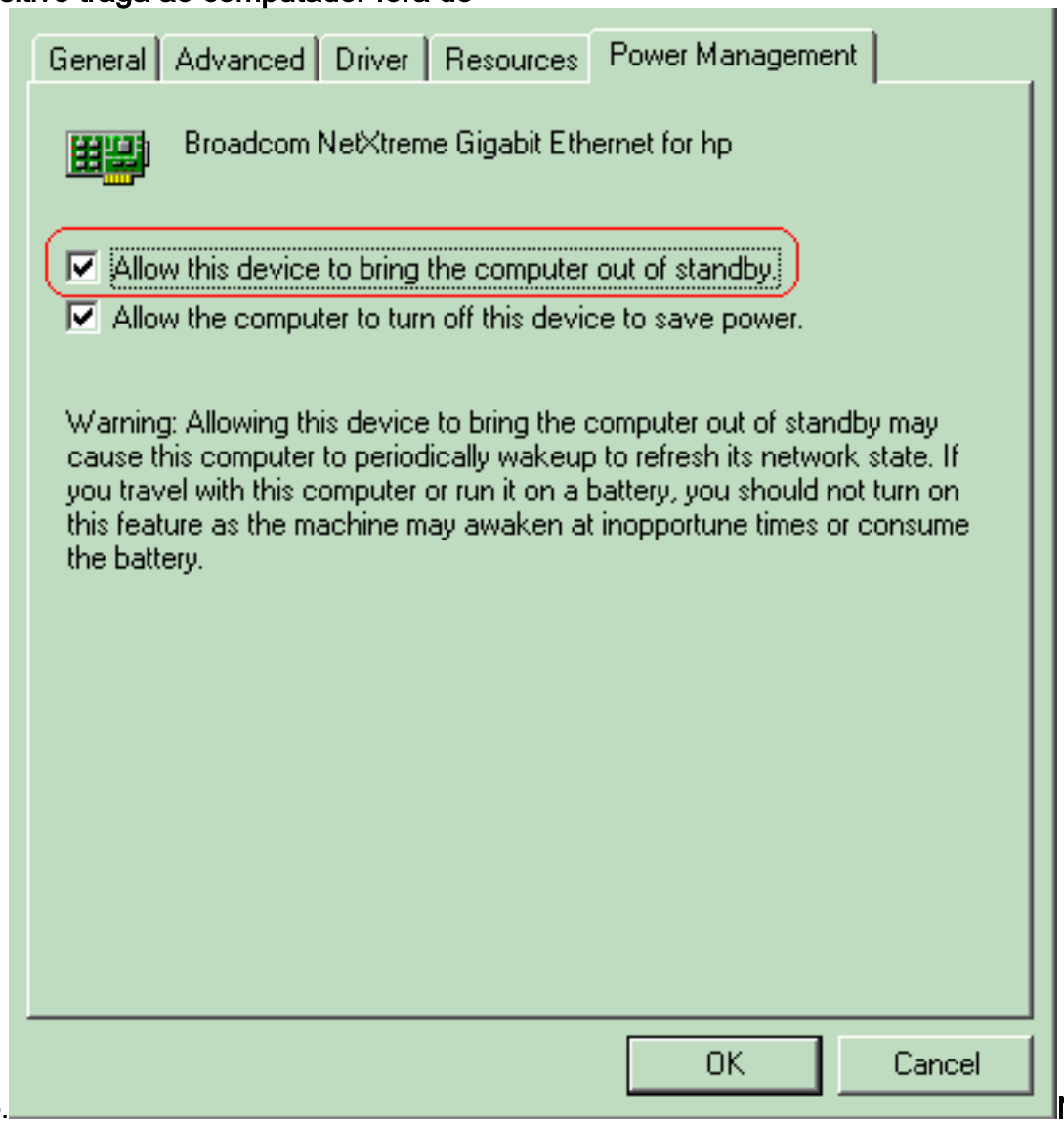
A maioria de cartões-matrizes hoje têm construído no NIC e apoiam a funcionalidade de WOL. Alguns computadores têm WOL desabilitados à revelia. Você tem que entrar nas opções básicas do sistema de entrada/saída (BIOS) permitir WOL. Este é o procedimento para permitir WOL em um PC cliente:

1. Entre na tela do ajuste BIOS durante o computador? s de potência self-test sobre (CARGO).**Nota:** Geralmente o **F10** ou a **tecla delete** são pressionados para incorporar os ajustes BIOS.
2. Dentro da tela BIOS, navegue aos ajustes e então às **opções avançados do dispositivo**.
3. Dentro desta tela, procure os ajustes relativos ao Vigília-Em-**LAN** e permita-os.
4. Salvar e retire os ajustes BIOS.**Nota:** O procedimento e as opções exatos disponíveis no BIOS para permitir WOL são diferentes com cada fabricação de computador. Refira o manual do cartão-matriz fornecido com cada computador para obter mais informações sobre dos ajustes BIOS.
5. Verifique as propriedades avançadas de sua placa de rede a fim assegurar-se de que a funcionalidade de WOL esteja permitida.Escolha o **começo > os ajustes > a rede e as conexões dial-up**, a seguir clicar com o botão direito em sua **conexão de área local**.Clique **propriedades** e escolha-as **configuram**.Navegue ao **guia avançada**. Ajuste a propriedade das **capacidades acordar aos ambos** e a **velocidade de WOL ao**



automóvel.Clique a

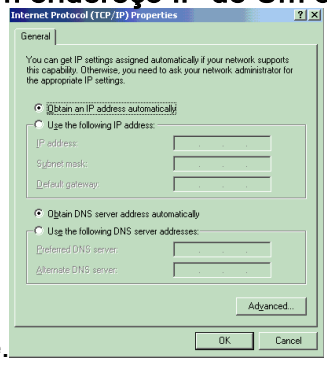
aba do **gerenciamento de energia** e verifique a caixa que os estados **permitem que este dispositivo traga ao computador fora do**



apoio. **Nota:** Em máquinas do Microsoft Windows XP, há uma mais opção: **Permita somente que as estações de gerenciamento tragam o computador fora do apoio**. Esta última opção gira sobre o computador somente se um pacote mágico de WOL é recebido. Sem esta opção verificada, todo o tráfego enviado ao adaptador de rede gira sobre o PC.

Termine estas etapas para que o cliente obtenha um endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor DHCP:

1. Escolha o **começo > os ajustes > a rede e as conexões dial-up**, a seguir clicar com o botão direito em sua **conexão de área local** e escolha **propriedades**.
2. Sob o **tab geral**, clique o **protocolo de internet (TCP/IP)** e então as **propriedades**.
3. Escolha **obtêm um endereço IP de Um ou Mais Servidores Cisco ICM NT**



automaticamente.

Configuração do PC do server

Termine estas etapas a fim configurar o server de WOL:

1. Transfira e instale a utilidade Vigília-Em-LAN.
2. Configurar o PC com um endereço IP estático de 172.16.3.2/24.
3. Configurar o PC como um servidor DHCP.
4. Crie três espaços com estes detalhes:Refira como instalar e configurar um servidor DHCP em um grupo de trabalho em Windows Server 2003 para obter mais informações sobre da configuração do servidor de DHCP.

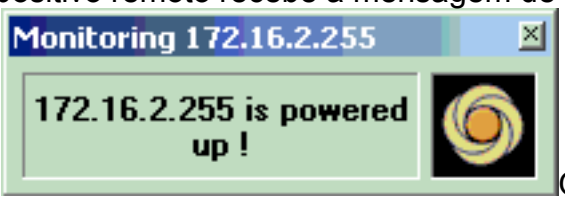
Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Conclua estes passos:

1. A potência nos PC e conecta-os aos switch respectivos segundo as indicações do diagrama da rede.
2. O log em cada PC e faz a anotação dos endereços e de endereços IP de Um ou Mais Servidores Cisco ICM NT MAC.**Nota:** Abra um comando prompt e incorpore o comando de **/all do ipconfig** a fim determinar o MAC address e o endereço IP de Um ou Mais Servidores Cisco ICM NT.
3. Use o sibilo a fim verificar a Conectividade entre os PC.
4. Desligue todo o cliente PC (PC1, PC2 e PC3) após a verificação de uma Conectividade bem sucedida.
5. Lance a utilidade de WOL no server PC (PC 4).
6. Incorpore o MAC address e endereço IP de Um ou Mais Servidores Cisco ICM NT do PC que você quer a “de alerta” como mostrado aqui: 

Nota: O endereço IP de Um ou Mais Servidores Cisco ICM NT pode ser todo o endereço (mesmo broadcast de sub-rede) nesse intervalo de sub-rede VLAN a que o PC cliente é conectado. Somente o MAC address do PC cliente precisa de combinar.
7. Clique sobre o ícone **acordar PC** a fim enviar uma série de pacotes mágicos ao alvo PC na tentativa de pôr sobre o dispositivo. 

8. Quando o dispositivo remoto recebe a mensagem de alerta e se põe sobre, esta mensagem está indicada: 

O PC cliente é posto agora sobre.

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Suporte a Produtos de LAN
- Suporte de tecnologia de switching de LAN
- Suporte Técnico e Documentação - Cisco Systems