

Лабораторная работа. Поиск и устранение неполадок с помощью сетевых служебных программ

Цели

- Интерпретируйте выходные данные для наиболее часто используемых сетевых служебных программ командной строки.
- Определите, какие сетевые служебные программы могут предоставить необходимые сведения для выполнения действий в рамках восходящей стратегии поиска и устранения неполадок.

Исходные данные/сценарий

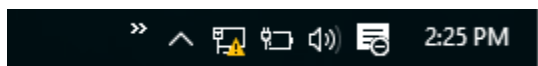
Существует целый ряд неполадок, которые могут вызвать проблемы с сетевыми подключениями. В этой лабораторной работе вы будете использовать сетевые служебные программы, которые помогают выявлять проблемы с подключениями в беспроводных сетях. Сетевые служебные программы командной строки также применяются для выявления проблем с подключениями в проводных сетях.

Необходимые ресурсы:

- компьютер с установленной ОС Windows 10;
- установленная беспроводная сетевая плата;
- установленная сетевая плата Ethernet;
- беспроводной маршрутизатор;
- Подключение к Интернету.

Шаг 1: Подключение к беспроводной сети.

- Отсоедините кабель Ethernet от компьютера. Над значком «Подключения» загорится оранжевый треугольник.

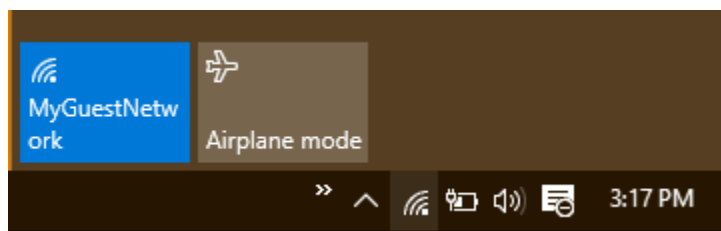


- Щелкните значок «Подключения» на панели задач. Назовите имя доступного беспроводного соединения.

- Нажмите одно из доступных беспроводных соединений. Подключитесь к сети. При необходимости введите учетные данные для входа в систему. Убедитесь в том, что подключение выполнено успешно.



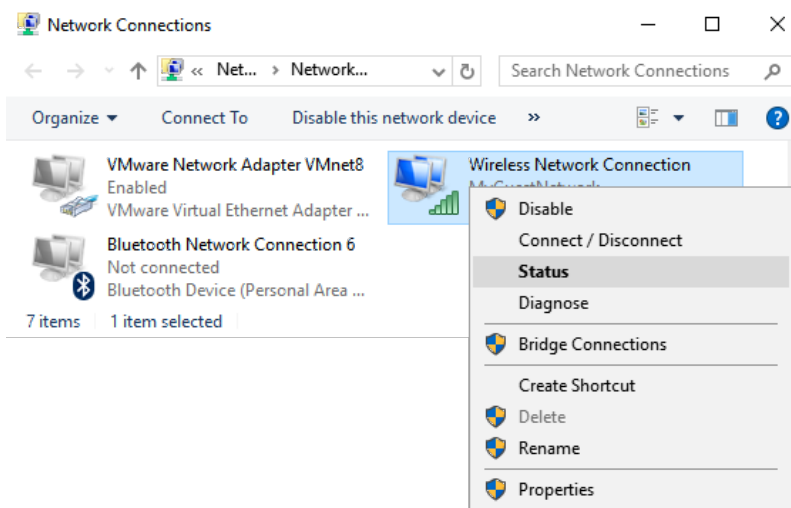
- Убедитесь в том, что подключение выполнено успешно.



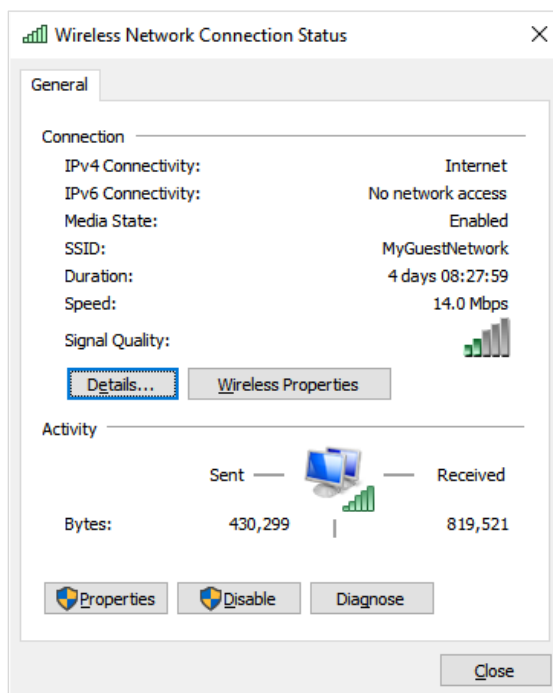
Шаг 2: Убедитесь в работоспособности сетевого адаптера.

При получении уведомления о проблемах с подключением первым действием в рамках восходящей стратегии поиска и устранения неполадок станет определение работоспособности сетевой интерфейсной платы (NIC) и проверка параметров операционной системы.

- Откройте «Панель управления», выберите элемент **Центр управления сетями и общим доступом**. Щелкните правой кнопкой мыши кнопку **Пуск** и выберите **Панель управления**. Нажмите **Центр управления сетями и общим доступом**. Щелкните кнопку **Изменить параметры сетевого адаптера**.
- Выберите пункт «Беспроводное сетевое соединение». Щелкните правой кнопкой мыши сетевой адаптер и выберите в меню пункт **Состояние**. Если пункт **Состояние** неактивен, это означает, что сетевой адаптер не включен или не подключен к беспроводному идентификатору SSID.



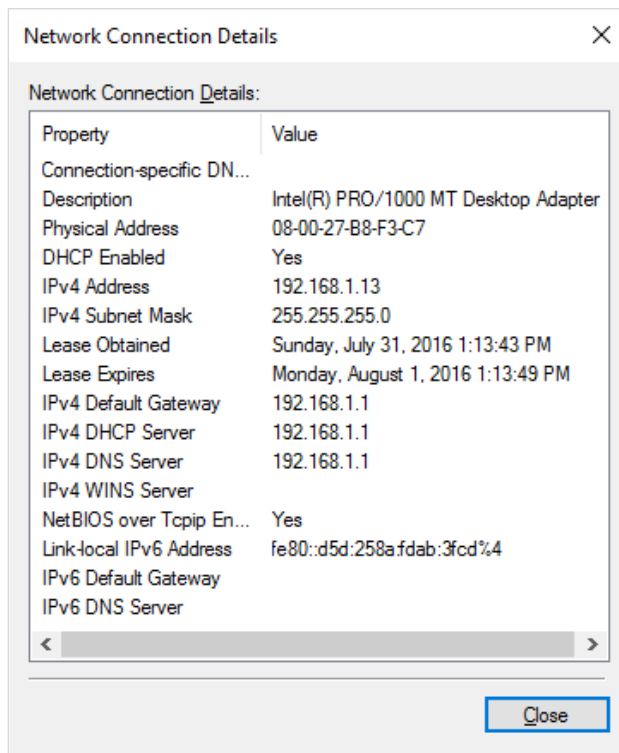
- При открытии окна состояния убедитесь в том, что беспроводное соединение включено и указан верный идентификатор SSID. Щелкните кнопку **Сведения** для открытия окна со сведениями о сетевом адаптере.



- d. Окно «Сведения о сетевом адаптере» содержит информацию о текущих настройках IP для выбранного сетевого адаптера. Это окно содержит сведения о конфигурациях IPv4 и IPv6. Если включен сервер DHCP, то в этом окне также отображаются сведения об аренде IP-адресов.

Включен ли сервер DHCP на этом компьютере? _____

Когда истекает срок аренды IP-адресов DHCP? _____



Шаг 3: Подтвердите конфигурацию IP-адреса.

- a. Откройте окно командной строки. Щелкните правой кнопкой мыши кнопку **Пуск** и выберите **командную строку**.
- b. Введите **ping 127.0.0.1**. Вместо IP-адреса 127.0.0.1 также можно указывать имя localhost. Успешная отправка ping-запроса на локальный хост-компьютер свидетельствует о том, что на компьютере работает стек протоколов TCP/IP. Если локальный хост-компьютер не отвечает на команду ping-запроса, возможно, возникли неполадки с драйвером устройства или платой сетевого интерфейса.

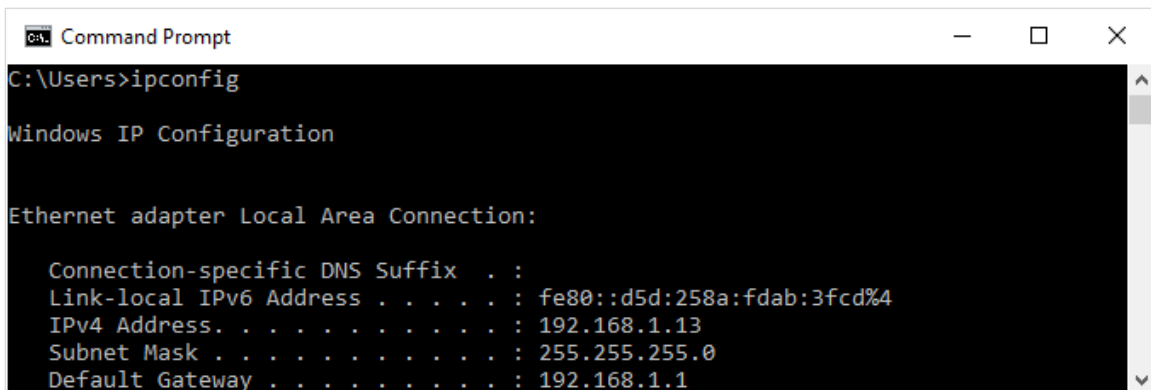
```
cmd Command Prompt
C:\Users>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Проверка связи с помощью команды **ping** выполнена успешно? _____

- с. Введите команду **ipconfig**. Определите полученный IP-адрес, маску подсети и основной шлюз для этого компьютера.



```
C:\Users>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::d5d:258a:fdab:3fcd%4
    IPv4 Address. . . . . : 192.168.1.13
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1
```

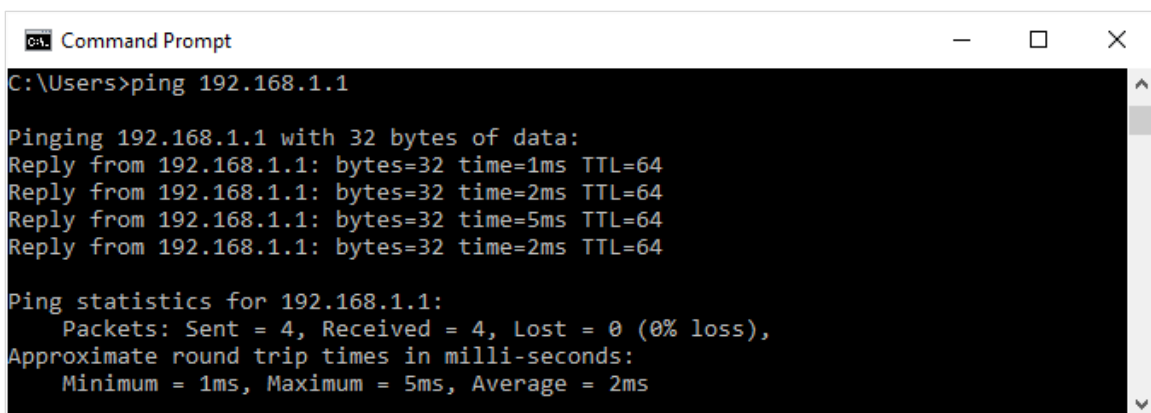
В случае, если адрес IPv4 хоста принадлежит сети 169.254.0.0/16, это значит, что компьютер получил конфигурацию IP-адреса с помощью функции автоматического назначения частных IP-адресов (APIPA) операционной системы Windows.

Какие неполадки может вызвать получение IP-адреса компьютера с помощью функции автоматического назначения частных IP-адресов (APIPA)?

Если компьютеру был присвоен IP-адрес с помощью функции автоматического назначения частных IP-адресов (APIPA), это означает, что возникли неполадки с сервером DHCP. Если беспроводной маршрутизатор предоставляет службы DHCP, убедитесь, что служба DHCP настроена правильно, а диапазон существующих IP-адресов достаточен для размещения всех устройств, которые могут подключаться по беспроводной сети.

Какой IP-адрес для основного шлюза назначен на вашем компьютере? _____

Чтобы проверить связь ПК с основным шлюзом по сети, выполните команду **ping** для IP-адреса основного шлюза.



```
C:\Users>ping 192.168.1.1

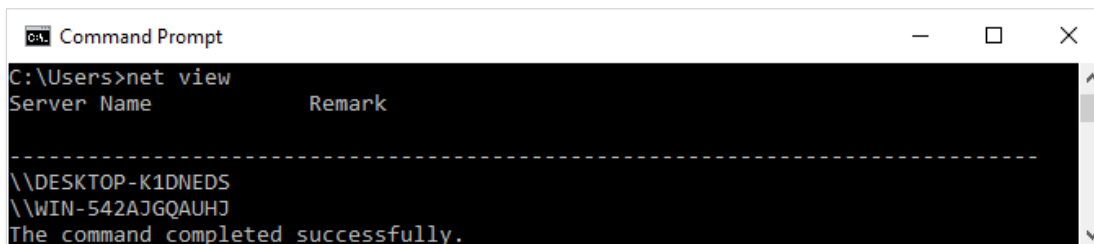
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Reply from 192.168.1.1: bytes=32 time=5ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 5ms, Average = 2ms
```

Успешный результат проверки связи означает, что подключение между компьютером и основным шлюзом установлено.

В случае если команда **ping** не была выполнена успешно, убедитесь, что IP-адрес шлюза по умолчанию был введен верно, а беспроводное подключение включено.

- d. Введите команду **net view**. При выполнении команды **net view** на ПК под управлением операционной системы Windows отображается список имен компьютеров или других устройств Windows в вашей рабочей группе или домене. Если после введения команды **net view** отображается список имен компьютеров, это означает, что ваш ПК способен успешно отправлять и принимать сообщения по сети.



```
Command Prompt
C:\Users>net view
Server Name          Remark
-----
\\DESKTOP-K1DNEDS
\\WIN-542AJGQAUHJ
The command completed successfully.
```

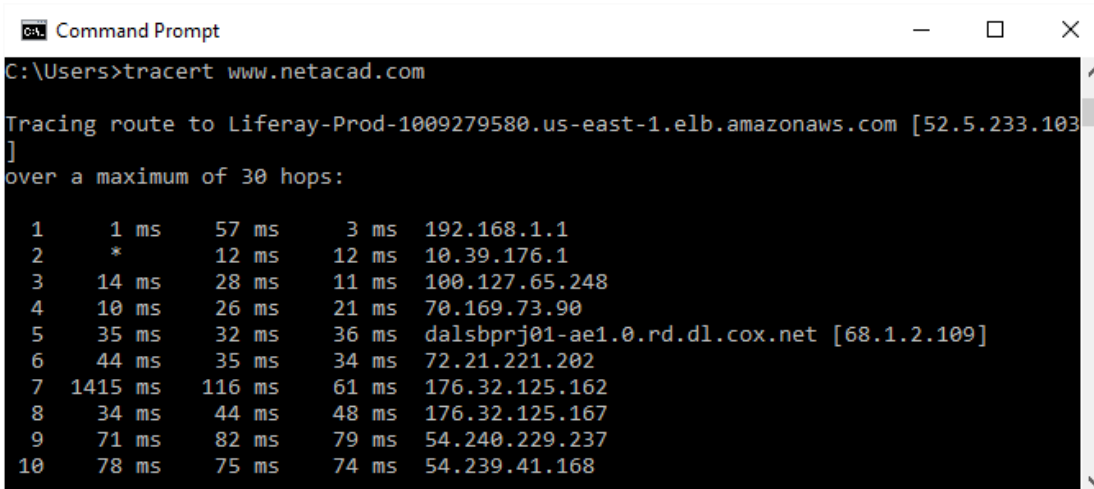
Перечислите полученные имена компьютеров.

Примечание. В зависимости от конфигурации компьютеров в вашей лабораторной работе, после введения команды **net view** список имен компьютеров может не отображаться или появиться сообщение об ошибке. В этом случае переходите к выполнению следующего шага.

Шаг 4: Проверьте внешнее подключение.

Если вы используете внешнее подключение, используйте следующие методы для проверки работоспособности основного шлюза и службы DNS.

- a. Команда **tracert** в ОС Windows служит для выполнения тех же функций, что и команда **traceroute**, используемая в Cisco IOS. Введите команду **tracert** вместе с URL-адресом веб-сайта вашего учебного заведения или веб-сайта Сетевой академии Cisco. Пример. Введите **tracert www.netacad.com**. **Примечание.** Некоторые выходные данные опущены.



```
Command Prompt
C:\Users>tracert www.netacad.com

Tracing route to LiferaY-Prod-1009279580.us-east-1.elb.amazonaws.com [52.5.233.103]
over a maximum of 30 hops:

  0  0 ms  0 ms  0 ms  192.168.1.1
  1  1 ms  57 ms  3 ms  192.168.1.1
  2  *      12 ms  12 ms  10.39.176.1
  3  14 ms  28 ms  11 ms  100.127.65.248
  4  10 ms  26 ms  21 ms  70.169.73.90
  5  35 ms  32 ms  36 ms  dalsbprj01-ae1.0.rd.dl.cox.net [68.1.2.109]
  6  44 ms  35 ms  34 ms  72.21.221.202
  7  1415 ms  116 ms  61 ms  176.32.125.162
  8  34 ms  44 ms  48 ms  176.32.125.167
  9  71 ms  82 ms  79 ms  54.240.229.237
 10  78 ms  75 ms  74 ms  54.239.41.168
```

Команда **tracert** отображает путь пакета, перемещаемого между IP-адресами источника и назначения. После ввода команды **tracert** все маршрутизаторы, через которые пакет проходит к IP-адресу назначения, отображаются в выходных данных в виде переходов. В случае неполадок в сети процесс отображения выходных данных после ввода команды **tracert** остановится на последнем удачном переходе. Первый переход в выходных данных — это основной шлюз компьютера-источника, а последний переход — это IP-адрес компьютера-назначения, если команда **tracert** была выполнена успешно.

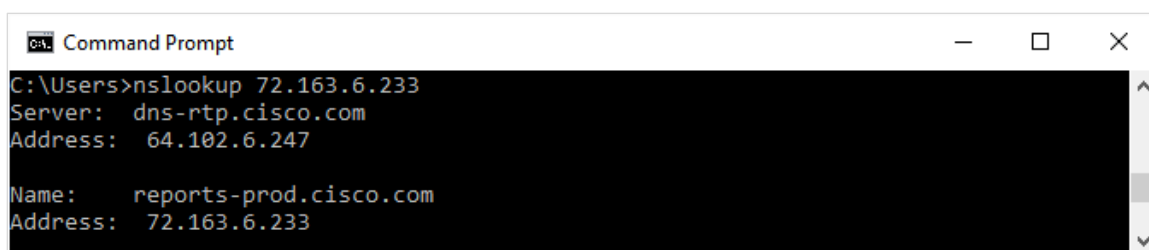
- b. Команда **tracert** использует настроенный сервер DNS для преобразования полного имени домена в IP-адрес перед началом отслеживания маршрутизатора до места назначения. Использование команд **tracert** или **ping** с доменным именем вместо IP-адреса может подтвердить тот факт, что служба DNS обеспечивает разрешение имен.

Какой IP-адрес был возвращен сервером DNS? _____

Что произойдет, если сервер DNS не сможет преобразовать доменное имя сервера?

- c. Введите команду **nslookup** с полученным IP-адресом. **Nslookup** — это сетевая служебная программа, предназначенная для решения проблем, связанных с сервером DNS.

Введите **nslookup 72.163.6.233**. IP-адрес в этом примере назначен серверу Cisco Systems. Какое доменное имя было возвращено?



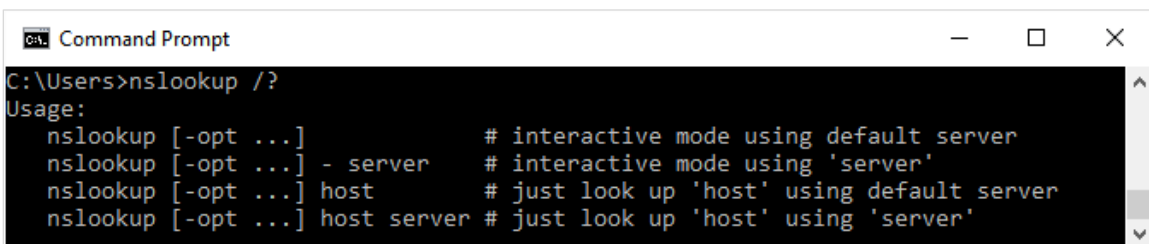
```
Command Prompt
C:\Users>nslookup 72.163.6.233
Server:  dns-rtp.cisco.com
Address:  64.102.6.247

Name:     reports-prod.cisco.com
Address:  72.163.6.233
```

Какой DNS-сервер выполнил команду **nslookup** для преобразования доменного имени?

Совпал ли IP-адрес DNS-сервера с адресом, который отображается в выходных данных при выполнении команды **ipconfig /all**.

В случае если сконфигурированный DNS-сервер не может преобразовать доменное имя или IP-адрес, возможно настроить сетевую служебную программу **nslookup** для преобразования имен с помощью другого DNS-сервера. Если второму DNS-серверу удалось преобразовать IP-адреса, а сконфигурированный DNS-сервер не смог выполнить эту задачу, то проблема заключается в настройке сконфигурированного DNS-сервера. Введите **nslookup /?** для просмотра параметров, которые могут использоваться для проверки, поиска и устранения неполадок.



```
Command Prompt
C:\Users>nslookup /?
Usage:
nslookup [-opt ...]           # interactive mode using default server
nslookup [-opt ...] - server  # interactive mode using 'server'
nslookup [-opt ...] host      # just look up 'host' using default server
nslookup [-opt ...] host server # just look up 'host' using 'server'
```

Шаг 5: Проверка возможностей подключения уровня приложений.

- а. Откройте веб-браузер. Введите **www.cisco.com** в поле «Адрес» и нажмите кнопку **ВВОД**.



Загружается ли веб-страница Cisco.com в браузере? Какие базовые сетевые функции должны работать для загрузки веб-страницы?

Вопросы для повторения

- Шаги в этой лабораторной работе представляют собой восходящую стратегию поиска и устранения неполадок, при которой процесс проверки начинается с уровня модели взаимодействия открытых систем (OSI) и заканчивается проверкой функций уровня приложения. Назовите две основные стратегии поиска и устранения неполадок, используемые техническими специалистами по сетям для выявления неполадок.

- Какую из стратегий необходимо использовать при неполадках в сетевых подключениях в первую очередь? Почему?
