

# Глава 6. Практические навыки организации работы сети

Основы информационных технологий 7.0



# Сетевая адресация

## Два сетевых адреса



### Формат MAC-адреса

Формат адреса	Описание
00-50-56-BE-D7-87	Два шестнадцатеричных числа, разделенные дефисами
00:50:56:BE:D7:87	Два шестнадцатеричных числа, разделенные двоеточиями
0050.56BE.D787	Два шестнадцатеричных числа, разделенные точками

### Формат IPv4-адреса

32 бита в десятичном формате с разделением точками

**192.168.200.8**

### Формат IPv6-адреса

128 битов в шестнадцатеричном формате

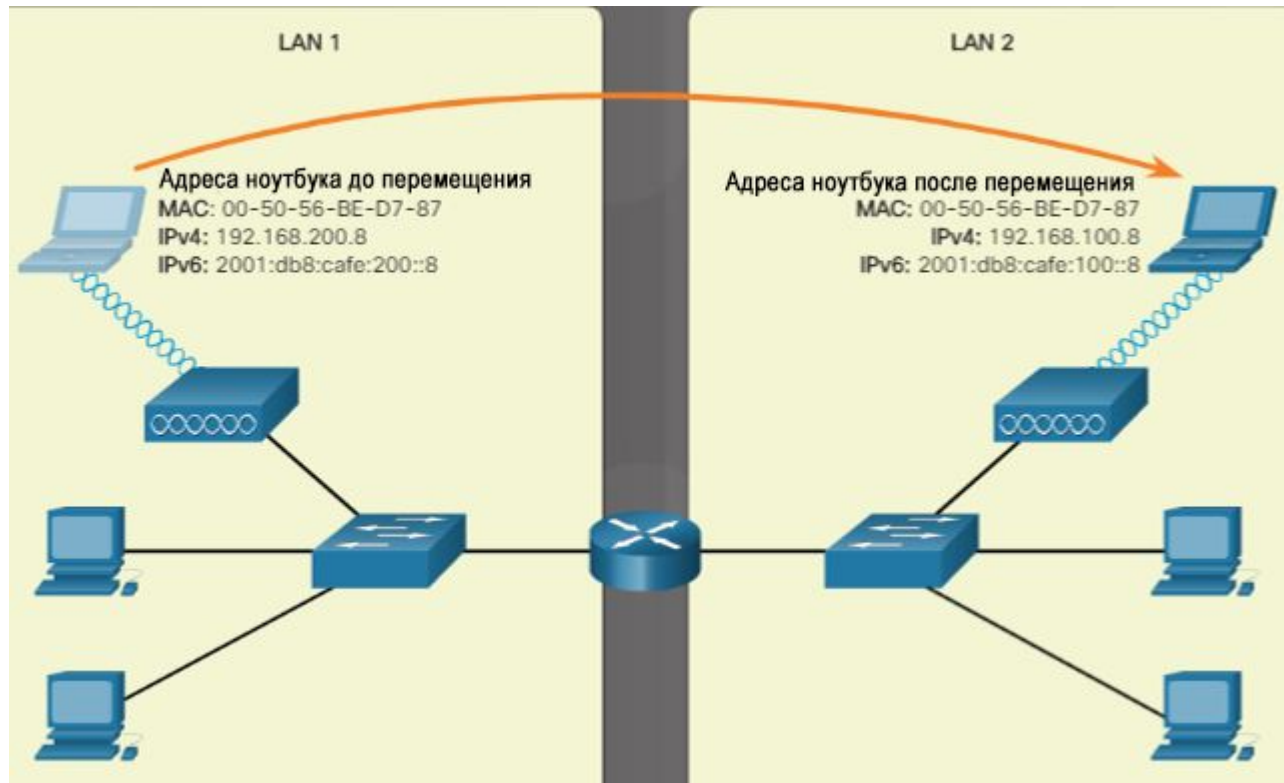
**2001:0db8:cafe:0200:0000:0000:0000:0008**

128 битов в сжатом формате

**2001:db8:cafe:200::8**

## Два сетевых адреса (продолжение)

- Когда ноутбук переносится в зону нахождения другой сети, MAC-адрес остается прежним, однако адреса IPv4 и IPv6 изменяются.
- MAC-адрес — это уникальное число, являющееся частью NIC.
- IP-адреса присваиваются компанией или Интернет-провайдером.



# Отображение адресов

Используйте переключатель /all с командой ipconfig, чтобы увидеть MAC-адрес (физический).

```
C:\> ipconfig /all
```

## Windows IP Configuration

```
Host Name . . . . . : ITEuser
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
```

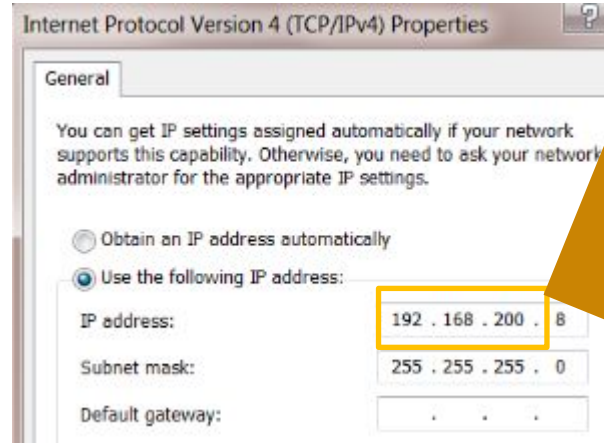
## Ethernet adapter Local Area Connection:

```
Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) PRO/1000 MT Network Connection
Physical Address. . . . . : 00-50-56-BE-D7-87
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : 2001:db8:cafe:200::8(Preferred)
Link-local IPv6 Address . . . . . : fe80::8cbf:a682:d2e0:98a%11(Preferred)
IPv4 Address. . . . . : 192.168.200.8(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 2001:db8:cafe:200::1
                            192.168.200.1
```

# Сетевая адресация

## Формат IPv4-адреса

- Две части IP-адреса:
  - Сеть
  - Хост
- Маска подсети определяет, какая часть адреса относится к сети.



Сетевая часть адреса,  
заданная маской подсети

	Часть, относящаяся к сети	Часть, относящаяся к хосту
192.168.200.8	11000000.10101000.11001000	.00001000
255.255.255.0	11111111.11111111.11111111	.00000000
192.168.200.0	11000000.10101000.11001000	.00000000

# Сетевая адресация

## Формат IPv6-адреса

### Правила:

- Пропустить начальные нули: 0db8 можно преобразовать в db8
- Пропустить все нулевые сегменты: использовать двойные двоеточия (::)

```
2001 : 0DB8 : 0000 : 1111 : 0000 : 0000 : 0000 : 0200
FE80 : 0000 : 0000 : 0000 : 0123 : 4567 : 89AB : CDEF
FF02 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0001
```

Полностью развернутый вид	2001:0db8:0000:1111:0000:0000:0000:0200
Без начальных нулей	2201: db8: 0:1111: 0: 0: 0: 200
Сжатый вид	2001:db8:0:1111::200

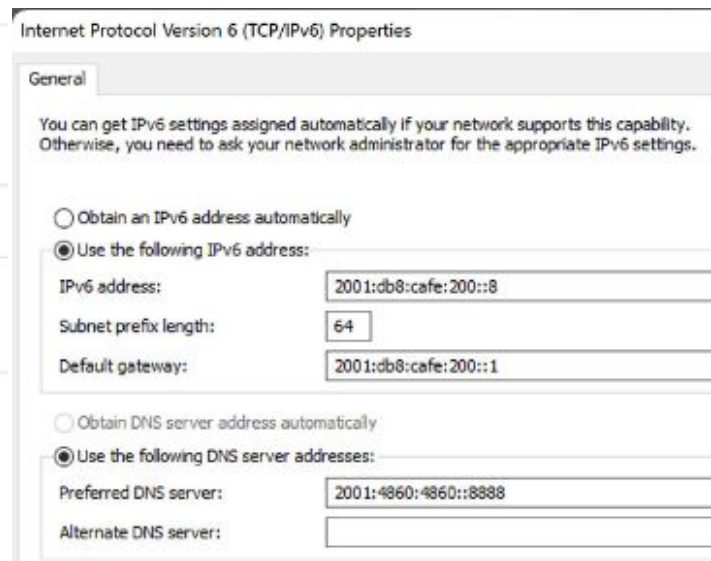
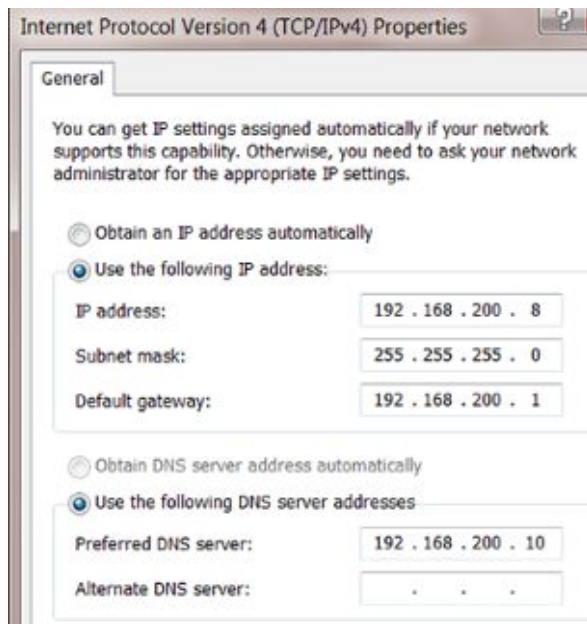
Полностью развернутый вид	fe80:0000:0000:0000:0123:4567:89ab:cdef
Без начальных нулей	fe80: 0: 0: 0: 123:4567:89ab:cdef
Сжатый вид	fe80::123:4567:89ab:cdef

Полностью развернутый вид	ff02:0000:0000:0000:0000:0000:0000:0001
Без начальных нулей	ff02: 0: 0: 0: 0: 0: 0: 1
Сжатый вид	ff02::1

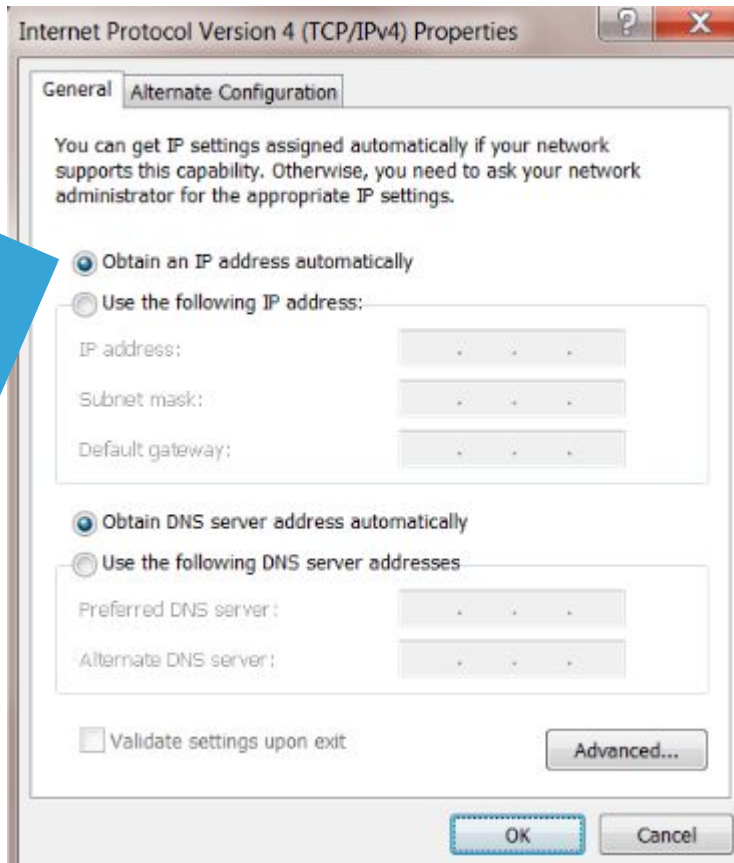
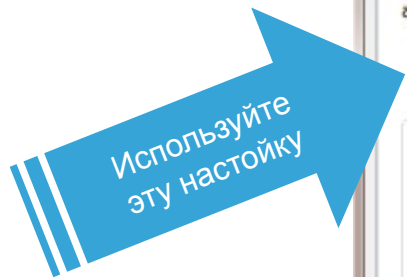
# Сетевая адресация

## Статическая адресация

- Сведения о статическом адресе необходимы для коммуникации с другими сетями и с Интернетом:
  - IP-адрес
  - Маска подсети
  - Шлюз, используемый по умолчанию (адрес маршрутизатора для возможности отправки информации в другие сети)
  - Сервер DNS (преобразует доменные имена или адреса URL в IP-адреса для удобства связи с удаленными веб-сайтами и устройствами)



# Динамическая адресация

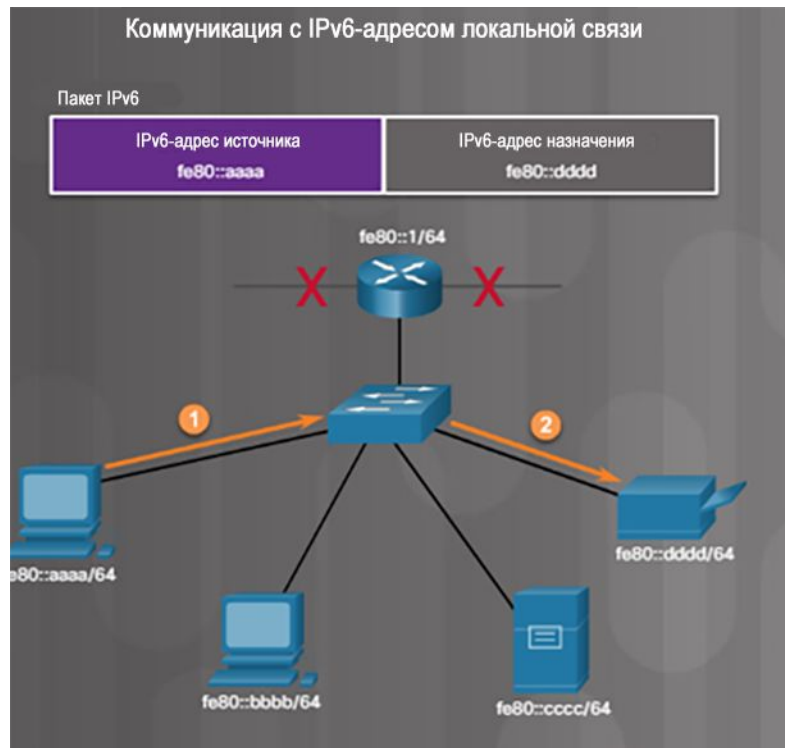


- Информация об IP-адресации поступает от сервера DHCP



# Адреса локальной связи IPv4 и IPv6

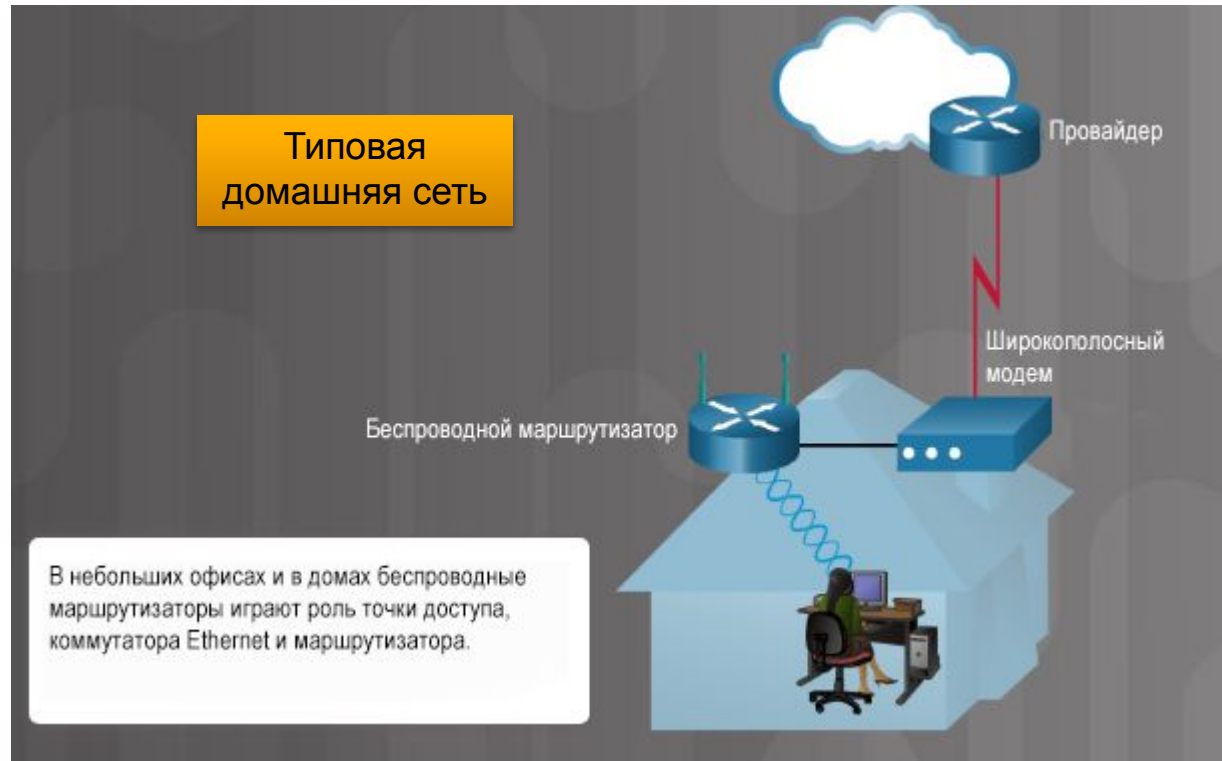
- Используются устройством IPv4, если это устройство не может получить IP-адрес IPv4.
- Устройство IPv6 всегда должно иметь динамический или настраиваемый вручную адрес локальной связи IPv6.



# Настройка платы NIC

## Компоновка сети

- Компоненты сети
- Компоновка сети



# Настройка платы NIC

## Выбор платы NIC



Проводная  
сеть Ethernet



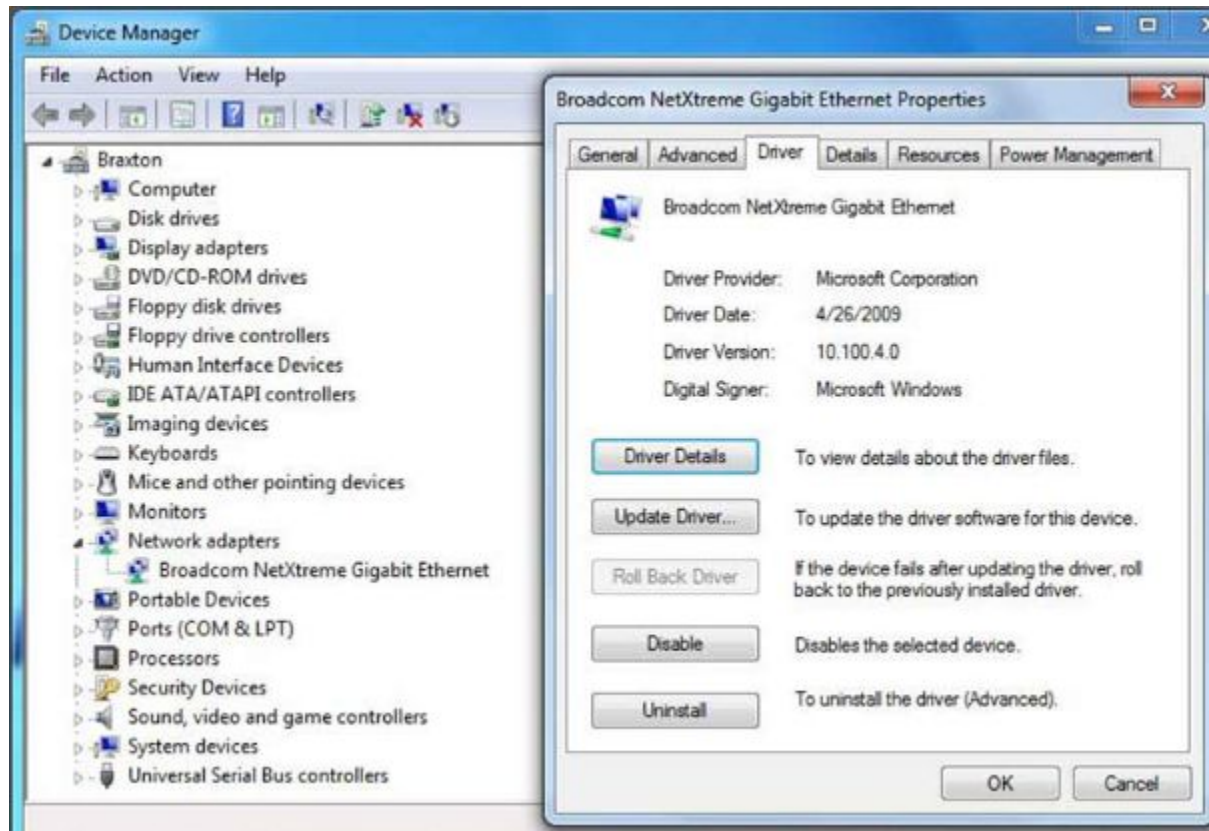
Беспроводная  
сеть Ethernet



Беспроводная  
сеть Ethernet

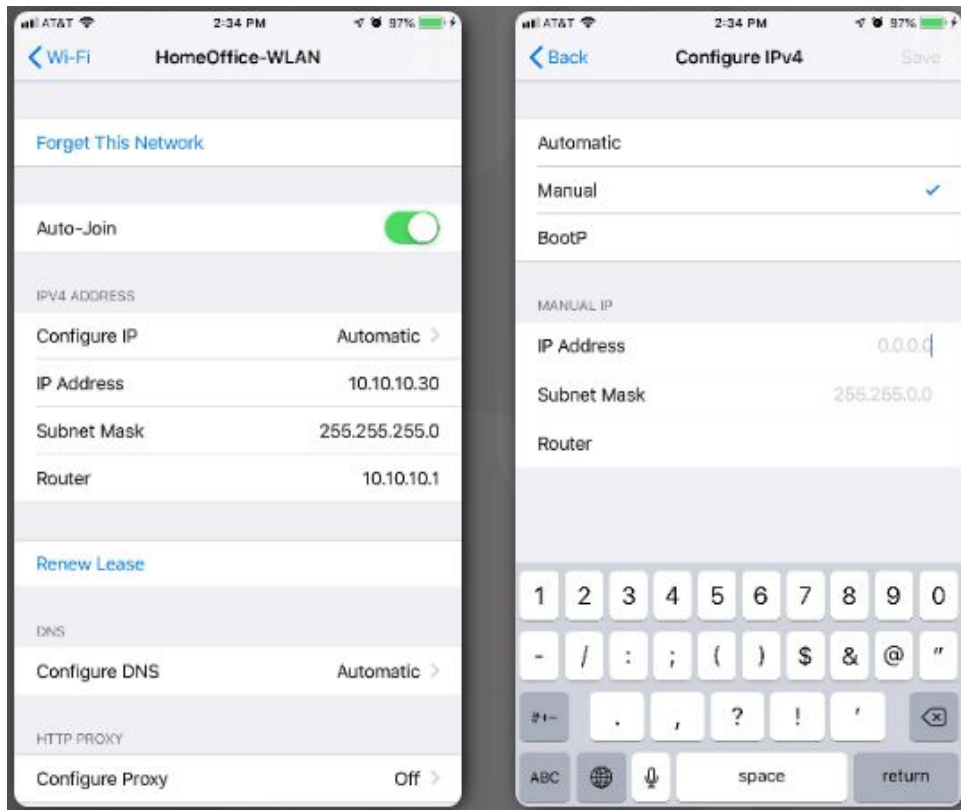
# Установка и обновление платы NIC

- При установке беспроводной платы NIC расположите антенну так, чтобы обеспечивался оптимальный охват.
- Используйте **Менеджер устройств** для просмотра сведений о драйвере:
  - Разверните категорию *Сетевые адаптеры*
  - Правой кнопкой мыши выберите конкретную NIC > *Свойства* или *Обновить драйвер*



# Настройка платы NIC

## Настройка платы NIC



- Беспроводным устройствам, включая смартфоны, также необходимы IP-адреса для подключения к беспроводной сети.

# Настройка платы NIC ICMP

## Опции переключателя команды эхо-запроса

- Протокол управляющих сообщений в Интернете (ICMP) используется для отправки управляющих сообщений и сообщений об ошибках.
- Команда **эхо-запроса** является частью ICMP.

```
C:\> ping cisco.com

Pinging e144.dscb.akamaiedge.net [23.200.16.170] with 32 bytes of data:
Reply from 23.200.16.170: bytes=32 time=25ms TTL=54
Reply from 23.200.16.170: bytes=32 time=26ms TTL=54
Reply from 23.200.16.170: bytes=32 time=25ms TTL=54
Reply from 23.200.16.170: bytes=32 time=25ms TTL=54

Ping statistics for 23.200.16.170:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 25ms, Maximum = 26ms, Average = 25ms
```

```
C:\> ping /?
```

```
Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
           [-r count] [-s count] [[-j host-list] | [-k host-list]]
           [-w timeout] [-R] [-S srcaddr] [-4] [-6] target_name
```

### Options:

-t	Ping the specified host until stopped. To see statistics and continue - type Control-Break; To stop - type Control-C.
-a	Resolve addresses to hostnames.
-n count	Number of echo requests to send.
-l size	Send buffer size.
-f	Set Don't Fragment flag in packet (IPv4-only).
-i TTL	Time To Live.
-v TOS	Type Of Service (IPv4-only. This setting has been deprecated and has no effect on the type of service field in the IP Header).
-r count	Record route for count hops (IPv4-only).
-s count	Timestamp for count hops (IPv4-only).
-j host-list	Loose source route along host-list (IPv4-only).
-k host-list	Strict source route along host-list (IPv4-only).
-w timeout	Timeout in milliseconds to wait for each reply.
-R	Use routing header to test reverse route also (IPv6-only).
-S srcaddr	Source address to use.
-4	Force using IPv4.
-6	Force using IPv6.

# Подключение проводных устройств к Интернету

Подключение устройства к домашней или небольшой офисной проводной сети:

1. Подсоедините к устройству кабель.
2. Подсоедините другой конец кабеля к коммутатору (желтый порт).
3. Подсоедините кабель между беспроводным маршрутизатором (синий порт) и широкополосным модемом.



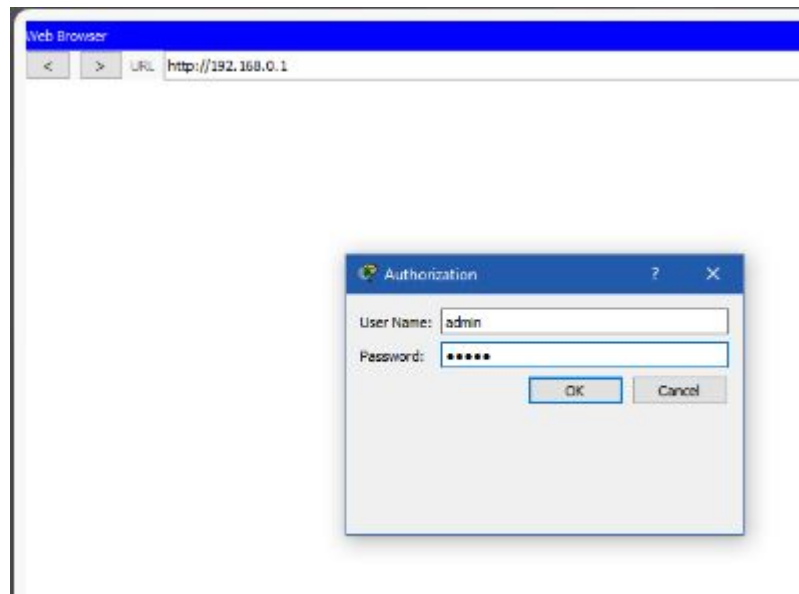
К модему

К компьютеру



# Вход в систему на маршрутизаторе

- Откройте браузер и введите IP-адрес маршрутизатора, заданный по умолчанию.
- Незамедлительно измените имя пользователя и пароль, заданные по умолчанию.





## Основные настройки сети

1. Войдите в систему маршрутизатора.
2. Измените пароль, заданный по умолчанию.
3. Выполните вход с новым паролем.
4. Задайте диапазон адресов DHCP.
5. Обновите IP-адреса на устройствах (выполните команды **ipconfig /release** и **ipconfig /renew**).
6. Измените IP-адрес, заданный по умолчанию, и выполните вход с новым IP-адресом.

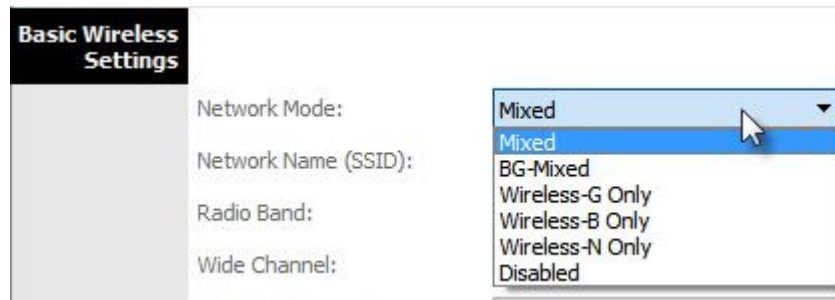
The screenshot shows a web browser window displaying the configuration page for a Wireless-N Broadband Router (WRT300N). The browser's address bar shows the URL `http://192.168.0.1/index.asp`. The page title is "Wireless-N Broadband Router" with the firmware version "v0.93.3". The navigation menu includes "Setup", "Wireless", "Security", "Access Restrictions", "Applications & Gaming", "Administration", and "Status". The "Setup" menu is expanded to show "Basic Setup", "DDNS", "MAC Address Clone", and "Advanced Routing". The "Internet Setup" section is active, showing "Automatic Configuration - DHCP" selected. Below this, there are fields for "Host Name", "Domain Name", and "MTU" (set to 1500). The "Network Setup" section shows the "Router IP" as 10.10.10.1 and the "Subnet Mask" as 255.255.255.0. The "DHCP Server" is set to "Enabled", and the "Start IP Address" is 192.168.0.100. A "DHCP Reservation" button is visible on the right side of the form.

# Настройка проводной и беспроводной сети

## Основные настройки сети

1. Проверьте настройки сети WLAN, заданные по умолчанию.
2. Измените сетевой режим.
3. Настройте SSID.
4. Настройте канал.
5. Настройте режим безопасности.
6. Задайте кодовую фразу.

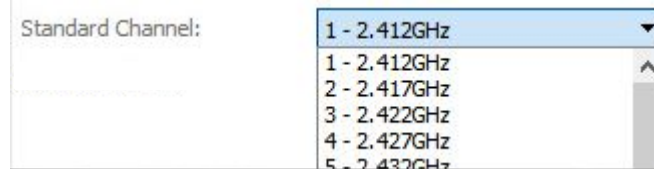
2.



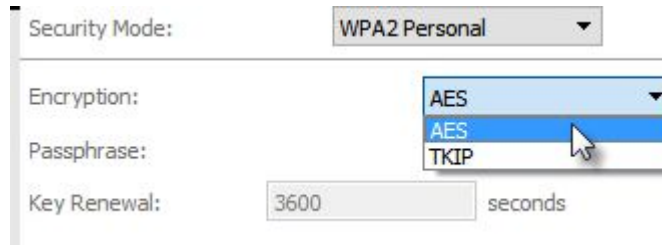
3.

Network Name (SSID):

4.



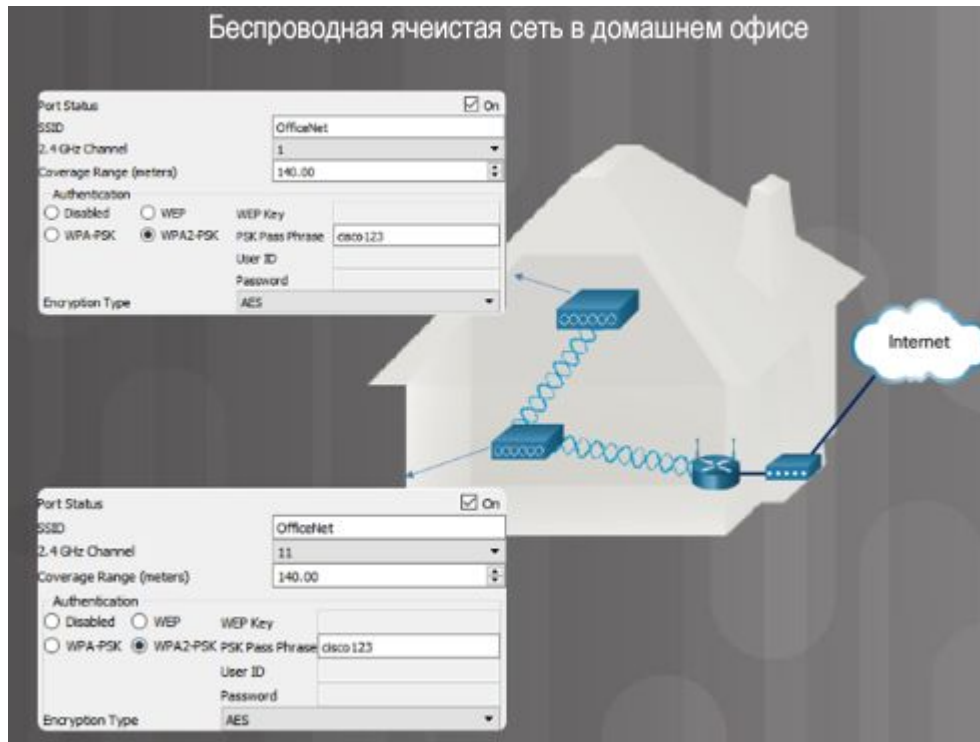
5.



6.

Passphrase:

## Настройка беспроводной ячеистой сети



# Настройка проводной и беспроводной сети

## NAT для IPv4

- Преобразование сетевых адресов (Network Address Translation, NAT) служит для конвертации частных адресов IPv4 в публичные адреса IPv4, маршрутизируемые в Интернете.



The screenshot shows a web browser window with the URL `http://10.10.10.1/status_router.asp`. The page title is "Wireless N Broadband Router". The navigation menu includes "Status", "Setup", "Wireless", "Security", and "Access Restrictions". The "Status" page is divided into two sections: "Router Information" and "Internet Connection".

Router Information	
Firmware Version:	v0.93.3
Current Time:	Not Available
Internet MAC Address:	000D.BDA5.3001
Host Name:	
Domain Name:	

Internet Connection	
Connection Type:	Automatic Configuration - DHCP
Internet IP Address:	209.165.201.11
Subnet Mask:	255.255.255.0
Default Gateway:	209.165.201.1
DNS 1:	64.100.0.100
DNS2:	
DNS3:	
MTU:	1500
DHCP Lease Time:	1 days 0:0:0

Buttons: IP Address Release, IP Address Renew

# Настройка проводной и беспроводной сети

## Качество обслуживания

- Настройка качества обслуживания (QoS) дает возможность установить приоритет для определенных типов трафика.

Basic Advanced Cancel Apply

Advanced Home

Setup

Internet Setup

Wireless Setup

LAN Setup

**QoS Setup**

Storage

Security

Administration

Advanced Setup

### QoS Setup

#	QoS Policy	Priority	Description
1	IP Phone	High	IP Phone applications
2	Counter Strike	High	Online Gaming Counter Strike
3	Netflix	High	Online Video Streaming Netflix
4	FTP	Medium	FTP Applications
5	WWW	Medium	WWW Applications
6	Gnutella	Low	Gnutella Applications
7	SMTP	Medium	SMTP Applications

Edit Delete Delete All

Add Priority Rule

# Настройки межсетевого экрана UPnP

- Настройка Universal Plug and Play (UPnP) ненадежна и создает риск нарушения безопасности.
- UPnP дает устройствам возможность динамически добавлять себя к беспроводной сети без вмешательства/конфигурации.

Allowed Remote Ip Address:

Any Ip Address

0 . 0 . 0 . 0 to 0

Remote Management Port: 8080

---

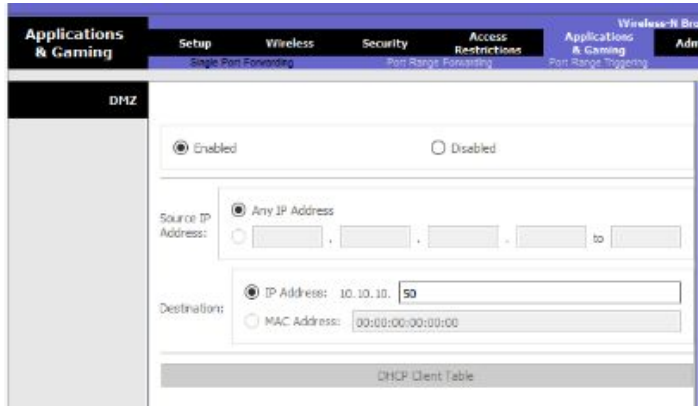
Upnp:  Enabled  Disabled

Allow Users to Configure:  Enabled  Disabled

Allow Users to Disable Internet Access:  Enabled  Disabled

# Настройки межсетевого экрана DMZ

- Демилитаризованная зона (DMZ) — это сеть, предоставляющая недоверенной сети доступ к службам.
- В DMZ часто находятся серверы.
- Некоторые беспроводные маршрутизаторы поддерживают создание DMZ.



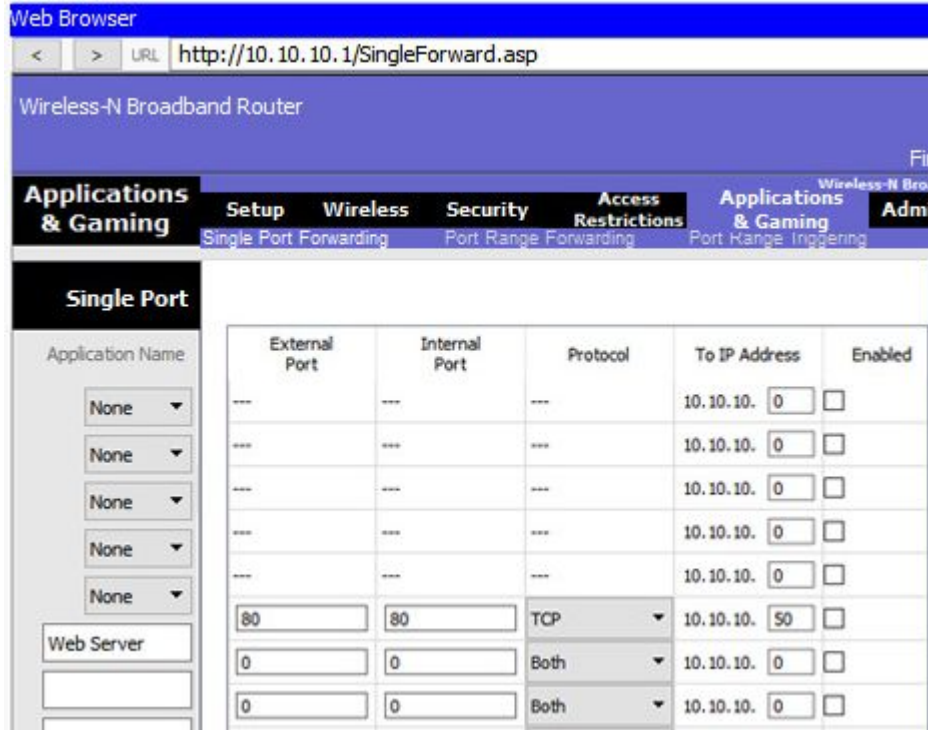
CISCO



# Настройки межсетевого экрана

## Переадресация портов

- Переадресация портов служит для отправки трафика на конкретные порты.
- Запуск портов дает возможность временно открыть межсетевой экран для передачи трафика на конкретные входящие порты/диапазон портов для поддержки работы приложения или игры.



Web Browser

URL: http://10.10.10.1/SingleForward.asp

Wireless-N Broadband Router

Applications & Gaming

Setup Wireless Security Access Restrictions Applications & Gaming

Single Port Forwarding Port Range Forwarding Port Range Forwarding

### Single Port

Application Name

None

None

None

None

None

Web Server

External Port	Internal Port	Protocol	To IP Address	Enabled
---	---	---	10.10.10. 0	<input type="checkbox"/>
---	---	---	10.10.10. 0	<input type="checkbox"/>
---	---	---	10.10.10. 0	<input type="checkbox"/>
---	---	---	10.10.10. 0	<input type="checkbox"/>
---	---	---	10.10.10. 0	<input type="checkbox"/>
80	80	TCP	10.10.10. 50	<input type="checkbox"/>
0	0	Both	10.10.10. 0	<input type="checkbox"/>
0	0	Both	10.10.10. 0	<input type="checkbox"/>



# Настройки межсетевых экранов

## Фильтрация MAC-адресов

- Фильтрация MAC-адресов применяется, чтобы задать MAC-адреса, допустимые в беспроводной сети.

В настройках беспроводного маршрутизатора слева MAC-адреса пока не внесены в список фильтрации MAC-адресов.

Wireless MAC Filter

Enabled  Disabled

Prevent PCs listed below from accessing the wireless network

Permit PCs listed below to access wireless network

Wireless Client List

MAC 01:	00:00:00:00:00:00	MAC 26:	00:00:00:00:00:00
MAC 02:	00:00:00:00:00:00	MAC 27:	00:00:00:00:00:00
MAC 03:	00:00:00:00:00:00	MAC 28:	00:00:00:00:00:00
MAC 04:	00:00:00:00:00:00	MAC 29:	00:00:00:00:00:00
MAC 05:	00:00:00:00:00:00	MAC 30:	00:00:00:00:00:00
MAC 06:	00:00:00:00:00:00	MAC 31:	00:00:00:00:00:00
MAC 07:	00:00:00:00:00:00	MAC 32:	00:00:00:00:00:00
MAC 08:	00:00:00:00:00:00	MAC 33:	00:00:00:00:00:00
MAC 09:	00:00:00:00:00:00	MAC 34:	00:00:00:00:00:00
MAC 10:	00:00:00:00:00:00	MAC 35:	00:00:00:00:00:00

## Формирование белых и черных списков

- **Белый список** разрешает пользователям, например, детям или сотрудниками, доступ к конкретным IP-адресам.
- **Черный список** служит для блокировки известных веб-сайтов.

The screenshot shows the 'Internet Access Policy' configuration page in a Cisco router's web interface. The page is divided into several sections:

- Access Policy:** A dropdown menu showing '10' and buttons for 'Delete This Entry' and 'Summary'.
- Enter Policy Name:** A text field containing 'Whitelist'.
- Status:** Radio buttons for 'Enabled' (selected) and 'Disabled'.
- Applied PCs:** An 'Edit List' button and a note: '(This Policy applies only to PCs on the List.)'
- Access Restriction:** Radio buttons for 'Deny' and 'Allow' (selected).
- Schedule:** A section for 'Internet access during selected days and hours.' It includes:
  - Days:** Checkboxes for 'EveryDay' (checked), 'Sun', 'Mon', 'Tue', 'Wed', 'Thu', 'Fri', and 'Sat'.
  - Times:** Radio buttons for '24Hours' (selected) and a time range selector (12 AM : 00 to 12 AM : 00).
- Website Blocking by URL Address:** Four text fields labeled 'URL 1:', 'URL 2:', 'URL 3:', and 'URL 4:'.
- Keyword:** Two text fields labeled 'Keyword 1:' and 'Keyword 2:'.

# Настройка устройств IoT

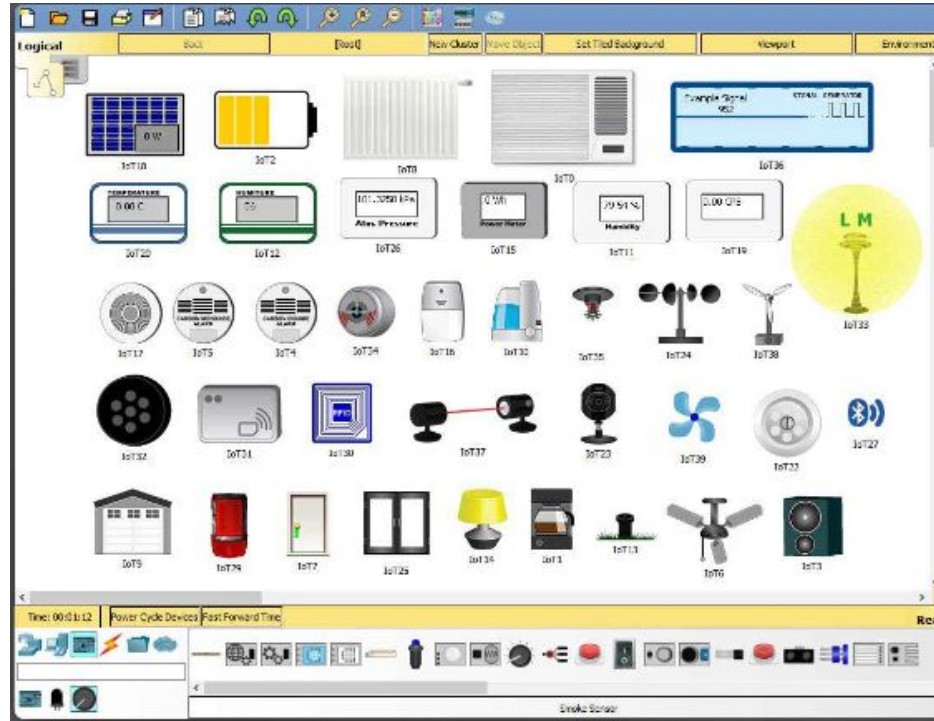
## Интернет вещей

- Интернет вещей (IoT) может подключаться к существующей сети или к собственной сети.
- Устройства IoT используются в умных домах.



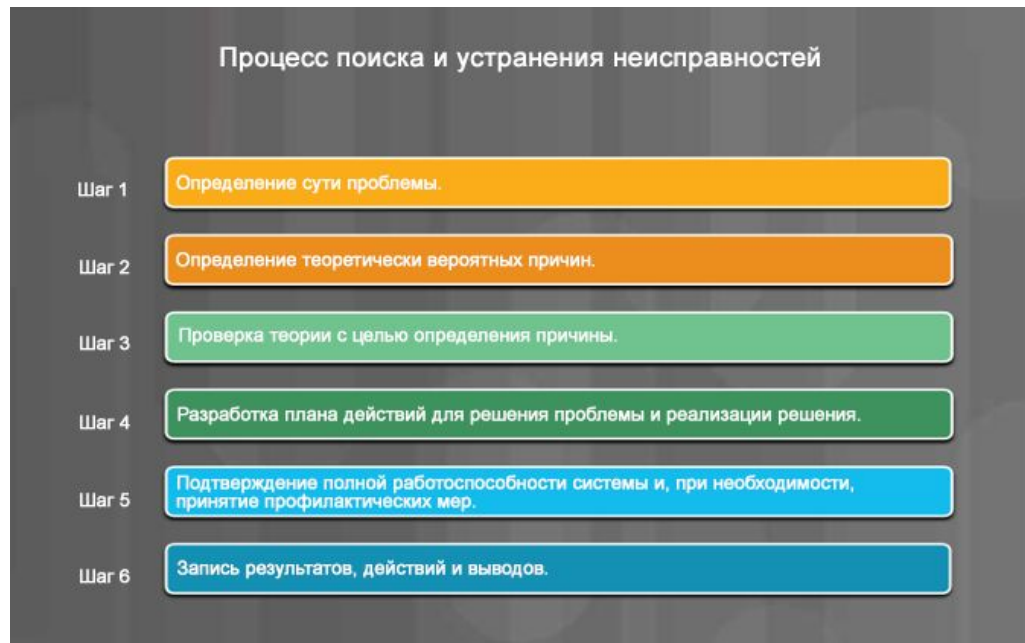
# Настройка устройств IoT

## Устройства IoT в Packet Tracer



## 6.2. Процесс поиска и устранения неисправностей

# Процесс поиска и устранения неисправностей



## Шесть этапов поиска и устранения неисправностей в работе сетей. Этап 1

Этап 1. Определить суть проблемы.	
Открытые вопросы	<ul style="list-style-type: none"><li>• Какие проблемы с устройством вы испытываете?</li><li>• Какое ПО было недавно установлено на устройстве?</li><li>• Какие действия вы выполняли, когда была обнаружена проблема?</li><li>• Какие сообщения об ошибках вы получали?</li><li>• Какое сетевое соединение использует устройство?</li></ul>
Закрытые вопросы	<ul style="list-style-type: none"><li>• Кто-нибудь еще пользовался недавно вашим устройством?</li><li>• Видите ли вы файлы или принтеры, открытые для общего доступа?</li><li>• Вы недавно меняли пароль?</li><li>• Можете ли вы войти в Интернет?</li><li>• В данный момент вы находитесь в сети?</li><li>• Возникла ли такая же проблема у кого-то еще?</li><li>• Происходили ли любые изменения во внешней среде или в инфраструктуре сети?</li></ul>

Проблемы в работе сетей могут быть простыми или сложными и бывают обусловлены разными факторами, связанными с аппаратным обеспечением, ПО и сбоями соединений. Будучи техническим специалистом, вы должны применять логический и последовательный подход для диагностирования сети, поочередно устраняя проблемы.

Например, чтобы оценить характер проблемы, выясните, на каком количестве устройств она возникла. Если проблема затрагивает только одно устройство, начните с него. Если проблема затрагивает все устройства, начните поиск и устранение неисправностей в помещении, в котором находятся все подключенные сетевые устройства.

Первый этап процесса поиска и устранения неисправностей — это определение сути проблемы. Используйте приведенные выше открытые и закрытые вопросы, чтобы получить информацию от клиента.

# Шесть этапов поиска и устранения неисправностей в работе сетей. Этап 2

Этап 2. Предположить, какова вероятная причина.	
Типовые причины неисправностей в работе сетей	<ul style="list-style-type: none"><li>• Неплотно присоединены кабели</li><li>• Неправильно установлена NIC</li><li>• Не работает Интернет-провайдер</li><li>• Низкая мощность беспроводного сигнала</li><li>• Недействительный IP-адрес</li><li>• Сбой в работе сервера DNS</li><li>• Сбой в работе сервера DHCP</li></ul>
<p>Поговорив с клиентом, вы сможете предположить, какова вероятная причина. В списке перечислены возможные причины проблем в работе сетей.</p>	



## Шесть этапов поиска и устранения неисправностей в работе сетей. Этап 3

### Этап 3. Проверить предположения, чтобы определить причину.

Стандартные шаги для определения причины:

- Проверить правильность подсоединения всех кабелей.
- Отсоединить и снова подсоединить кабели и разъемы.
- Перезагрузить компьютер или сетевое устройство.
- Войти в систему под именем другого пользователя.
- Восстановить или перезагрузить сетевое соединение.
- Обратиться к администратору сети.
- Отправить эхо-запрос на шлюз устройства, заданный по умолчанию.
- Попробовать открыть удаленную веб-страницу, например, <http://www.cisco.com>.

Сделав предположения относительно характера и причин неисправности, проверьте их, чтобы выяснить реальную причину. В списке выше описан ряд быстрых способов, которыми можно воспользоваться для уточнения причины проблемы и даже для ее устранения. Если быстрая процедура не помогла устранить проблему, возможно, потребуется выполнить полную функциональную проверку системы или дополнительно проанализировать проблему, чтобы точно определить ее причину.

## Шесть этапов поиска и устранения неисправностей в работе сетей. Этап 4

### Этап 4. Разработать план действий для решения проблемы и применить решение на практике.

Если способ решения проблемы не найден на предыдущем шаге, необходимо углубленное исследование.

- Журналы ремонтных работ службы поддержки.
- Опрос других технических специалистов.
- Веб-сайты изготовителей с ответами на часто задаваемые вопросы.
- Технические веб-сайты.
- Группы новостей.
- Руководства по эксплуатации компьютеров.
- Руководства по эксплуатации устройств.
- Веб-форумы.
- Поиск в Интернете.

Определив точную причину проблемы, разработайте план действий по ее устранению и по внедрению практического решения. Выше указаны источники дополнительной информации, которыми вы можете воспользоваться.

# Шесть этапов поиска и устранения неисправностей в работе сетей. Этап 5

Этап 5. Проверить работоспособность системы и, если применимо, принять профилактические меры.	
Подтвердите, что система полностью работоспособна и, если применимо, примите профилактические меры.	<ul style="list-style-type: none"><li>• Используйте команду <b>ipconfig /all</b>, чтобы отобразить информацию об IP-адресах всех сетевых адаптеров.</li><li>• Используйте команду <b>ping</b>, чтобы проверить сетевые подключения. Эта команда отправит пакет на указанный адрес и покажет полученный ответ.</li><li>• Убедитесь, что устройство имеет доступ к авторизованным ресурсам, например, почтовым серверам компании, и к Интернету.</li><li>• Воспользуйтесь дополнительными командами или спросите руководителя, какими еще программами тестирования вы можете воспользоваться.</li></ul>
Устранив проблему, подтвердите полную работоспособность системы и, если применимо, примите профилактические меры. Действия по проверке решения перечислены выше.	

# Шесть этапов поиска и устранения неисправностей в работе сетей. Этап 6

<b>Этап 6. Задокументировать полученные данные, выполненные действия и результаты.</b>	
Задокументируйте полученные данные, выполненные действия и результаты.	<ul style="list-style-type: none"><li>• Обсудите примененное решение с клиентом.</li><li>• Попросите клиента убедиться в том, что проблема устранена.</li><li>• Предоставьте клиенту всю документацию.</li><li>• Задокументируйте действия, выполненные для решения проблемы, в заказе на обслуживание и в журнале технических работ.</li><li>• Задокументируйте все компоненты, которые использовались при ремонте.</li><li>• Задокументируйте время, которое потребовалось, чтобы решить проблему.</li></ul>
<p>На последнем шаге процесса запишите все результаты, действия и выводы в соответствии со списком.</p>	

## Типовые проблемы при работе с сетью и их решение

Определение характера проблемы

**Не горят светодиоды сетевой платы NIC.**

Пользователь не может использовать протокол защищенной оболочки (SSH) для доступа к удаленному устройству.

Устройство не может обнаружить беспроводной маршрутизатор.

IPv4-адрес компьютера под управлением Windows — 169.254.x.x.

Удаленное устройство не отвечает на эхо-запрос.

Пользователь может входить в локальную сеть, но не может выйти в Интернет.

Сеть работает нормально, но беспроводное устройство не может к ней подключиться.

Недоступны локальные ресурсы, например, принтеры или файлообменники.

### Не горят светодиоды сетевой платы NIC.

Вероятные причины	Возможные решения
<ul style="list-style-type: none"><li>Сетевой кабель отсоединен или поврежден.</li></ul>	<ul style="list-style-type: none"><li>Подключите кабель к компьютеру или замените кабель.</li></ul>
<ul style="list-style-type: none"><li>Сетевая плата повреждена.</li></ul>	<ul style="list-style-type: none"><li>Замените сетевую плату.</li></ul>

Показать PDF

# Сложные проблемы с сетевыми подключениями и их решение

### Определение характера проблемы

Устройство может подключиться к сетевому устройству по IP-адресу, но не может подключиться по имени хоста.

Устройство не получает или не обновляет IP-адрес в сети.

При подключении устройства к сети появляется сообщение о конфликте IP-адресов.

Устройство имеет доступ к сети, но не может выйти в Интернет.

Пользователи жалуются на медленную скорость передачи данных, слабый сигнал и перебои с подключением к беспроводной сети.

### Устройство может подключиться к сетевому устройству по IP-адресу, но не может подключиться по имени хоста.

Вероятные причины	Возможные решения
Некорректное имя хоста.	Введите имя хоста еще раз.
Некорректные настройки DNS.	Введите IP-адрес сервера DNS еще раз.
Сервер DNS не функционирует.	Перезапустите сервер DNS.

Показать PDF

# Сложные проблемы при подключении к FTP и безопасном подключении к Интернету и их решение

Определение характера проблемы

Пользователь не может войти на FTP-сервер.

Клиентское ПО FTP не может найти FTP-сервер.

Устройство не может зайти на конкретный сайт HTTPS.

**Пользователь не может войти на FTP-сервер.**

Вероятные причины	Возможные решения
FTP блокируется межсетевым экраном на маршрутизаторе.	Убедитесь, что порты 20 и 21 разрешены на межсетевом экране для выходного трафика маршрутизатора.
FTP блокируется межсетевым экраном Windows.	Убедитесь, что порты 20 и 21 разрешены на межсетевом экране для выходного трафика Windows.
Достигнуто максимальное количество пользователей.	Увеличьте максимальное количество одновременно работающих пользователей FTP на FTP-сервере.

Показать PDF

## Сложные проблемы и их решение с помощью сетевых инструментов

### Определение характера проблемы

Устройство в одной сети не может отправить эхо-запрос на устройство в другой сети.

Компьютер не может установить соединение Telnet с удаленным компьютером.

Команда nslookup выдает сообщение: "Can't find server name for address {ip-address}: timed out", where ip-address... (Не получается найти имя сервера для адреса ip-адрес: время сеанса истекло), где ip-address может быть любым IP-адресом)

Как результат выполнения команды ipconfig /release или ipconfig /renew отображается следующее сообщение: "No operation can be performed..."

Как результат выполнения команды ipconfig /release или ipconfig /renew отображается следующее сообщение: "The operation failed as no adapter is..."

### Устройство в одной сети не может отправить эхо-запрос на устройство в другой сети.

Вероятные причины	Возможные решения
Связь между двумя сетями нарушена.	С помощью трассировки определите, где нарушена связь, и устраните это нарушение.
На маршрутизаторе заблокирован протокол Internet Control Message Protocol (ICMP).	Настройте маршрутизатор так, чтобы он разрешал отправку и получение эхо-запросов по протоколу ICMP.
ICMP блокируется на межсетевом экране Windows.	Настройте межсетевой экран Windows так, чтобы он разрешал отправку и получение эхо-запросов по протоколу ICMP.

Показать PDF



## Новые термины и команды

- |  |  |
|--|--|
| <ul style="list-style-type: none"><li>• MAC-адрес</li><li>• IPv4-адрес</li><li>• IPv6-адрес</li><li>• Статический адрес</li><li>• Динамический адрес</li><li>• Адрес локальной связи</li><li>• ICMP</li><li>• DHCP</li><li>• Преобразование сетевых адресов (NAT) для IPv4</li><li>• QoS</li></ul> | <ul style="list-style-type: none"><li>• Межсетевой экран</li><li>• UPnP</li><li>• DMZ</li><li>• Переадресация портов</li><li>• Запуск портов</li><li>• Фильтрация MAC-адресов</li><li>• Белый список</li><li>• Черный список</li><li>• IoT</li></ul> |
|--|--|

