Пример конфигурации коммутатора Catalyst уровня 2 для поддержки Wake-On-LAN через сети VLAN

Содержание

Введение

В настоящем документе описывается пример конфигурации поддержки Wake-On-LAN (WOL) через сети VLAN с помощью коммутатора Catalyst уровня 3.

Предварительные условия

Требования

Cisco рекомендует ознакомиться с темами в данном документе перед началом конфигурации:

- Создание сетей Ethernet VLAN на коммутаторах Catalyst
- Понимание протокола VLAN Trunk Protocol (VTP)
- Как настроить маршрутизацию InterVLAN на коммутаторах уровня 3
- Использование функции PortFast и других команд для устранения задержек соединения во время запуска рабочей станции

- Общие сведения и устранение неисправностей DHCP на коммутаторе Catalyst или корпоративных сетях

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Коммутатор Catalyst версии 3750 с ПО Cisco IOS® версии 12.2(25r)SEC
- Коммутатор Catalyst версии 2950 с ПО Cisco IOS® версии 12.1(19)EA1a
- PC с операционной системой Microsoft Windows 2000
- Бесплатная утилита Wake-On-LAN в SolarWinds**Примечание:** Cisco не рекомендует применять утилиту Wake-On-LAN.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Общие сведения

Wake-On-LAN

Wake-On-LAN (WOL) – это совокупность технологий программного и аппаратного обеспечения для возобновления работы систем. WOL отправляет запрограммированные сетевые пакеты, которые называются специальными пакетами (magic packet), в оснащенные и активированные системы для ответа на данные пакеты. Эта дополнительная функция позволяет администраторам выполнять поддержку систем, даже если пользователь выключил питание. Функция WOL позволяет администраторам включать питание на удаленных компьютерах. Таким образом, их можно обновлять. WOL работает по принципу, если PC отключается, NIC не теряет мощности и ждет появления в сети специальных пакетов. Данный специальный пакет можно отправлять через множество протоколов без предварительного соединения (UDP, IPX), но UDP используют наиболее часто.

Если отправить пакеты WOL из удаленных сетей, маршрутизаторы необходимо настроить для разрешения прямой широковещательной рассылки. Это необходимо выполнить по двум причинам:

- Так как PC отключен, у него нет IP-адреса, и он не ответит на протоколы разрешения адресов (ARP) в маршрутизаторе. Таким образом, в сегменте передается только широковещательный IP-пакет локальной подсети без ARP.
- Если между маршрутизатором и PC находится коммутатор уровня 2, который подходит для большинства сетей, данному коммутатору неизвестно, к какому порту физически подключен PC. Только широковещательная рассылка уровня 2 или одноадресный кадр отправляют на все порты коммутаторов. Все IP-пакеты широковещательной рассылки

предназначены для MAC-адреса широковещательной рассылки.

Предупреждение – Прямые широковещательные рассылки

Прямые широковещательные IP-рассылки очень часто используются для атаки smurf. Таким образом, такие рассылки также могут использоваться и для атак, аналогичных атакам smurf.

IP directed broadcast – это дейтограмма, отправляемая на широковещательный адрес подсети, с которой отправляющий сообщения компьютер напрямую не соединен. Управляемая широковещательная рассылка рассылается по сети в качестве одноадресного пакета, пока не достигает заданной подсети, где преобразуется в широковещательную рассылку канального уровня. Из-за особенностей архитектуры IP-адресации только последний маршрутизатор в цепочке, подключенный напрямую к подсети назначения, может точно идентифицировать направленное широковещание. Направленные рассылки иногда осуществляются для законных целей, но такое использование — редкость вне сферы финансовых услуг.

При атаке смарф злоумышленник, использующий сфальсифицированный адрес отправителя, отправляет эхо-запросы ICMP на адрес прямой широковещательной рассылки. После этого все узлы, принадлежащие атакуемой подсети, посылают отклики на сфальсифицированный адрес. Отправляя непрерывный поток таких запросов атакующий может создать намного больший по объему поток откликов. Таким образом, поток этих ответов может полностью "затопить" хост, адрес которого был сфальсифицирован.

Если для интерфейса Cisco была настроена команда no ip directed-broadcast, тогда направленные широковещательные рассылки, которые в противном случае были бы преобразованы в рассылки канального уровня, будут отброшены на этом интерфейсе. Это означает, что команду no ip directed-broadcast необходимо настроить на всех интерфейсах всех маршрутизаторов, которые подключены к атакуемой подсети. Настроить данную команду только на маршрутизаторах межсетевых экранов будет недостаточно. **Команда no ip directed-broadcast установлена по умолчанию в Cisco IOS версии 12.0 и последующих версий.** В более ранних версиях данную команду применяли к каждому интерфейсу LAN, о котором отсутствовала информация, что он пересылает легальные прямые широковещательные рассылки.

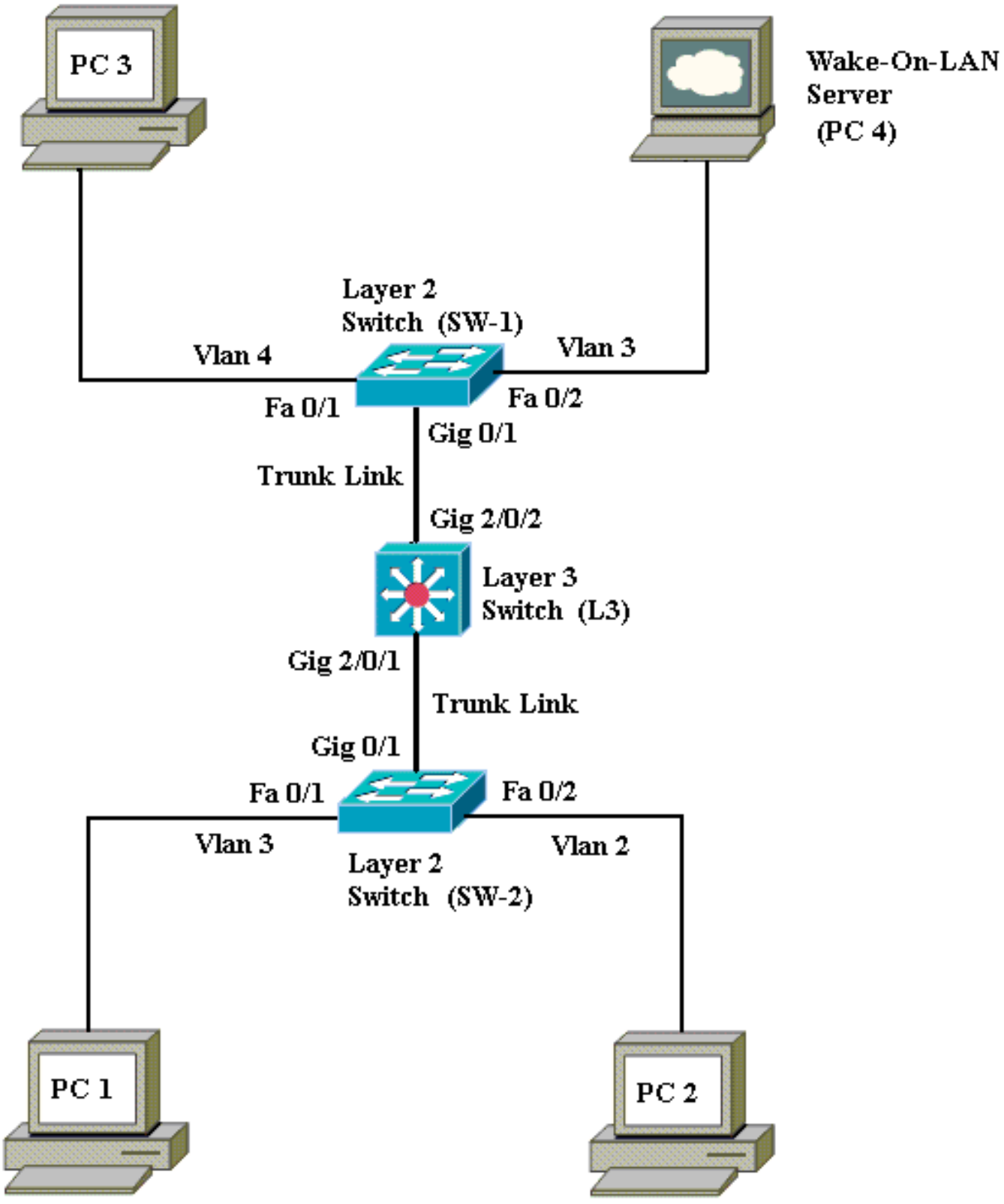
Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

Схема сети

В настоящем документе используется следующая схема сети:



Ниже представлены подробности настройки данной сети:

- PC 1, 2 и 3 являются клиентскими PC, которые необходимо подключить.
- PC 4 не является сервером WOL, также как и сервер DHCP.
- PC 4 настраивается с помощью статического IP-адреса 172.16.3.2/24.
- Клиентские PC настраиваются для получения IP-адреса с сервера DHCP.
- Сервер DHCP (PC 4) настраивается с помощью трех IP-областей для клиентов, которые подключаются к сетям VLAN 2, 3 и 4.

- SW-1 и SW-2 (Catalyst 2950) используются в качестве коммутаторов уровня 2, а L3 (Catalyst 3750) используются в качестве коммутатора уровня 3.
- PC 1 и 4 подключаются к одной VLAN (VLAN 3).
- PC 2 и 3 подключаются к VLAN 2 и 4 соответственно.

Конфигурации коммутаторов

В данном документе используются следующие конфигурации коммутаторов:

- Коммутатор 3 уровня - L3
- Коммутаторы уровня 2 – SW-1 и 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#
```

SW1

```
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#
```

SW2

```
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#
```

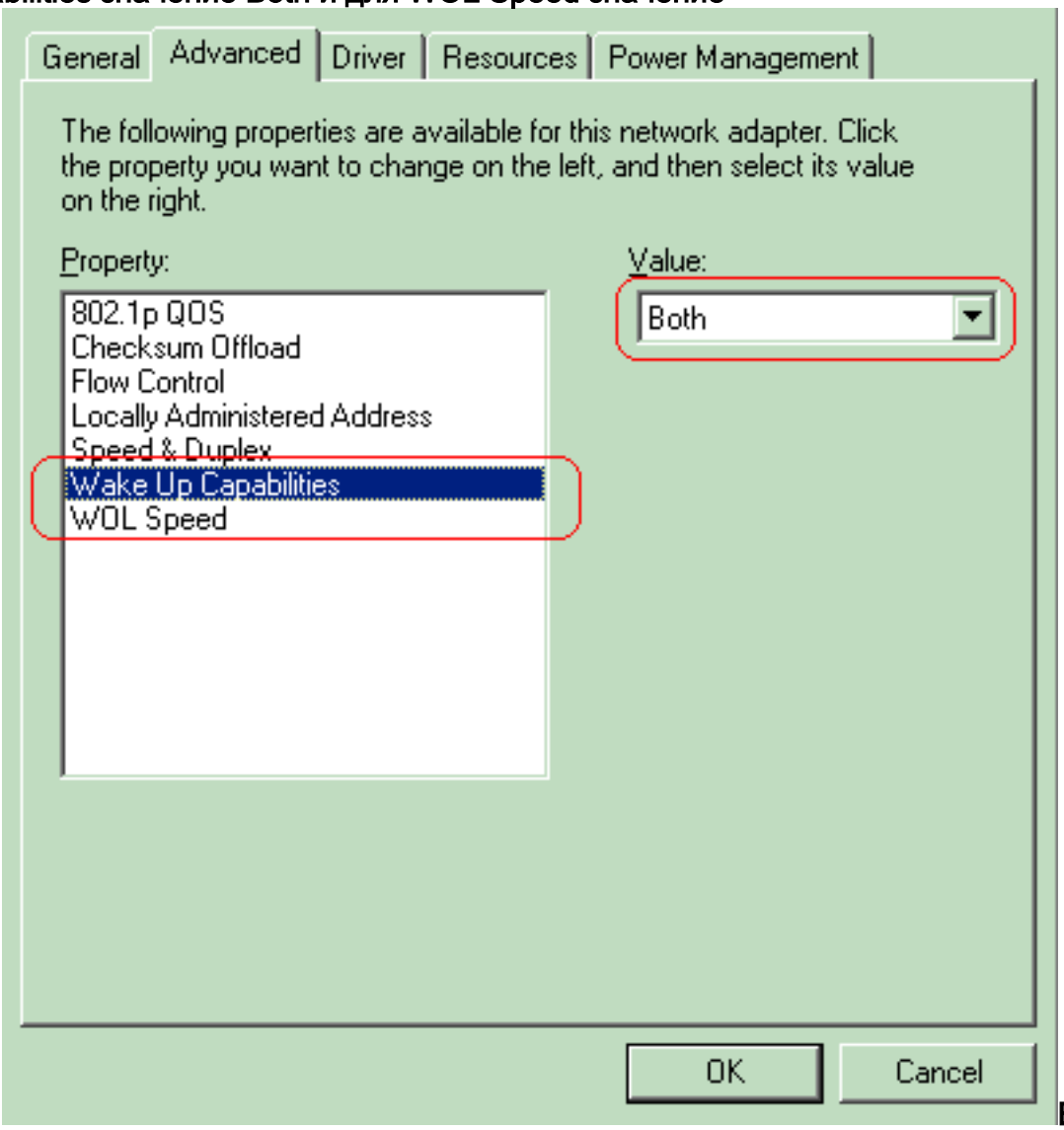
Конфигурация клиентского PC

Сегодня большинство материнских плат имеют встроенную NIC и поддерживают функцию WOL. В некоторых компьютерах WOL по умолчанию отключен. Необходимо перейти к параметрам базовой системы ввода-вывода (BIOS), чтобы включить WOL. Ниже преставлена процедура активации WOL на клиентском PC:

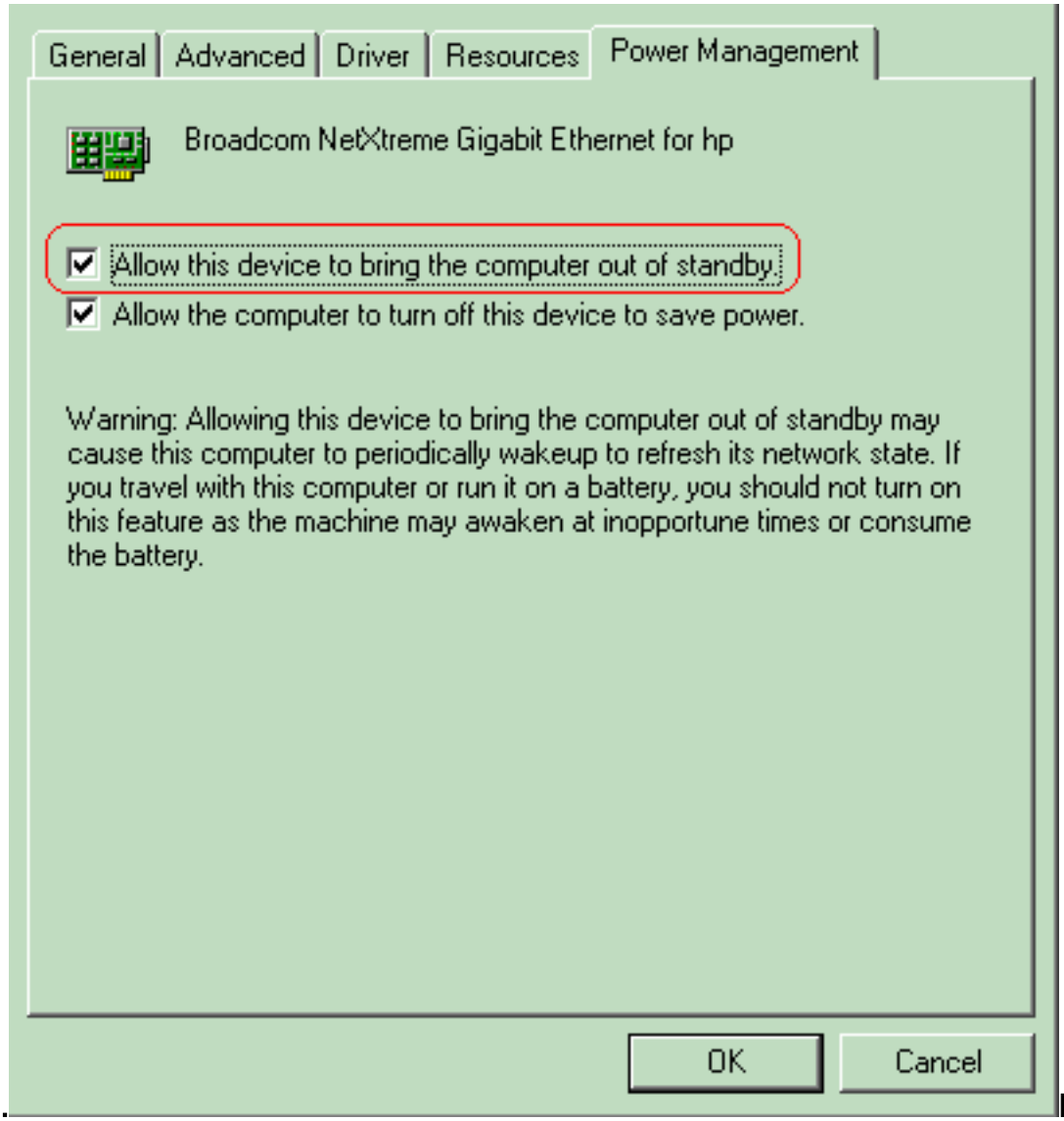
1. Войдите в экран параметров BIOS во время процедуры начального самотестирования компьютера (POST).**Примечание: Чтобы ввести параметры BIOS, обычно нажимают клавишу F10 или Delete.**
2. **В экране BIOS перейдите к параметрам Advanced, а потом Device Options.**
3. **На экране найдите параметры, связанные Wake-On-LAN и активируйте.**
4. Сохраните и выйдите из параметров BIOS.**Примечание:** Точная процедура и параметры, доступные в BIOS для включения WOL, различаются в зависимости от производителя компьютера. Дополнительные сведения о параметрах BIOS см. в

материнской плате, которая идет в комплекте с каждым компьютером.

5. Проверьте дополнительные свойства сетевой карты, чтобы убедиться, что функция WOL включена.**Выберите Start > Settings > Network and Dial-up Connections, а потом правой кнопкой мыши щелкните Local Area Connection.Щелкните Properties и выберите Configure.Перейдите к вкладке Advanced. Установите для свойства Wake Up Capabilities значение Both и для WOL Speed значение**



Auto. **Выберите вкладку Power Management и установите флажок Allow this device to bring the computer out of standby (разрешить устройству вывести компьютер из режима**

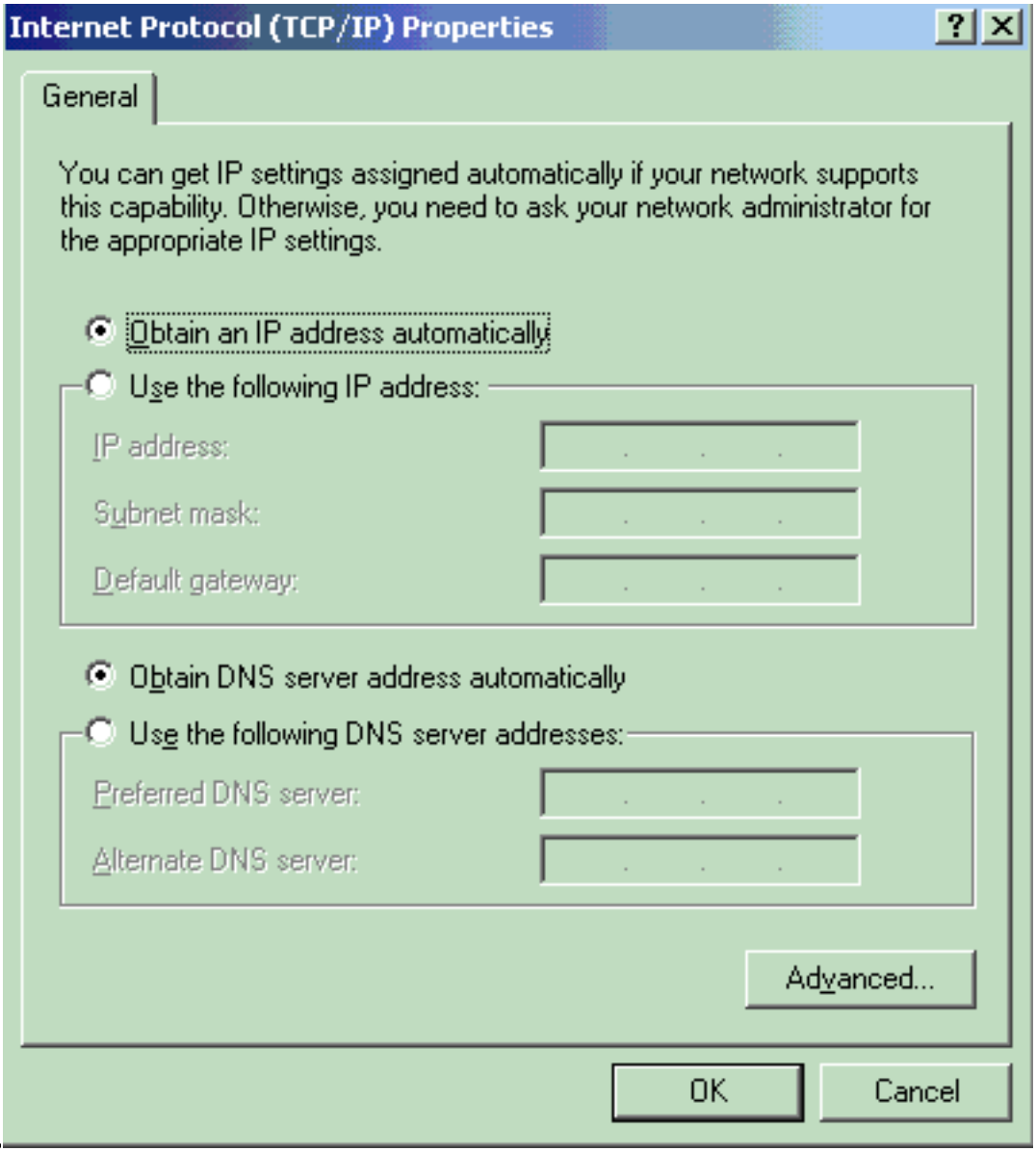


ожидания). **Прим ечание:** В компьютерах Microsoft Windows XP существует еще один параметр: **Only allow management stations to bring the computer out of standby (разрешить управляющим станциям только вывести компьютер из режима ожидания).** С помощью последнего параметра можно включить компьютер, только если получен специальный пакет WOL. Без проверки данного параметра любой трафик, отправленный в адаптер сети, включает PC.

Выполните следующие действия, чтобы получить для клиента IP-адрес из сервера DHCP:

1. **Выберите Start > Settings > Network and Dial-up Connections, а потом правой кнопкой мыши щелкните Local Area Connection.**
2. **Под вкладкой General щелкните Internet Protocol (TCP/IP), а потом Properties.**
3. **Выберите Obtain an IP address automatically (получать IP-адрес**

автоматически).



Конфигурация сервера PC

Выполните следующие действия, чтобы настроить сервер WOL:

1. Загрузите и установите утилиту Wake-On-LAN.
2. Настройте PC с помощью статического IP-адреса 172.16.3.2/24.
3. Настройте PC в качестве сервера DHCP.
4. Создайте три области со следующими элементами:Дополнительные сведения о конфигурации сервера DHCP см. в разделе Как установить и настроить сервер DHCP в рабочей группе с сервером Windows 2003.

Проверка

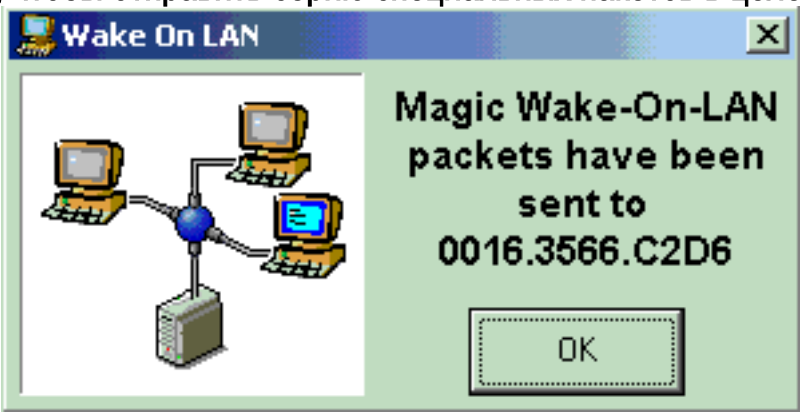
Воспользуйтесь данным разделом для проверки правильности функционирования вашей конфигурации.

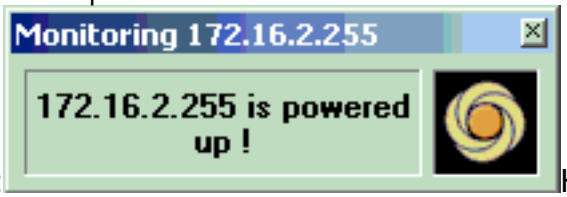
Выполните следующие действия:

1. Включите PC и подключите их к соответствующим коммутаторам, как показано на

Схеме сети.

2. Войдите в систему каждого PC и отметьте MAC-адреса и IP-адреса.**Примечание: Откройте командную строку и введите команду ipconfig /all, чтобы определить MAC-адрес и IP-адрес.**
3. Используйте Ping, чтобы проверить подключения между PC.
4. После проверки успешного подключения выключите клиентские PC (PC 1, PC 2 и PC 3).
5. Запустите утилиту WOL на сервере PC (PC 4).
6. Введите MAC-адрес и IP-адрес того PC, который необходимо включить, как показано ниже: 

Примечание: IP-адрес может быть любым адресом (даже широковещательной рассылкой подсети) в диапазоне подсети той VLAN, к которой подключен клиентский PC. Совпадать должен только MAC-адрес клиентского PC.
7. **Щелкните значок Wake UP PC, чтобы отправить серию специальных пакетов в целевой PC для включения устройства.** 

8. Если удаленное устройство получает сообщение о включении и включается, отображается следующее сообщение: 

Клиентский PC сейчас включен.

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Дополнительные сведения

- Поддержка продуктов для ЛВС
- Поддержка технологии коммутации локальных сетей
- Cisco Systems – техническая поддержка и документация