Configure Layer 3 Switch for Wake-On-LAN Support across VLANs

Contents

Introduction

This document describes a sample configuration for Wake-On-LAN (WOL) support across VLANs with a Catalyst Layer 3 switch.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics before you attempt this configuration:

- Create Ethernet VLANs on Catalyst Switches
- Understand VLAN Trunk Protocol (VTP)
- Configure InterVLAN Routing on Layer 3 Switches
- Using PortFast and Other Commands to Fix Workstation Startup Connectivity Delays
- Troubleshoot DHCP in Catalyst Switch or Enterprise Networks

Components Used

The information in this document is based on these software and hardware versions:

- Catalyst 3750 Series Switch that runs Cisco IOS® system Software Release 12.2(25r)SEC
- Catalyst 2950 Series Switches that run Cisco IOS system Software Release 12.1(19)EA1a

- PCs that run Microsoft Windows 2000 operating system
- Freeware Wake-On-LAN utility from SolarWinds.

> **Note**: Cisco does not recommend any Wake-On-LAN utility.

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, ensure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Background Information

Wake-On-LAN

Wake-On-LAN (WOL) is a combination of hardware and software technologies to wake up sleeping systems. WOL sends specially coded network packets, called magic packets, to systems equipped and enabled to respond to these packets. This additional functionality allows administrators to perform maintenance on systems even if the user has powered them down. The WOL feature allows the administrator to remotely power up all sleeping machines so that they can receive updates. WOL is based on the principle that when the PC shuts down, the NIC still receives power, and keeps listening on the network for the magic packet to arrive. This magic packet can be sent over a variety of connectionless protocols (UDP, IPX), but UDP is most commonly used.

If you send WOL packets from remote networks, the routers must be configured to allow directed broadcasts. This must be done for these two reasons:

- Because the PC is asleep, it cannot have an IP address and cannot respond to Address Resolution Protocols (ARPs) from the router. Therefore, only a local subnet IP broadcast packet is transmitted on the segment without an ARP.
- If there is a Layer 2 switch between the router and the PC, which is true for most networks today, the switch does not know to which port the PC is physically connected. Only a Layer 2 broadcast or an unknown unicast frame is sent out to all switch ports. All IP broadcast packets are addressed to the broadcast MAC address.

Caveat - Directed Broadcasts

IP directed broadcasts are used in the common and popular smurf denial of service attack, and can also be used in related attacks.

An IP directed broadcast is a datagram which is sent to the broadcast address of a subnet to which the sending machine is not directly attached. The directed broadcast is routed through the network as a unicast packet until it arrives at the target subnet, where it is converted into a link-layer broadcast. Because of the nature of the IP addressing architecture, only the last router in the chain, the one that is connected directly to the target subnet, can conclusively identify a directed broadcast. Directed broadcasts are occasionally used for legitimate purposes, but such use is not common outside the financial services industry.

In a smurf attack, the attacker sends ICMP echo requests from a falsified source address to a directed broadcast address. This causes all the hosts on the target subnet to send replies to the falsified source. By sending a continuous stream of such requests, the attacker can create a much larger stream of replies. This can completely inundate the host, whose address is falsified.

If a Cisco interface is configured with the **no ip directed-broadcast** command, directed broadcasts that are otherwise exploded into link-layer broadcasts at that interface are dropped instead. This means that the **no ip directed-broadcast** command must be configured on every interface of every router that is connected to a target subnet. It is not sufficient to configure only on firewall routers. The no ip directed-broadcast command is the default in Cisco IOS Software Release 12.0 and later. In earlier releases, the command must be applied to every LAN interface that is not known to forward legitimate directed broadcasts.

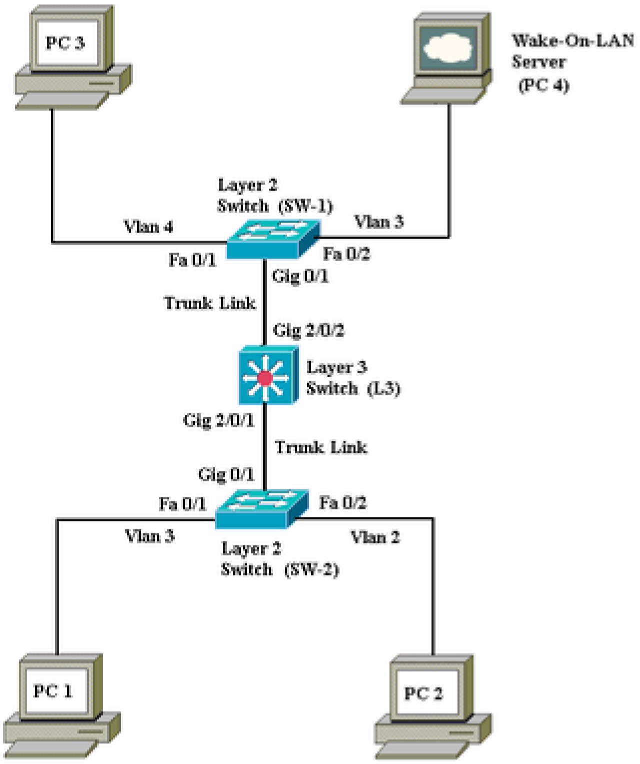
Configure

In this section, you are presented with the information to configure the features described in this document.

> **Note**: Use the Command Lookup Tool in order to obtain more information on the commands used in this section. Only registered Cisco users can access internal Cisco tools and information.

Network Diagram

This document uses this network setup:



Network Diagram

These are the details of this network setup:

- PCs 1, 2 and 3 are the client PCs which need to be woken up.
- PC 4 is the WOL server as well as the DHCP server.

- PC 4 is configured with a static IP address of 172.16.3.2/24.
- Client PCs are configured to obtain the IP address from a DHCP server.
- DHCP server (PC 4) is configured with three IP scopes for clients that connect to VLANs 2, 3 and 4.
- SW-1 and SW-2 (Catalyst 2950) are used as the Layer 2 switches and L3 (Catalyst 3750) is used as the Layer 3 switch.
- PCs 1 and 4 are connected in the same VLAN (VLAN 3).
- PCs 2 and 3 are connected in VLAN 2 and 4 respectively.

Switch Configurations

This document uses these switch configurations:

- Layer 3 switch - L3
- Layer 2 switches - SW-1and SW-2

L3

<#root>

```
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

<#root>

```
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 must 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 can 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 must 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 can 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

```
<#root>

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 must 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 can 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 must 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 can 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 Configuration

Most motherboards today have a built in NIC and support WOL functionality. Some computers have WOL disabled by default. You have to go into the Basic Input Output System (BIOS) options to enable WOL. This is the procedure to enable WOL on a client PC:

1. Enter the BIOS setting screen during the computerâ€™s Power On Self Test (POST).

    Note: Usually the F10 or Delete key is pressed to enter the BIOS settings.

2. Within the BIOS screen, navigate to the **Advanced** settings and then **Device Options**.

3. Within this screen, look for settings related to **Wake-On-LAN** and enable it.

4. Save and exit the BIOS settings.

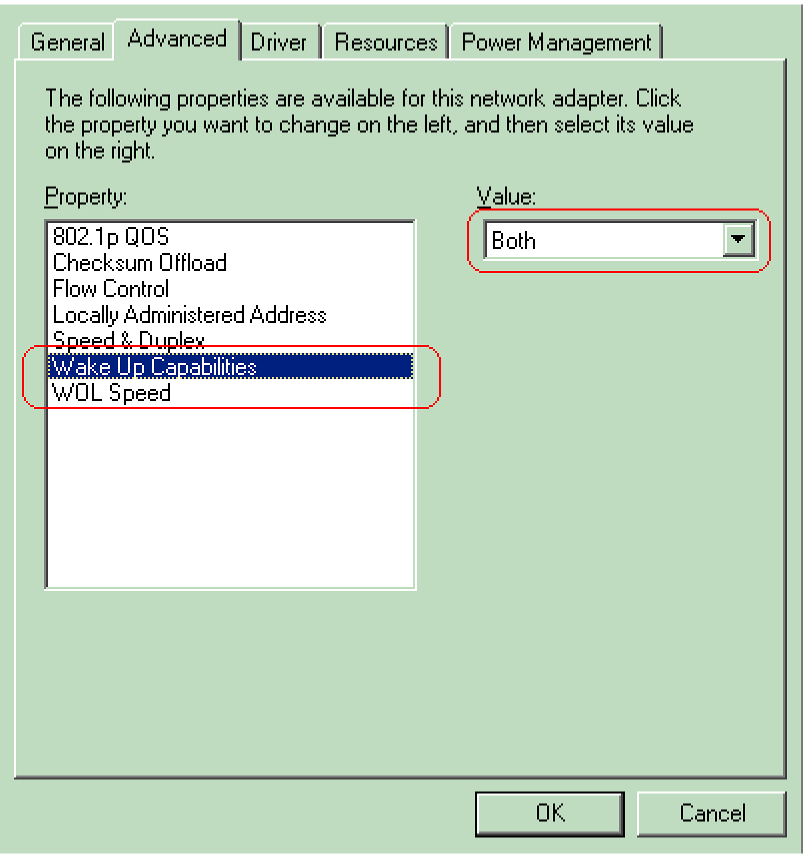
    Note: The exact procedure and options available in BIOS to enable WOL are different with each computer manufacturer. Refer to the motherboard manual provided with each computer for more information on the BIOS settings.

5. Check the advanced properties of your network card in order to ensure that the WOL functionality is enabled.

   a. Choose **Start** > **Settings** > **Network and Dial-up Connections** , then right-click on your **Local Area Connection**.

   b. Click **Properties** and choose **Configure**.

   c. Navigate to the **Advanced** tab. Set the **Wake Up Capabilities** property to **Both** and **WOL Speed** to**Auto**.



The following properties are available for this network adapter. Click the property you want to change on the left, and then select its value on the right.

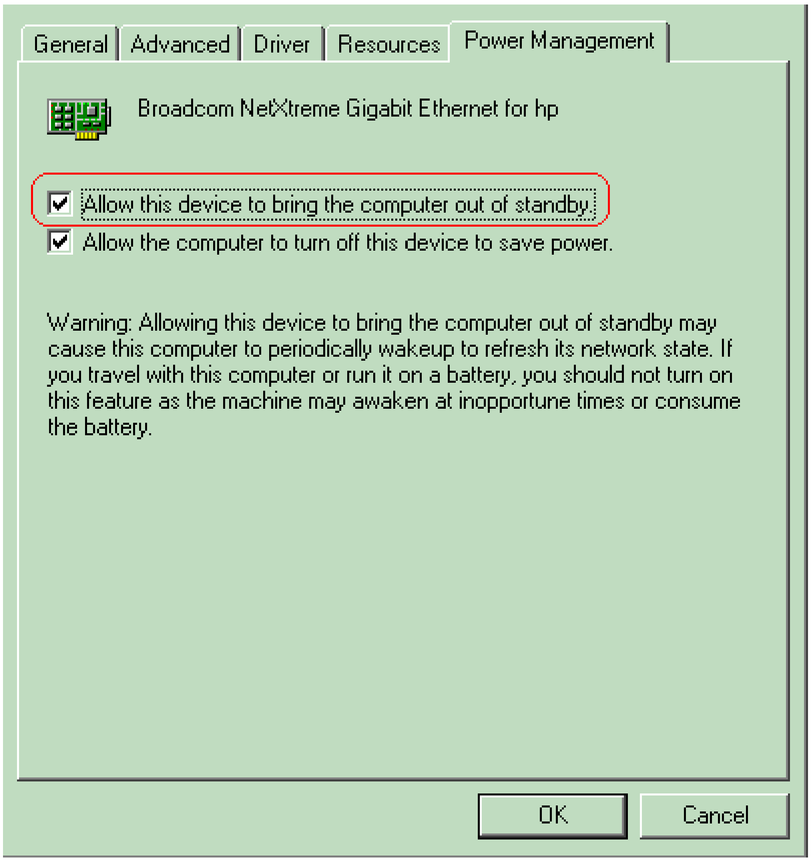
Property:

802.1p QOS
Checksum Offload
Flow Control
Locally Administered Address
Speed & Duplex
Wake Up Capabilities
WOL Speed

Value: Both

Wake Up Capabilities

d. Click the **Power Management** tab and check the box that states **Allow this device to bring the computer out of standby**.



Broadcom NetXtreme Gigabit Ethernet for hp

☑ Allow this device to bring the computer out of standby.

☑ Allow the computer to turn off this device to save power.

Warning: Allowing this device to bring the computer out of standby may cause this computer to periodically wakeup to refresh its network state. If you travel with this computer or run it on a battery, you should not turn on this feature as the machine may awaken at inopportune times or consume the battery.

Bring the Computer out of Standby

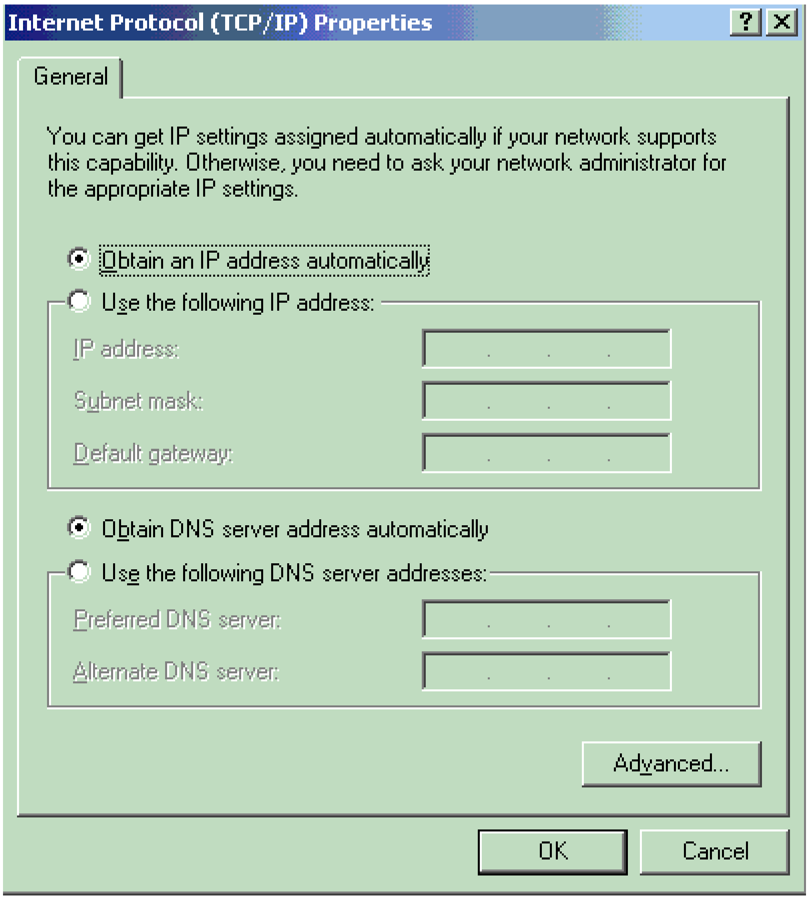
> **Note**: In Microsoft Windows XP machines, there is one more option: Only allow management stations to bring the computer out of standby. This last option turns on the computer only if a WOL magic packet is received. Without this option checked, any traffic sent to the network adapter turns on the PC.

Complete these steps in order for the client to obtain an IP address from the DHCP server:

1. Choose **Start > Settings > Network and Dial-up Connections** , then right-click on your **Local Area Connection** and choose **Properties**.

2. Under the **General** tab, click **Internet Protocol (TCP/IP)** and then **Properties**.

3. Choose **Obtain an IP address automatically**.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Obtain IP Address Automatically

Server PC Configuration

Complete these steps in order to configure the WOL server:

1. Download and install the Wake-On-LAN utility.
2. Configure the PC with a static IP address of 172.16.3.2/24.
3. Configure the PC as a DHCP server.
4. eate three scopes with these details:

Scope	IP Range	IP Excluded Range
VLAN 2	172.16.2.1 - 172.16.2.254 Mask - 255.255.255.0	172.16.2.1
VLAN 3	172.16.3.1 - 172.16.3.254 Mask - 255.255.255.0	172.16.3.1 and 172.16.3.2
VLAN 4	172.16.4.1 - 172.16.4.254 Mask - 255.255.255.0	172.16.4.1

Refer to How To Install and Configure a DHCP Server in a Workgroup in Windows Server 2003 for more information on the DHCP server configuration.

Verify

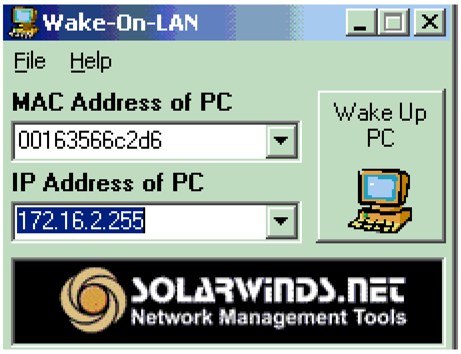
Use this section in order to confirm that your configuration works properly.

Complete these steps:

1. Power on the PCs and connect them to the respective switches as shown in the Network Diagram.
2. Log into each PC and make note of the MAC addresses and IP addresses.

> **Note**: Open a command prompt and enter the ipconfig /all command in order to determine the MAC address and IP address.

3. Use Ping in order to check the connectivity between the PCs.
4. Turn off all the client PCs (PC 1, PC 2 and PC 3) after verification of a successful connectivity.
5. Launch the WOL utility on the server PC (PC 4).
6. Enter the MAC address and IP address of the PC you want to "Wake-Up" as shown here:



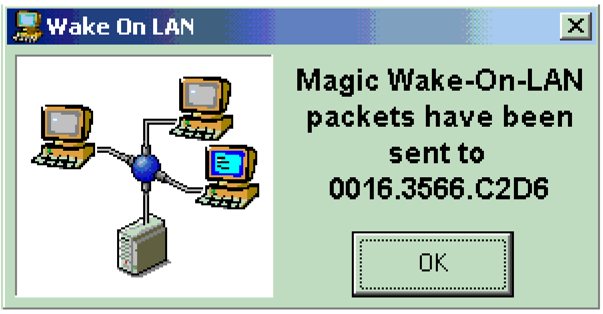
MAC Address of PC: 00163566c2d6

IP Address of PC: 172.16.2.255

IP Address of PC

> **Note**: The IP address can be any address (even subnet broadcast) in that VLAN subnet range to which the client PC is connected. Only the MAC address of the client PC needs to match.

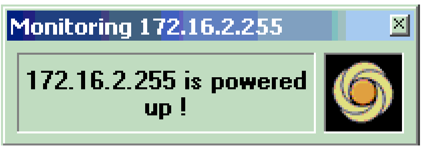
7. Click on the **Wake UP PC** icon in order to send a series of Magic packets to the target PC in an attempt to power on the device.



Magic Wake-On-LAN packets have been sent to 0016.3566.C2D6

Magic Packets to the Target PC

8. When the remote device receives the wake-up message and powers itself on, this message is displayed:



Monitoring 172.16.2.255

172.16.2.255 is powered up !

Wake-up Message and Powers On

The client PC is now powered on.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- **LAN Product Support**
- **LAN Switching Technology Support**
- **Cisco Technical Support & Downloads**