СОДЕРЖАНИЕ

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Проведение лабораторных работ предусмотрено для расширения и закрепления знаний по теоретическому курсу.

Выполнение работ необходимо проводить с пояснениями, расчетами и выводами. На каждую работу оформляется отдельный отчет.

Перечень лабораторных работ

Номер работы	Тема лабораторной работы	Количество пар
1	Изучение и настройка сетевого оборудования	2
2	Построение локальной компьютерной сети	2
3	Основы организации инфокоммуникационной сети Интернет	2
4	Пакетные радиосети	2
	Итого	**8**

ЛАБОРАТОРНАЯ РАБОТА №1

Изучение и настройка сетевого оборудования

Необходимость выполнения работы: получить представление о том, как выглядят реальные компоненты сетей связи. Чтобы в дальнейшем понимать к чему относится проходимая в дальнейшем теория работы систем передачи информации.

Цель работы: Изучить интерфейс сетевого оборудования, виды портов и их назначение. Получить навыки настройки сетевого оборудования.

Подготовка к работе:

1. Изучить теоретическое описание (Приложение к лабе)

2. Посмотреть документацию на различные устройства популярных вендоров телекоммуникационного оборудования на их официальных сайтах:

https://eltex-co.ru/

https://www.cisco.com/c/ru_ru/index.html

https://www.huawei.com/ru/

https://www.juniper.net/ru/ru/

Задания:

В ходе лабораторной работы вам предстоит изучить внешний вид какого-то сетевого устройства (маршрутизатора, коммутатора) и познакомиться с его характеристиками и компонентами, такими как выключатель питания, порты управления, LAN- и WAN-интерфейсы, световые индикаторы, слоты расширения сети, слоты расширения памяти и др.

Кроме того, вы определите внутренние компоненты и характеристики IOS, подключившись к маршрутизатору через консоль и выполнив из интерфейса командной строки (CLI) команды **show version** и **show interfaces**.

Задание №1. В рукописной форме ответить на следующие вопросы:

1) Напишите 5 примеров мировых компаний - производителей телекоммуникационного оборудования.
2) Какие российские компании (производителей телекоммуникационного оборудования) вы знаете ?
3) Что содержит в себе оборудование, помимо аппаратной части.
4) Перечислите различные активные компоненты сетей связи.

5) Чем активные компоненты сети отличаются от пассивных?

6) Какие активные компоненты имеют свое программное обеспечение?

7) Какие виды ПО для сетевых устройств вы знаете? Приведите 3 примера.

8) Какие требования предъявляются к электропитанию оборудования систем связи?

9) Какое напряжение используется для питания оборудования систем связи?

10) Что такое Cisco IOS CLI ?

Задание №1. Осмотрите переднюю и заднюю панель устройтсва и ответьте на следующие вопросы.

Изучите данное вам оборудование:

1) Напишите название производителя и его краткую характеристику. Перечислите достоинства и недостатки этого производителя в сравнении с другими.

2) Напишите модель устройства. Что можно сказать об устройстве по названию модели? К какому классу сетевых устройств относится данное оборудование?

Рис.1 Внешний вид сетевого оборудования

3) Какое напряжение требуется для работы оборудовани?

4) Нарисуйте сетевое устройство (можно только вид спереди и сзади) и подпишите каждый порт, назначение каждого порта. Вы можете нарисовать на изображении стрелки или кружки, чтобы обозначить все элементы.

Рис.1 Пример передней панели

5) Какие виды кабелей используются для подключения к данному устройству?

Нарисуйте конструкцию разъемов кабелей, их распиновку и цель применения.

6) Изучите индикаторы режимов (они обозначены метками, например SYS, ACT, POE и др.). Напишите, что означают все аббревиатуры.

Изучение внутренних характеристик устройства

Задание №2. Подключите компьютер к сетевому устройству. Для этого следуйте следующей инструкции:

Получение доступа к коммутатору через консольный порт последовательного подключения

Вы подключите ПК к коммутатору с помощью rollover-консольного кабеля. Это подключение обеспечит доступ к интерфейсу командной строки (CLI) и позволит просмотреть параметры или настроить коммутатор.

Шаг 1: Соедините коммутатор и компьютер с помощью rollover-консольного кабеля. a. Подключите один конец rollover-консольного кабеля к консольному порту RJ-45 на коммутаторе.

b. Другой конец кабеля подключите к последовательному порту COM на компьютере.

Примечание. Последовательные порты COM больше не доступны на большинстве компьютеров. Для консольного подключения между компьютером и устройством можно использовать адаптер USB–DB9 с rollover-консольным кабелем. Адаптеры USB–DB9 можно приобрести в любом магазине электроники.

Примечание. При использовании адаптера USB–DB9 для подключения к порту COM может потребоваться установка драйвера для адаптера. Этот драйвер предоставляется изготовителем компьютера. Как определить порт COM, используемый адаптером, см. часть 3, шаг 4. Номер порта COM требуется для

подключения к устройству под управлением IOS при помощи эмулятора терминала в шаге 2.

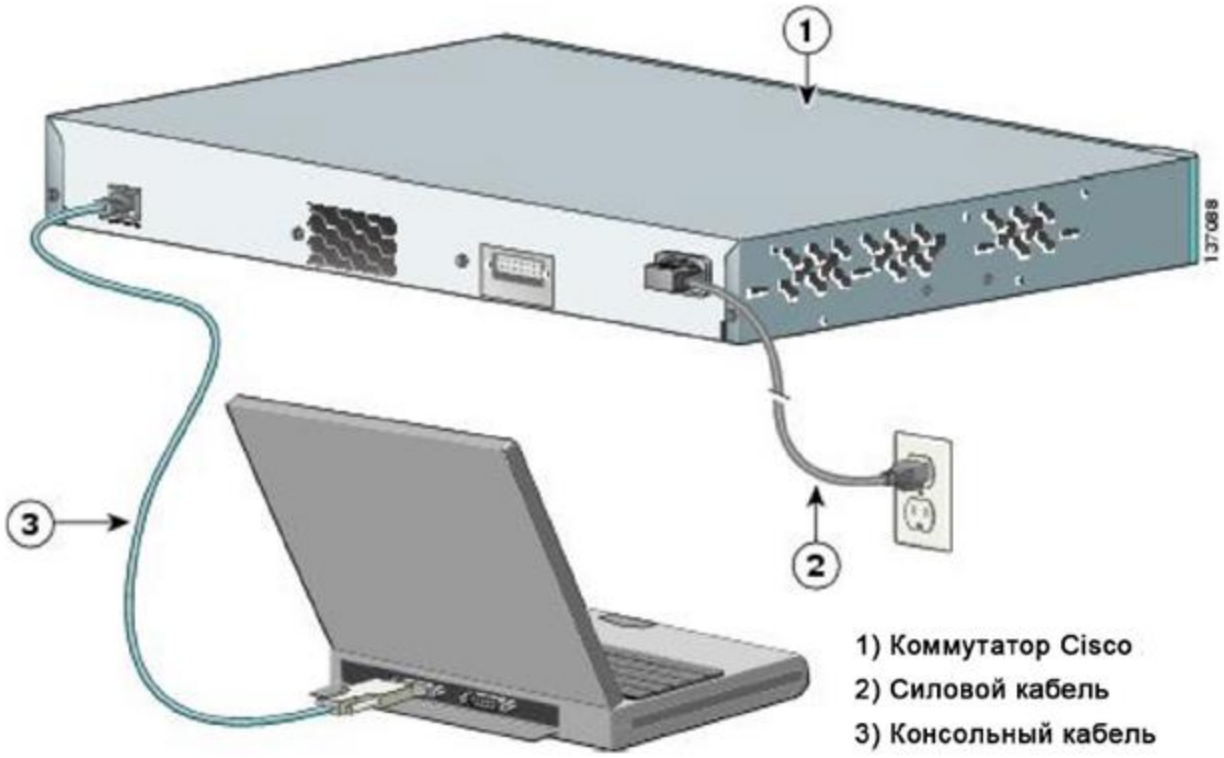


Рисунок 2 – Подключение ноутбука к коммутатору (или маршрутизатору)

c. Включите коммутатор и компьютер.

Шаг 2: Настройте Tera Term, чтобы установить сеанс консоли с коммутатором.

Tera Term — это программа эмуляции терминала. Она обеспечивает доступ к выходным данным терминала коммутатора, а также позволяет настроить коммутатор.

a. Запустите программу Tera Term, нажав кнопку **Пуск** на панели задач Windows. Найдите **Tera Term** в списке **Все программы**.

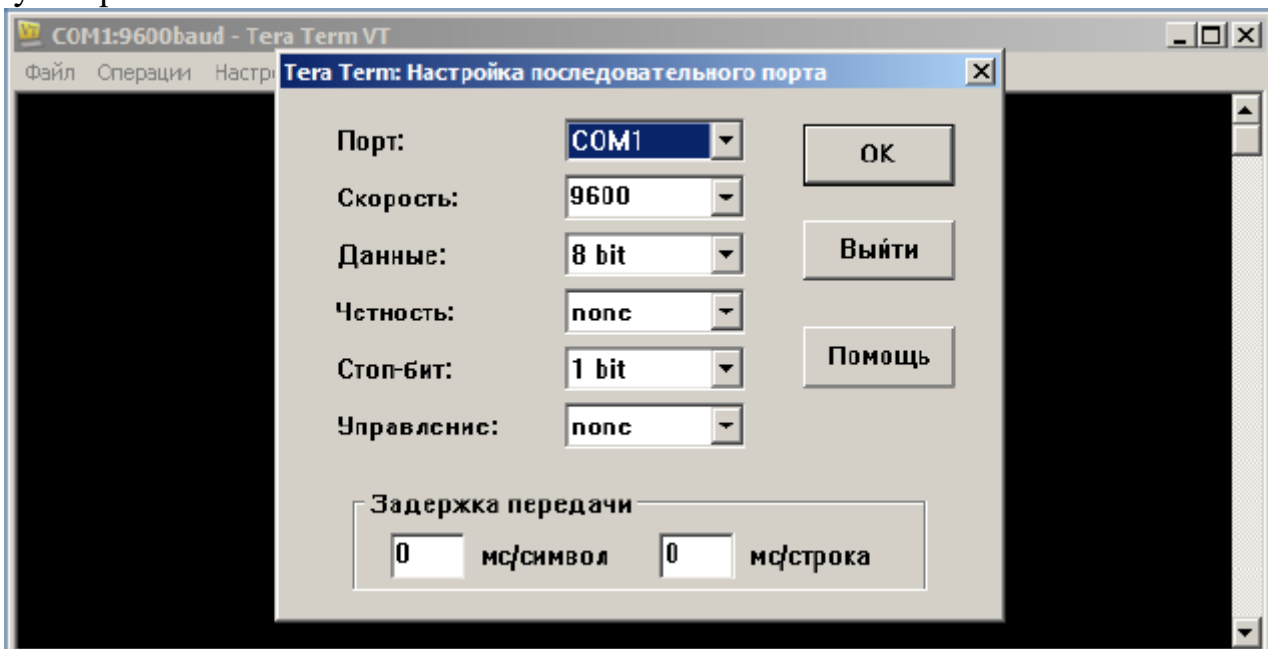
Примечание. Если программа Tera Term не установлена на компьютере, ее можно загрузить, перейдя по следующей ссылке и выбрав **Tera Term**:

http://logmett.com/index.php?/download/free-downloads.html

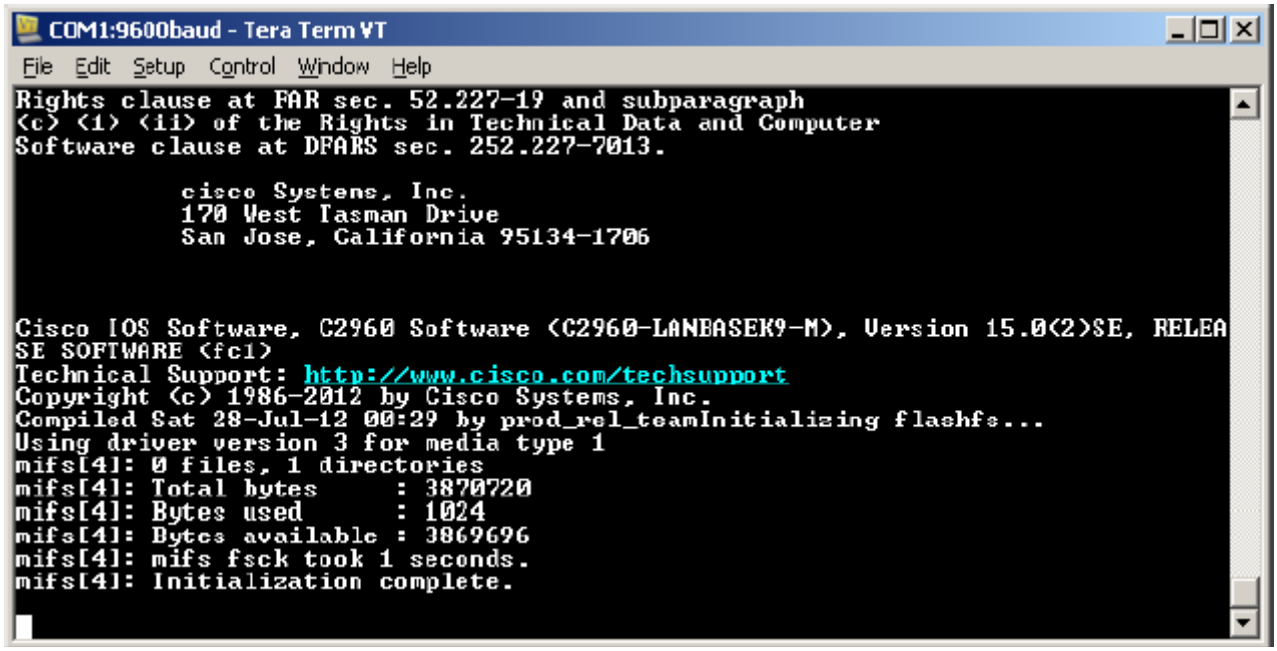
b. В диалоговом окне New Connection (Новое подключение) выберите **Serial** (Последовательное). Убедитесь, что выбран правильный порт COM, и для продолжения нажмите **OK**.

c. В меню **Setup** (Настройка) программы Tera Term выберите **Serial port…** (Последовательный порт...) и проверьте параметры последовательного порта. Параметры консольного порта по умолчанию: 9600 бод, 8 бит данных, без контроля четности, 1 стоповый бит, без управления потоком. Параметры Tera

Term по умолчанию совпадают с параметрами консольного порта для связи с коммутатором IOS.



d. Когда отобразятся выходные данные терминала, все готово к настройке коммутатора. В следующем примере консоли показаны выходные данные терминала в процессе загрузки коммутатора.



Шаг 3: Отобразите версию образа IOS на коммутаторе.

a. Когда процесс запуска коммутатора завершится, появится следующее сообщение. Для продолжения введите n.

```
Would you like to enter the initial configuration dialog? [yes/no]: n
```

b. В пользовательском режиме EXEC отобразите версию IOS на коммутаторе.

```
Switch> show version
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Sat 28-Jul-12 00:29 by prod_rel_team
ROM: Bootstrap program is C2960 boot loader
BOOTLDR: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(53r)SEY3, RELEASE SOFTWARE (fc1)
Switch uptime is 2 minutes
System returned to ROM by power-on
System image file is "flash:/c2960-lanbasek9-mz.150-2.SE.bin"
     <output omitted>
```

У операционной системы IOS есть несколько режимов работы (конфигурирования):

- **пользовательский режим** (приглашение терминала в этом режиме имеет вид >) позволяет только просмотреть базовые настройки сетевого устройства;
- **привилегированный режим** (#) — для полноценной настройки всех функций;
- **режим конфигурирования** ((config)#), в котором выполняются глобальные настройки.

Помимо этого, для настройки каждого отдельного интерфейса есть **режим специфической конфигурации** (Router(config-subif)#).

Посмотрите какие команды доступны в **пользовательский режиме, набрав знак вопроса**

Switch> ?

Наберите
Switch> show ?

c. Войдите в **привилегированный режим командой**

Войдите в привилегированный режим.
`S1> enable`
`S1#`
Можно писать в будущем не всю команду, а сокращенную `en`

Посмотрите какие команды доступны в этом режиме

Switch# ?

Наберите любую команду и приведите в отчет результат

Войдите в режим глобальной конфигурации

```
Switch# configure terminal
Enter configuration commands, one per line. End with
CNTL/Z.
```

Можно писать в будущем не всю команду, а сокращенную `conf t`

Посмотрите какие команды доступны в этом режиме

Switch(config)#?

Наберите любую команду и приведите в отчет результат

Зайдите в настройки интерфейса

Switch(config)#interface FastEthernet0/1

Посмотрите какие команды доступны в этом режиме

Switch(config-if)#?

Контрольные вопросы:

1. Какой командой можно посмотреть текущие настройки роутера?
2. Какими командами настраивается сетевой интерфейс роутера.
3. Как просмотреть конфигурационные настройки коммутатора?
4. Что такое vlan?
5. Как определить распределение vlan по портам коммутатора?
6. Перечислите основные режимы конфигурации при настройке коммутатора.
7. Перечислите основные режимы конфигурации при настройке роутера.
8. Зачем нужна таблица маршрутизации. Как посмотреть таблицу маршрутизации на роутере?
9. Какие команды формируют таблицу маршрутизации роутера?
10. Какими командами настраиваются vlan на коммутаторе?
11. Какими командами настраивается взаимодействие между вилланами?

ЛАБОРАТОРНАЯ РАБОТА №2

Построение локальной компьютерной сети

Необходимость выполнения работы: научитесь проектировать и настраивать сети передачи данных, чтобы при необходимости могли развернуть сеть в любом офисе, торговом центре, предприятии, военной базе и т.д., да где угодно – интернет нужен всем везде (а военной базе нужна своя отдельная ведомственная сеть связи).

Цель работы: Получить навыки по моделированию и настройке оборудования сетей передачи данных с использованием среды **CISCO Packet Tracer**.

Подготовка к работе:

1. Изучить теоретическое описание (см. Приложение к лабораторной на сайте)

2. Изучить соответствующие разделы в литературе:

1) Величко В. В. Основы инфокоммуникационных технологий: учеб. пособие для вузов / В. В. Величко, Г. П. Катунин, В. П. Шувалов. - М.: Горячая линия – Телеком, 2018. http://www.iprbookshop.ru/74561.html

2) Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. – СПб.: Питер, 2012. – 944 с.

Задания:

В ходе этой лабораторной работы вы изучите структуру протокола IPv4. Определите различные типы IPv4-адресов и компоненты, из которых они составляются — сетевую и узловую части, маску подсети. В число рассматриваемых типов адресов входят публичные и частные адреса, адреса для одноадресной и многоадресной рассылки.

Задание №1. В рукописной форме ответить на следующие вопросы:

1) Что такое LAN-сеть?
2) Какие топологии имеют локальные компьютерные сети?
3) Возможно ли построить беспроводную LAN сеть?
4) Чем отличается маршрутизатор от коммутатора и концентратора?
5) Что такое модель OSI и зачем она была разработана?
6) Какие уровни включает в себя модель OSI?
7) Что такое MAC адрес?
8) Что такое IP адрес?

9) Что такое маска?
10) Что такое протокол?
11) Какие протоколы вы знаете, напишите 5 примеров?
12) Какие есть альтернативные программы CISCO Packet Tracer и какие у них преимущества?

Задание №1
Определение IPv4-адресов

Проанализируйте приведенную ниже таблицу и определите сетевую и узловую части указанных IPv4-адресов.

Сокращения, используемые в таблице:
С = все 8 бит для октета содержатся в сетевой части адреса
с = бит в сетевой части адреса
У = все 8 бит для октета содержатся в узловой части адреса
у = бит в узловой части адреса

Пример

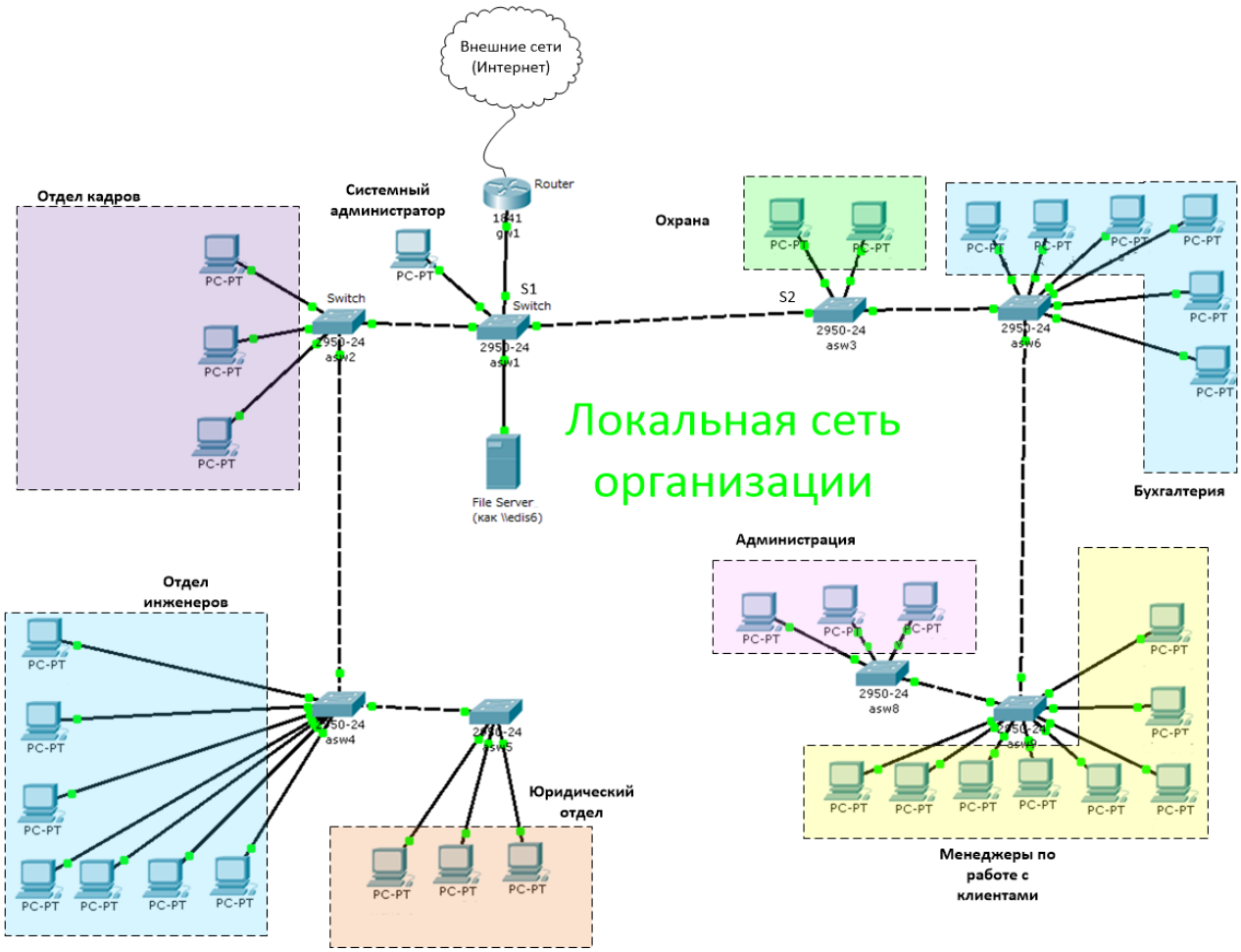
IP-адрес/префикс	Сеть/узел С,с = сеть, У,у = узел	Маска подсети	Сетевой адрес
192.168.10.10/24	С.С.С.У	255.255.255.0	192.168.10.0
10.101.99.17/23	С.С.ссссссу.У	255.255.254.0	10.101.98.0
209.165.200.227/27			
172.31.45.252/24			
10.1.8.200/26			
172.16.117.77/20			
10.1.1.101/25			
209.165.202.140/27			
192.168.28.45/28			

Задание №2.1 Соберите сеть организации

CISCO Packet Tracer

Шаг 1 Запустите среду моделирования Cisco packet tracer. Ознакомьтесь с ее интерфейсом. Прочитайте Приложение к лабе№2 на сайте и посмотрите видео для знакомства с программой Cisco packet tracer.

Представим сеть какой-либо организации (офис компании по продажам, банк, ВУЗ и т.д.). Сеть наша средних размеров и мы выбрали для сети диапазон частных IP-адресов 172.16.0.0/16



Для удобства и порядка мы поделили нашу локальную сеть на сегменты (подсети). Как видно из таблицы 1, для организации адресов подсетей мы использовали новую маску. Каждый сегмент сети содержит диапазон IP-адресов

Таблица 1. План адресации

№ сегмента сети	Структурное подразделение	IP-адрес
1	Адрес шлюза (порт роутера)	172.16.0.1/16
2	Для серверов	172.16.0.0/24
3	Отдел кадров	172.16.2.0/24
4	Охрана	172.16.3.0/24
5	Бухгалтерия	172.16.4.0/24
6	Администрация	172.16.5.0/24
7	Менеджеры	172.16.6.0/24
8	Юридический отдел	172.16.7.0/24
9	Отдел инженеров	172.16.8.0/24
10	Для управления устройствами сети	172.16.1.0/24

Задание №2.2 Настройте IP адреса на устройствах сети

Настройка ПК

Настройте IP-адреса для всех компьютеров PC в соответствии с адресацией в таблице 1.

Шаг 1: Настройте IP-адреса для ПК.

a. Щелкните первый PC отдела кадров и откройте вкладку **Desktop** (Рабочий стол).

b. Щелкните **IP Configuration** (Настройка IP-адресов). В таблице адресации выше можно увидеть, что для компьютеров, сетевых принтеров, телефонов отдела кадров назначен диапазон IP-адресов 172.16.2.1 - 172.16.2.254. Введите любой из этих адресов для PC1 в окне **IP Configuration** (Настройка IP-адресов).

c. Повторите шаги 1a и 1б для всех компьютеров отдела кадров.

d. В соответствии с таблицей 1 настройте IP-адреса для всей сети

Сделайте вывод, удобно ли настраивать вручную IP адреса в сети для десятков-сотен-тысяч компьютеров и других устройств. Какое может быть решение этой задачи.

Шаг 2: Проверьте возможность удаленного подключения системным администратором к коммутаторам для их настройки.

a. Щелкните PC1. Закройте окно **IP Configuration** (Настройка IP-адресов), если оно открыто. На вкладке **Desktop** (Рабочий стол) нажмите **Command Prompt** (Командная строка).

b. Введите команду **ping** с IP-адресом коммутатора S1 и нажмите клавишу ввода.

```
Packet Tracer PC Command Line 1.0 PC> ping 172.16.1.3
```

Ответьте письменно на вопрос: Удалось ли выполнить команду? Дайте пояснение.

Задание №2.3 Настройка адресов для управления коммутаторами

Настройте IP-адреса для коммутаторов сети.

Общие сведения

Коммутаторы имеют особый интерфейс, который называется виртуальным интерфейсом коммутатора (switch virtual interface, SVI). Для SVI можно настроить IP-адрес, который обычно называется адресом управления. Адрес управления используется для удаленного доступа к коммутатору с целью просмотра или настройки параметров.

В этой лабораторной работе вы уже создали локальную сеть по технологии Ethernet на основе кабельных подключений и сейчас будете управлять коммутатором, используя консоль и методы удаленного доступа. Вы настроите основные параметры коммутатора, IP-адреса и продемонстрируете использование IP-адреса управления для удаленного управления коммутатором.

Шаг 1: Настройте IP-адрес для коммутатора S1. Коммутаторы можно использовать в режиме «plug & play». Это значит, что они могут начать работать и без

предварительной настройки. Коммутаторы пересылают данные между портами, опираясь на MAC- адреса. Для чего тогда нужно настраивать IP-адреса?

Щелкните коммутатор S1 и перейдите в CLI (Интерфейс командной строки)

Чтобы настроить IP-адрес интерфейса SVI коммутатора введите следующие команды

```
S1> ip address 172.16.1.3 255.255.255.0
```

Удалось ли выполнить команду? Если нет, значит у нас нет прав на это. Следуйте следующим шагам.

Чтобы настроить IP-адрес на коммутаторе S1, надо использовать следующие команды.

Войдите в привилегированный режим.

```
S1> enable
S1#
```

Можно писать в будущем не всю команду, а сокращенную `en`

Войдите в режим глобальной конфигурации

```
S1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

Можно писать в будущем не всю команду, а сокращенную `conf t`

В режиме глобальной конфигурации (можно сказать мы получили права админа на коммутаторе) настройте IP-адрес интерфейса SVI, чтобы обеспечить возможность удаленного управления коммутатором

```
S1(config)# interface vlan 1
S1(config-if)# ip address 172.16.1.3 255.255.255.0
S1(config-if)# no shutdown %LINEPROTO-5-UPDOWN: Line protocol on
Interface Vlan1, changed state to up
S1(config-if)#
S1(config-if)# exit
S1#
```

`Ответьте письменно на вопрос:` Зачем вы вводите команду **no shutdown**?

Шаг 2: Настройте IP-адреса для коммутатора S2. Используя данные из таблицы адресации, настройте IP-адрес для S2.

Шаг 3: Проверьте настройки IP-адресов на коммутаторах S1 и S2. Команда **show ip interface brief** выводит сведения об IP-адресе, а также о состоянии всех портов и интерфейсов коммутатора. Для этого можно также использовать команду **show running-config**.

Шаг 4: Проверьте подключение к сети. Подключение к сети можно проверить с помощью команды **ping**. Очень важно, чтобы подключения работали во всей сети. В случае сбоя необходимо устранить неполадку. Проверьте связь коммутаторов S1 и S2 с компьютерами PC1 и системного администратора.

a. Щелкните PC1 и откройте вкладку **Desktop** (Рабочий стол). Щелкните **Command Prompt** (Командная строка). С помощью команды ping проверьте доступность IP-адреса коммутатора S1.
b. Щелкните PC системного администратора и откройте **Command Prompt** (Командная строка). С помощью команды ping проверьте доступность IP-адреса коммутатора S1 и коммутатора S2.

Контрольные вопросы:

1. Что такое компьютерная сеть?
2. На какие группы делятся компьютерные сети по территориальной распределённости?
3. Какую сеть называют локальной? Привести 3 примера локальных сетей из жизни.
4. Какую сеть называют глобальной?
5. На какие группы делятся компьютерные сети по ведомственной принадлежности?
6. Что такое топология сети?
7. Что представляет собой топология сети «звезда»? Преимущества? Недостатки?
8. Что представляет собой топология сети «кольцо»? Преимущества? Недостатки?
9. Что представляет собой топология сети «шина»? Преимущества? Недостатки?
10. Что такое Шлюз (gateway)?

ЛАБОРАТОРНАЯ РАБОТА №3

Основы организации инфокоммуникационной сети Интернет

Необходимость выполнения работы: после изучения основ систем передачи информации и линий связи необходимо разобраться как всё это вместе образует глобальную единую сеть передачи данных по всему миру, каким образом компьютеры, смартфоны через глобальную сеть обмениваются данными с устройствами (серверами) с других континентов.

Цель работы: Получить навыки по моделированию сетей передачи данных с использованием среды **CISCO Packet Tracer**.

Подготовка к работе:

1. Изучить теоретическое описание (Приложение на сайте)

2. Изучить соответствующие разделы в литературе:

1) Величко В. В. Основы инфокоммуникационных технологий: учеб. пособие для вузов / В. В. Величко, Г. П. Катунин, В. П. Шувалов. - М.: Горячая линия – Телеком, 2018. http://www.iprbookshop.ru/74561.html

2) Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. – СПб.: Питер, 2012. – 944 с.

Задания:

Задание №1.

Проверьте конфигурацию TCP/IP с помощью утилиты ***ipconfig***. Заполните таблицу:

Имя хоста	
IP-адрес	
Маска подсети	
Основной шлюз	
Используется ли DHCP (адрес DHCP-сервера)	
Описание адаптера	
Физический адрес сетевого адаптера	
Адрес DNS-сервера	
Адрес WINS-сервера	

В рукописной форме ответить на следующие вопросы:

1) Что такое шлюз?
2) Что такое DNS?
3) Что такое DHCP?
4) Что такое WINS-сервера?
5) Может ли быть у компьютера два MAC адреса?
6) Может ли быть у компьютера два IP адреса?

Задание №2.

Моделирование сети передачи данных

Цель этого задания – помочь вам понять процессы движения трафика и изучить содержимое пакетов данных, передаваемых в сетях с пакетной передачей данных (с коммутацией пакетов).

Представьте, что у компании есть три офиса в различных районах города. Каждый офис имеет свою локальную компьютерную корпоративную сеть. Также все офисы должны быть связаны другу с другом. Поэтому мы имеем три локальных сети, объединенных друг с другом. Сеть в центральном офисе №1 будем называть Central, она имеет десятки компьютеров. Сеть в другом офисе №2 (филиале) будем называть Branch, она имеет маршрутизатор с доступом к Интернету и выделенным подключением к глобальной сети (WAN) для связи с центральным офисом №1. Третья сеть офиса №3 имеет маршрутизатор выделенным подключением к глобальной сети.

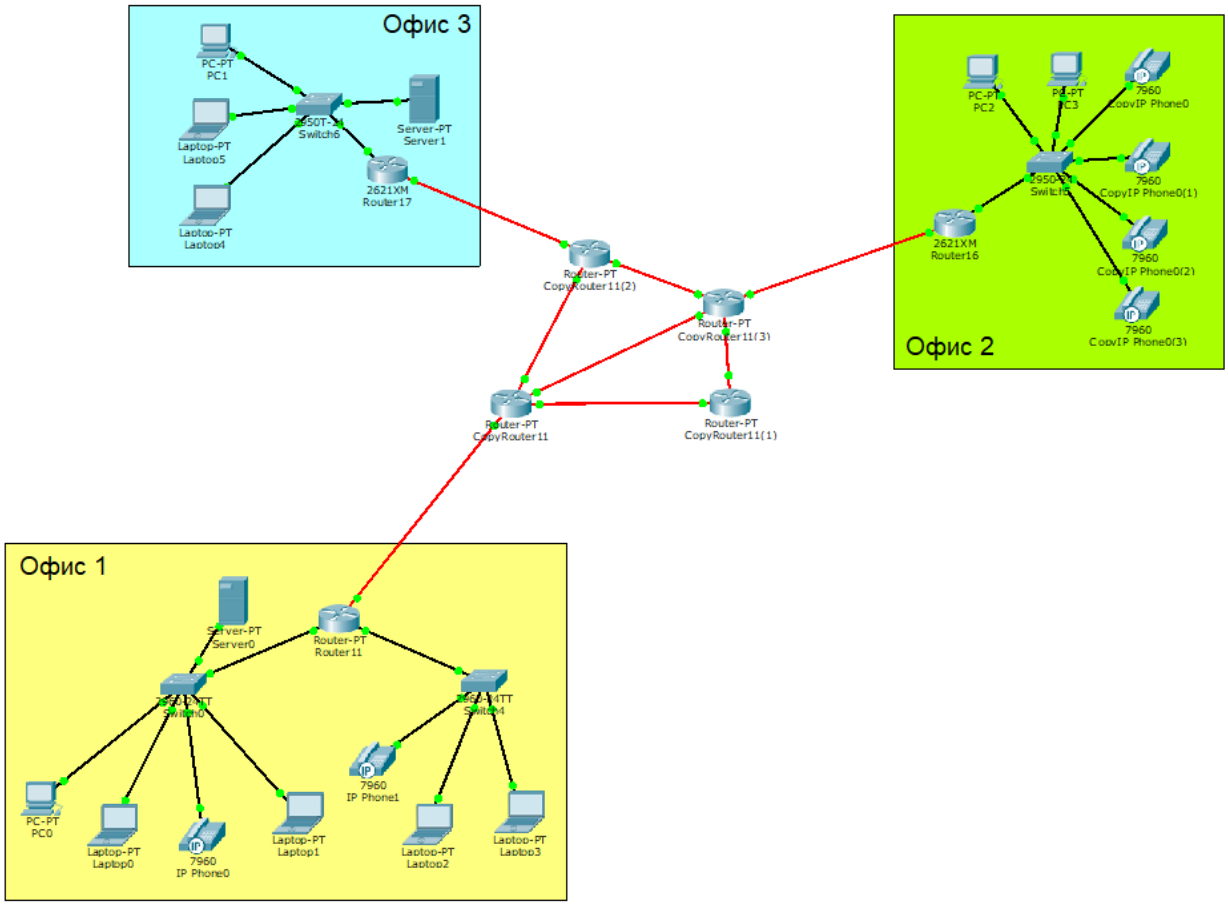
CISCO Packet Tracer

Шаг 2.1 Запустите среду моделирования Cisco packet tracer. Ознакомьтесь с ее интерфейсом. Прочитайте приложение к лабораторной.

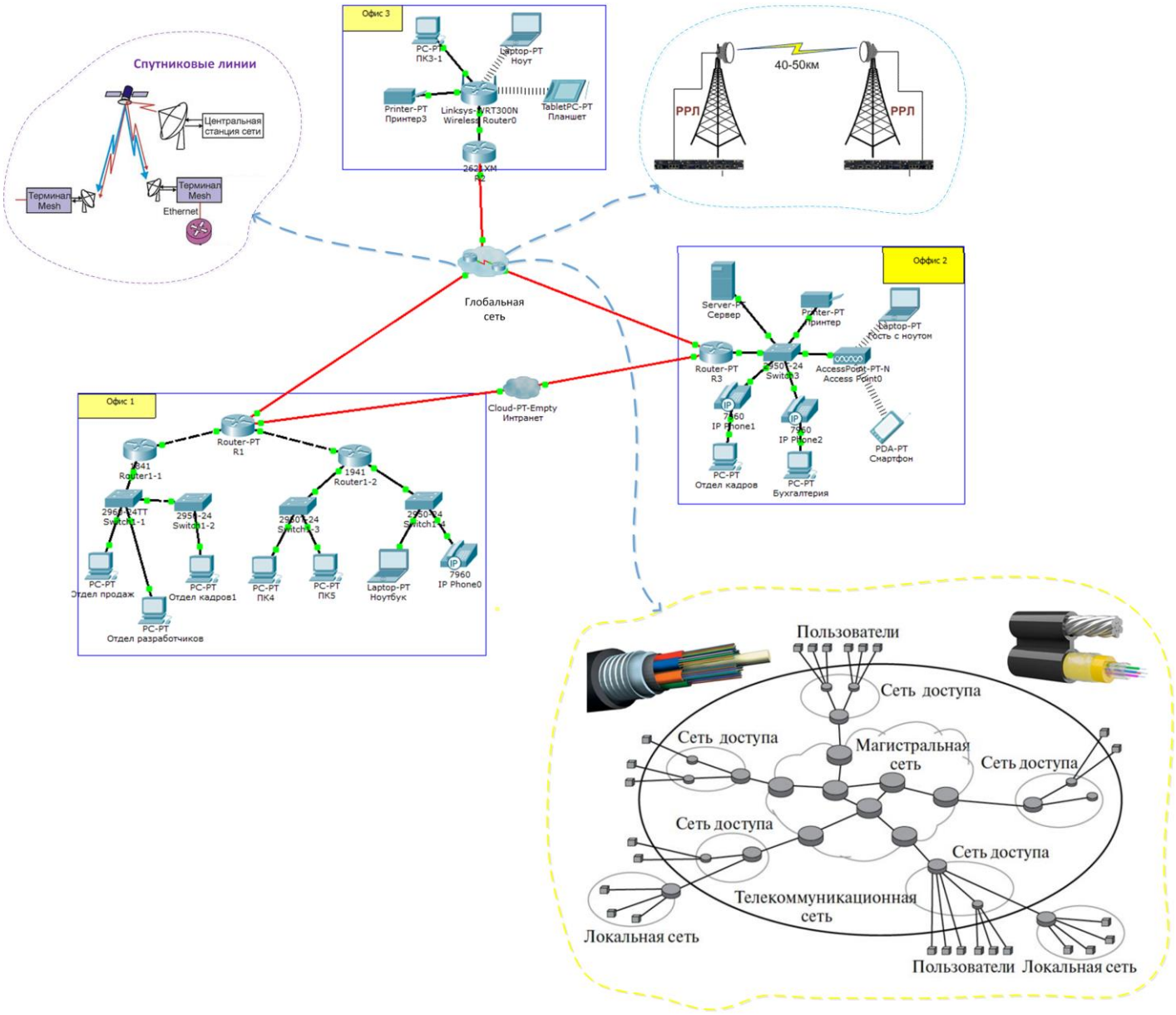
Шаг 2.2. Соберите схему по варианту 1 или 2. В более крупном формате рисунке на странице https://creatorblaga.ru/раздел-описис/opisis-lab3/

Шаг 2.3 После того, как вся сеть собрана, необходимо ее настроить. Когда дома в новом квартале города построены, им присваивают уникальные неповторяющиеся адреса – название улицы, № дома. Аналогично, когда построена новая сеть, ее элементам присваивают уникальные неповторяющиеся IP-адреса. **Придумайте и настройте корректную IP-адресацию построенной сети.**

Вариант 1


Офис 3
PC-PT
PC1
Laptop-PT
Laptop5
Laptop-PT
Laptop4
2950T-24
Switch6
Server-PT
Server1
2621XM
Router17
Router-PT
CopyRouter11(2)
Router-PT
CopyRouter11(3)
Router-PT
CopyRouter11
Router-PT
CopyRouter11(1)
Офис 2
PC-PT
PC2
PC-PT
PC3
7960
CopyIP Phone0
7960
CopyIP Phone0(1)
7960
CopyIP Phone0(2)
7960
CopyIP Phone0(3)
2621XM
Router16
Офис 1
Server-PT
Server0
Router-PT
Router11
PC-PT
PC0
Laptop-PT
Laptop0
7960
IP Phone0
Laptop-PT
Laptop1
7960
IP Phone1
Laptop-PT
Laptop2
Laptop-PT
Laptop3

Вариант 2



Шаг 2.4 В офисе №1 произведите ping процесс от отдела продаж до отдела разработчиков.

В Packet Tracer предусмотрен режим моделирования, в котором подробно описывается и показывается, как работает утилита Ping. Перейдите в режим моделирования, нажав на одноименный значок в нижнем правом нижнем углу рабочей области, или по комбинации клавиш Shift+S. Откроется «Панель моделирования», в которой будут отображаться все события, связанные с выполнения ping-процесса.

Теперь необходимо запустить ping-процесс.

После его запуска можно сдвинуть «Панель моделирования», чтобы на схеме спроектированной сети наблюдать за отправкой/приемкой пакетов.

Кнопка «Автоматически» подразумевает моделирование всего ping-процесса в едином процессе, тогда как «Пошагово» позволяет отображать его пошагово.

Чтобы узнать информацию, которую несет в себе пакет, его структуру, достаточно нажать правой кнопкой мыши на цветной квадрат в графе «Информация».

Моделирование прекращается либо при завершении ping-процесса, либо при закрытии окна «Редактирования» соответствующей рабочей станции.

Изучите данный текст, подпишите, что содержится в каждой строке.

Pinging 192.168.0.1with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time=183ms TTL=120
Reply from 192.168.0.1: bytes=32 time=90ms TTL=120
Reply from 192.168.0.1: bytes=32 time=118ms TTL=120
Reply from 192.168.0.1: bytes=32 time=87ms TTL=120
Ping statistics for 192.168.0.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 87ms, Maximum = 183ms, Average = 119ms
PC>

Задание №3. Составление карты сети

Включает в себя 4 задачи:

Задача 3.1. Проверка подключения к сети с помощью эхо-запроса с помощью команды ping

Дополнительные задачи (можно сделать дома):

Задача 3.2. Отслеживание маршрута к удалённому серверу с помощью утилиты Windows «traceroute»

Задача 3.3. Отслеживание маршрута к удалённому серверу с помощью программных и веб- средств

Задача 3.4. Сравнение результатов трассировки

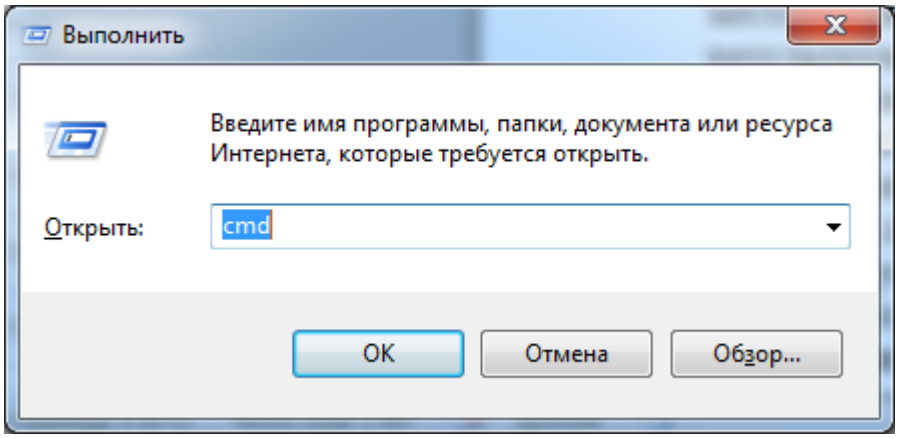
Задача 3.1. Проверка подключения к сети посредством эхо-запроса с помощью команды ping

Команда **ping** (Packet InterNet Groper) является очень распространенным средством для устранения неполадок, связанных с доступом к устройствам. В ней для определения активности удаленного хоста используются два типа сообщений протокола ICMP – эхо-запрос и эхо-ответ. Команда **ping** также измеряет количество времени, необходимого для получения эхо-ответа.

Шаг 1: Определите, доступен ли удалённый сервер.

Эхо-запрос с помощью команды ping — это средство для проверки доступности узла. Пакеты информации пересылаются удалённому узлу с требованием ответа. Локальный ПК определяет, получен ли ответ для каждого пакета, и рассчитывает, какое время заняла пересылка этих пакетов по сети. Название эхо-запрос пришло из области активной гидролокации, где оно обозначало звуковой сигнал, отправляемый под воду и отражающийся от дна или других кораблей.

Нажмите на клавиатуре сочетание клавиш «Windows + R» и в открывшемся окне введите команду **cmd**. Откроется командная строка.



В командной строке введите **ping www.youtube.com**

В первой строке полученных данных отображается **полное** доменное имя FQDN

wide-youtube.l.google.com

Затем следует IP-адрес [64.233.163.198].

В командной строке введите **ping www.instagram.com**

В первой строке полученных данных отображается **полное** доменное имя FQDN, затем следует IP-адрес [157.240.205.174].
Но поскольку данный сервис заблокирован Роскомнадзором, то пинговаться он не будет.

www.mmedia.microsoft.com

Имя сервера

домен 1 уровня

домен 2 уровня

домен 3 уровня

Соглашение о доменах 1 уровня:
страна, для США - тип организации

com – компании, edu – образование, org – организации, net – сетевые, gov – правительственные, mil – военные, arpa – выходит из употребления, сеть arpa
ru –Россия, ca – Канада, uk – Великобритания, au – Австралия и т.д.

Далее в командной строке введите **ping www.cisco.com**

```
C:\>ping www.cisco.com

Pinging e144.dscb.akamaiedge.net [23.1.48.170] with 32 bytes of data:
Reply from 23.1.48.170: bytes=32 time=56ms TTL=57
Reply from 23.1.48.170: bytes=32 time=55ms TTL=57
Reply from 23.1.48.170: bytes=32 time=54ms TTL=57
Reply from 23.1.48.170: bytes=32 time=54ms TTL=57

Ping statistics for 23.1.48.170:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 54ms, Maximum = 56ms, Average = 54ms
```

Веб-узлы компании Cisco, содержащие одну и ту же информацию, размещаются на различных серверах (так называемых зеркалах) по всему миру. Это значит, что **полное** доменное имя FQDN и IP-адрес будут отличаться в зависимости от вашего местонахождения.

Убедитесь, что были отправлены четыре эхо-запроса, на каждый из которых был получен ответ. Ответ поступил на все эхо-запросы, значит, потери пакетов нет (0 % потерь).
Для передачи пакетов по сети до недалеко расположенного хоста требуется менее 100 мс (Миллисекунда — это 1/1000 секунды), если же мы будем отправлять пакеты в Африку, время передачи может увеличиться в разы. От потери пакетов или медленного сетевого подключения в первую очередь страдает качество потокового видео и онлайн-игр.

Теперь отправьте эхо-запрос с помощью команды ping на веб-сайты регионального интернет- регистратора (RIR), расположенные в различных частях мира.

Африка: **ping www.afrinic.net**

Азия и Австралия: **ping www.apnic.net**

Европа: **ping www.ripe.net**

Южная Америка: **ping lacnic.net**

Северная Америка **ping arin.net**

Что происходит со средним временем эхо-запроса (в миллисекундах), когда данные передаются в пределах одного континента, по сравнению с ситуацией, когда данные пересылаются на другие континенты?

Что интересного можно сказать об эхо-запросах с помощью команды ping, отправленных на американский веб-сайт через океан?

Задача 3.2 Отслеживание маршрута к удалённому серверу с помощью утилиты «traceroute»

Команда трассировки

Там, где команда **ping** может быть использована для проверки связи между устройствами, команда **tracert** может использоваться для обнаружения трактов, по которым пакеты достигают удаленных адресатов, а также точек нарушения маршрутизации.

Инструмент **tracert** часто используется для поиска и устранения неполадок в сети. Она отображает список пройденных маршрутизаторов и позволяет определить, какой путь использовался для достижения определённого пункта назначения в одной сети или перехода между несколькими сетями. Каждый маршрутизатор — это точка соединения двух сетей, через которую пересылаются пакеты данных. Количество маршрутизаторов называется количеством «переходов», совершённых данными на пути от источника до места назначения.

Отображаемый список поможет определить, какие проблемы с потоком данных возникают при попытке доступа к какому-либо сервису, например веб-сайту. Также список может пригодиться при выполнении таких задач, как загрузка данных. Если один и тот же файл доступен на нескольких веб-сайтах

(зеркалах), можно проверить маршрут для каждого зеркала и выбрать наиболее быстрый вариант.

Две трассировки маршрута, выполненные между одними и теми же узлами источника и адресата, но в разное время, могут дать разные результаты. Это может быть связано с тем, что протоколы могут выбирать различные кабельные каналы для отправки пакетов – т.е. выбирать наиболее оптимальный маршрут в текущий момент времени.

Как правило, для запуска этого сетевого средства в командную строку необходимо ввести следующее:

tracert <destination network name or end device address>
(для операционных систем семейства Microsoft Windows)

или **traceroute** <destination network name or end device address>
(для Unix и подобных систем)

Утилиты трассировки маршрута позволяют определять пути или маршруты, а также вычислять время задержки в IP-сети.

Для выполнения данной работы необходима программа VisualRoute. Если на вашем компьютере программа VisualRoute не установлена, загрузите её по следующей ссылке: http://www.visualroute.com/download.html

Используя интернет-подключение и три различных утилиты трассировки маршрута, вы должны будете отследить путь прохождения пакетов данных через Интернет к сетям назначения. Сначала вы воспользуетесь командной строкой и командой «tracert», встроенной в ОС Windows, затем веб-средством для трассировки маршрута (http://www.subnetonline.com/pages/network-tools/online-traceroute.php) и, наконец, программой VisualRoute.

В командной строке введите **tracert** до какого-нибудь зарубежного сайта, например www.youtube.com

```
C:\Windows\system32\cmd.exe

Трассировка маршрута к wide-youtube.l.google.com [64.233.163.198]
с максимальным числом прыжков 30:

  1     1 ms    <1 мс    <1 мс  192.168.1.1
  2     2 ms     1 ms     1 ms  100.64.0.1
  3     2 ms     1 ms     2 ms  85-235-63-13.rev.utk.ru [85.235.63.13]
  4     1 ms     1 ms     2 ms  zoo-cr01-be19.4024.ekt.mts-internet.net [212.188.18.128]
  5     2 ms     1 ms     1 ms  zoo-cr02-ae0.16.ekt.mts-internet.net [195.34.50.222]
  6     1 ms     1 ms     1 ms  zoo-cr02-ae13.0.ekt.mts-internet.net [195.34.50.238]
  7    33 ms    33 ms    32 ms  zoo-cr01-be18.10.ekt.mts-internet.net [195.34.50.226]
  8    32 ms    31 ms    31 ms  zoo-cr03-be3.66.ekt.mts-internet.net [195.34.53.29]
  9    44 ms    41 ms    40 ms  psshag-cr01-ae13.74.chel.mts-internet.net [195.34.50.89]
 10    35 ms    38 ms    41 ms  che-cr02-ae10.63.sam.mts-internet.net [212.188.42.129]
 11    32 ms    32 ms    32 ms  a433-cr02-be13.63.msk.mts-internet.net [212.188.1.181]
 12    32 ms    32 ms    32 ms  a433-cr03-be5.77.msk.mts-internet.net [212.188.0.170]
 13    32 ms    32 ms    32 ms  74.125.118.22
 14    33 ms    33 ms    32 ms  108.170.250.129
 15    33 ms    38 ms    32 ms  108.170.250.146
 16    46 ms    45 ms    46 ms  142.251.237.156
 17  1100 ms  1042 ms   956 ms  142.251.237.146
 18    46 ms    46 ms    46 ms  142.250.56.129
 19     *        *        *     Превышен интервал ожидания для запроса.
 20     *        *        *     Превышен интервал ожидания для запроса.
 21     *        *        *     Превышен интервал ожидания для запроса.
 22     *        *        *     Превышен интервал ожидания для запроса.
 23     *        *        *     Превышен интервал ожидания для запроса.
 24     *        *        *     Превышен интервал ожидания для запроса.
 25     *        *        *     Превышен интервал ожидания для запроса.
 26     *        *        *     Превышен интервал ожидания для запроса.
 27     *        *        *     Превышен интервал ожидания для запроса.
 28    53 ms    53 ms    53 ms  lj-in-f198.1e100.net [64.233.163.198]

Трассировка завершена.

C:\Users\ADM-PK>
```

С помощью любого сервиса по определению местоположения по IP (например https://2ip.io/ru/geoip/) проверьте и напишите в отчет, где находится сервер YouTube

```
C:\Windows\system32\cmd.exe

C:\Users\ADM-PK>tracert www.likee.video

Трассировка маршрута к www.likee.video [169.136.83.240]
с максимальным числом прыжков 30:

  1     1 ms    <1 мс    <1 мс  192.168.1.1
  2     2 ms     1 ms     1 ms  100.64.0.1
  3     2 ms     1 ms     1 ms  85-235-63-9.rev.utk.ru [85.235.63.9]
  4     1 ms     1 ms     1 ms  asb-cr01-ae19.4024.ekt.mts-internet.net [212.188.18.130]
  5     1 ms     1 ms     1 ms  asb-cr02-be3.66.ekt.mts-internet.net [212.188.56.134]
  6    34 ms    32 ms    38 ms  psshag-cr01-ae5.74.chel.mts-internet.net [212.188.56.94]
  7    33 ms    33 ms    34 ms  che-cr02-ae10.63.sam.mts-internet.net [212.188.42.129]
  8     *        *       32 ms  a433-cr02-be13.63.msk.mts-internet.net [212.188.1.181]
  9    32 ms    32 ms    32 ms  m9-cr05-ae9.77.msk.mts-internet.net [212.188.28.137]
 10    35 ms    33 ms    32 ms  as10122.asbr.router [212.188.33.229]
 11    39 ms    34 ms    35 ms  10.110.192.46
 12    32 ms    32 ms    32 ms  169.136.83.240

Трассировка завершена.
```

С помощью любого сервиса по определению местоположения по IP (например https://2ip.io/ru/geoip/) проверьте и напишите в отчет, где находится сервер Likee

С помощью любого сервиса по определению местоположения по IP (например https://2ip.io/ru/geoip/) проверьте и напишите в отчет, где находится сервер aup.uisi.ru

Сохраните результаты, полученные после ввода команды «tracert», в текстовый файл, выполнив указанные ниже действия.

1) Нажмите правой кнопкой мыши на строку заголовка окна командной строки и выберите параметры **Изменить > Выделить всё**.

2) Ещё раз нажмите правой кнопкой мыши на строку заголовка окна командной строки и выберите параметры **Изменить > Копировать**.

3) Скопируйте результаты в документ отчёта лаб. работы.

Запустите команду **tracert** также для веб-сайтов в разных точках мира и сохраните полученные результаты

tracert www.afrinic.net – Африка

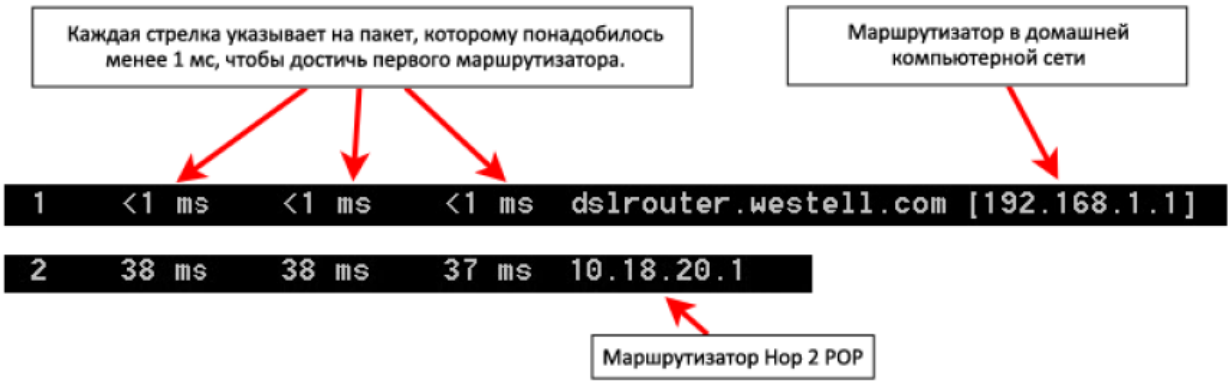
tracert www.lacnic.net – Южная Америка

Интерпретируйте данные, полученные с помощью утилиты **tracert**. В зависимости от зоны охвата вашего интернет-провайдера и расположения узлов источника и назначения отслеженные маршруты могут пересекать множество переходов и сетей. Каждый переход — это один маршрутизатор. Маршрутизатор представляет собой особый компьютер, который используется для перенаправления трафика через Интернет. Представьте, что вы отправились в поездку по автодорогам нескольких стран. Во время своего путешествия вы постоянно попадаете на развилки, где нужно выбирать одно из нескольких направлений. Теперь представьте себе, что на каждой такой развилке имеется устройство, которое указывает правильный путь к конечной цели вашего путешествия. То же самое делает маршрутизатор для пакетов в сети. Поскольку компьютеры используют язык цифр, а не слов, маршрутизаторам присваиваются уникальные IP-адреса (номера в формате x.x.x.x). Утилита **tracert** показывает, по какому пути проходит пакет данных до конечного пункта назначения. Кроме того, с помощью утилиты **tracert** можно определить, с какой скоростью проходит трафик через каждый сегмент сети. Каждому маршрутизатору на пути прохождения данных отправляются три пакета, время ответа на которые измеряется в миллисекундах. Используя данную информацию, проанализируйте результаты, полученные с помощью утилиты **tracert** при отправке пакетов

Ниже представлен пример трассировки и пример анализа результата

```
C:\>tracert www.cisco.com

Tracing route to e144.dscb.akamaiedge.net [23.1.144.170]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  dslrouter.westell.com [192.168.1.1]
  2    38 ms    38 ms    37 ms  10.18.20.1
  3    37 ms    37 ms    37 ms  G3-0-9-2204.ALBYNY-LCR-02.verizon-gni.net [130.8
1.196.190]
  4    43 ms    43 ms    42 ms  so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81
.22.46]
  5    43 ms    43 ms    65 ms  0.so-4-0-2.XT2.NYC4.ALTER.NET [152.63.1.57]
  6    45 ms    45 ms    45 ms  0.so-3-2-0.XL4.EWR6.ALTER.NET [152.63.17.109]
  7    46 ms    48 ms    46 ms  TenGigE0-5-0-0.GW8.EWR6.ALTER.NET [152.63.21.14]

  8    45 ms    45 ms    45 ms  a23-1-144-170.deploy.akamaitechnologies.com [23.
1.144.170]

Trace complete.
```

Детализируем.



В приведённом выше примере пакеты, отправленные утилитой «tracert», пересылаются из ПК источника на основной шлюз локального маршрутизатора (переход 1: 192.168.1.1), а затем на маршрутизатор в точке подключения (POP) к интернет-провайдеру (переход 2: 10.18.20.1). У каждого провайдера есть множество маршрутизаторов POP. Они отмечают границы сети интернет-провайдера и служат точками подключения к Интернету для клиентов. Пакеты передаются по сети компании Verizon, пересекают два перехода и попадают в маршрутизатор, принадлежащий alter.net. Это может означать, что пакеты достигли другого интернет-провайдера. Этот момент очень важен, поскольку при пересылке пакетов от одного к другому провайдеру возможны потери, а также важно помнить, что не все интернет-провайдеры способны обеспечить одинаковую скорость передачи данных. Как определить, является ли alter.net тем же самым или другим интернет-провайдером?

Существует интернет-сервис whois, с помощью которого можно узнать владельца доменного имени. Сервис whois доступен по адресу http://whois.domaintools.com/. Согласно информации, полученной с помощью whois, домен alter.net также принадлежит компании Verizon.

Home > Whois Lookup > Alter.net

Whois Record for Alter.net

Domain Profile

Registrant Org	Verizon Business Global LLC
Registrant Country	us
Registrar	MarkMonitor, Inc. MarkMonitor Inc. IANA ID: 292

Таким образом, интернет-трафик начинается на домашнем ПК и проходит через домашний маршрутизатор (переход 1). Затем он подключается к интернет-провайдеру и передаётся по его сети (переходы 2–7), пока не достигнет удалённого сервера (переход 8). Это довольно нетипичный пример, в котором от начала до конца задействован только один провайдер. Чаще всего в пересылке данных участвуют два и более интернет- провайдеров.

Контрольные вопросы:

1) Напишите определение термина «Инфокоммуникационная сеть»
2) Какие топологии имеют локальные сети?
3) Из каких компонентов строятся сети ?
4) Возможно ли подменить свой IP-адрес? Возможно ли подменить MAC-адрес?
5) Чем IPv6 отличается от IPv4?
6) Какие преимущества IPv4? Какие преимущества IPv6?
7) Какая информация необходима, чтобы определить соответствующую схему адресации для сети?
8) После распределения подсетей будут ли все адреса узлов использоваться в каждой подсети?
9) Напишите частные IP адреса
10) Что такое NAT?

ЛАБОРАТОРНАЯ РАБОТА №4

Пакетные радиосети

Цель работы:

Получить навыки использования программы Wireshark для захвата IP-адресов пакетов данных и MAC-адресов Ethernet-кадров.

Подготовка к лабораторной работе:

1. Узнать о возможностях программы Wireshark.
2. Выяснить назначение протоколов ICMP, http, ftp, а также системы DNS.

Введение

Wireshark это программа для анализа протоколов (анализатор пакетов), которая используется для поиска и устранения неполадок в сети, анализа, разработки программного обеспечения и протоколов, а также обучения. По мере движения потоков данных по сети анализатор «захватывает» каждую единицу данных протокола (PDU), после чего расшифровывает или анализирует ее содержание согласно соответствующему документу RFC или другим спецификациям.

Wireshark – полезный инструмент для всех, кто работает с сетями. Его можно использовать для анализа данных, а также для поиска и устранения неполадок.

Значительно углубить понимание сетевых протоколов можно, если увидеть их в действии, пронаблюдав за последовательностью сообщений, которыми обмениваются два элемента протокола, если вникнуть в детали работы протокола, заставив его выполнять определенные действия и наблюдать за этими действиями и их результатами. Такое можно осуществить либо с помощью моделируемых сценариев, либо в реальной сетевой среде, такой, как Интернет.

В этой лабораторной работе вы познакомитесь с программой Wireshark и выполните несколько простых действий по захвату пакетов и наблюдению за ними. Основной инструмент для наблюдения за сообщениями, которыми обмениваются элементы исполняемого протокола, называется анализатор пакетов (или сниффер). Как следует из названия, он анализирует (перехватывает) сообщения, которые отправляются или получаются вашим компьютером; он также обычно сохраняет и/или отображает содержимое различных полей протокола этих перехваченных сообщений. Анализатор пакетов является пассивной программой. Он только следит за сообщениями, отправленными и полученными приложениями и протоколами, запущенными на вашем компьютере, но сам никогда не отправляет пакеты. Полученные

пакеты тоже никогда явно не адресуются анализатору. Он просто получает копию этих пакетов.

На рис. 1 показана структура анализатора пакетов.

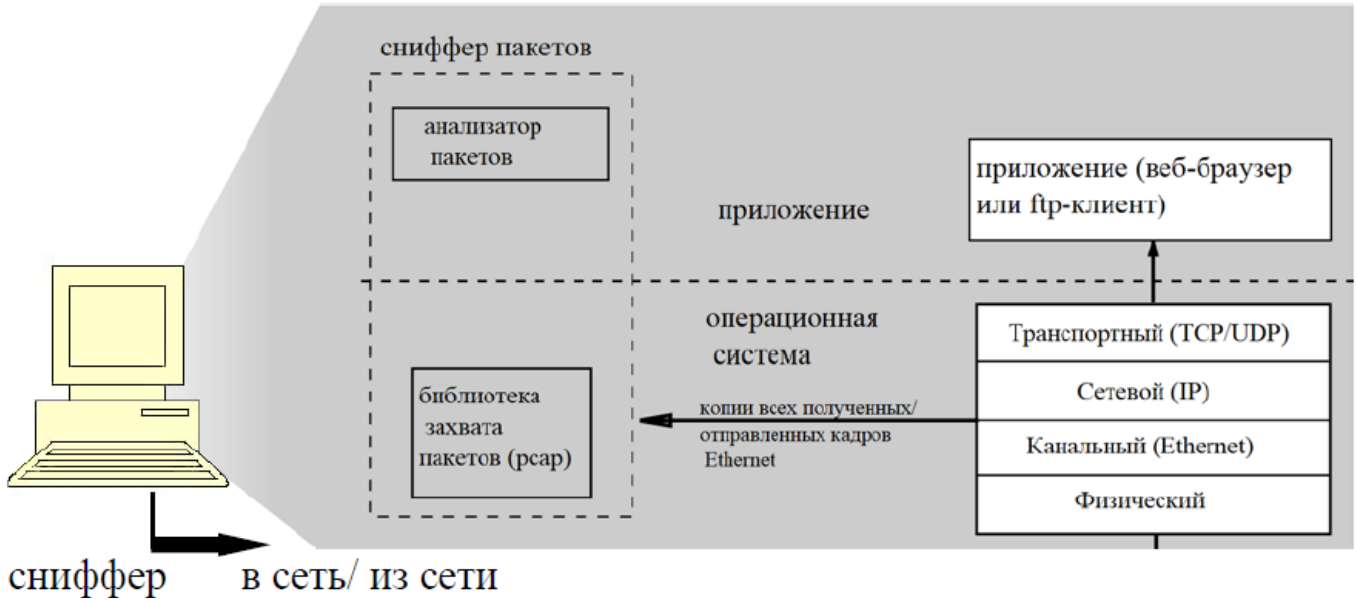


Рис. 1. Структура анализатора пакетов

В правой части рис.1 находятся протоколы (в данном случае, Интернет-протоколы) и приложения (например, веб-браузер или FTP-клиент), которые обычно работают на вашем компьютере. Анализатор пакетов (в пунктирном прямоугольнике) является дополнением к обычному программному обеспечению вашего компьютера и состоит из двух частей. Библиотека захвата пакетов получает копию каждого кадра канального уровня, который отправляется или получается компьютером.

Вспомним, что сообщения, которыми обмениваются протоколы более высокого уровня, такие как HTTP, FTP, TCP, UDP, DNS или IP, в конечном счете, заключены в кадры канального уровня, которые передаются через физический носитель, такой, как кабель Ethernet. На рис. 1 показано предположение, что физическим носителем является Ethernet, и поэтому все протоколы верхних уровней, в конечном счете, инкапсулируются в кадр Ethernet. Захват всех кадров канального уровня, таким образом, дает все сообщения, отправленные/полученные всеми протоколами и приложениями, выполняющимися на вашем компьютере.

Вторым компонентом является анализатор пакетов, который отображает содержимое всех полей в протокольном сообщении. Чтобы сделать это, анализатор пакетов должен «понимать» структуру всех сообщений, которыми обмениваются протоколы. Например, предположим, что мы хотим отобразить различные поля в сообщениях, которыми обменивается протокол HTTP на Рис. 1. Анализатор пакетов понимает формат Ethernet-кадров, и поэтому может идентифицировать IP-дейтаграммы внутри кадра Ethernet. Он также понимает формат IP-дейтаграммы, так что он может извлечь сегмент TCP из

IP-дейтаграммы. И, наконец, он понимает структуру сегмента TCP, поэтому он может извлечь сообщение HTTP, содержащееся в сегменте TCP. Наконец, он понимает протокол HTTP и поэтому, например, знает, что первые байты сообщения HTTP будут содержать строку GET, POST или HEAD.

Задание на лабораторную работу:

Задание 1

Сбор и анализ данных протокола ICMP в программе Wireshark

В части 1 этой лабораторной работы вы должны отправить эхо-запрос с помощью команды ping и перехватить ICMP-запросы и отклики в программе Wireshark. Кроме того,
вам нужно найти необходимую информацию в собранных кадрах. Этот анализ поможет понять, ка к
используются заголовки пакетов для передачи данных по месту назначения.

Шаг 1: Узнайте адреса интерфейсов своего ПК.

В данной лабораторной работе вам необходимо узнать IP-адрес компьютера и физический адрес сетевой интерфейсной платы (NIC), который называется MAC-адресом.

a. Откройте окно командной строки, введите команду **ipconfig /all** и нажмите клавишу ввода.

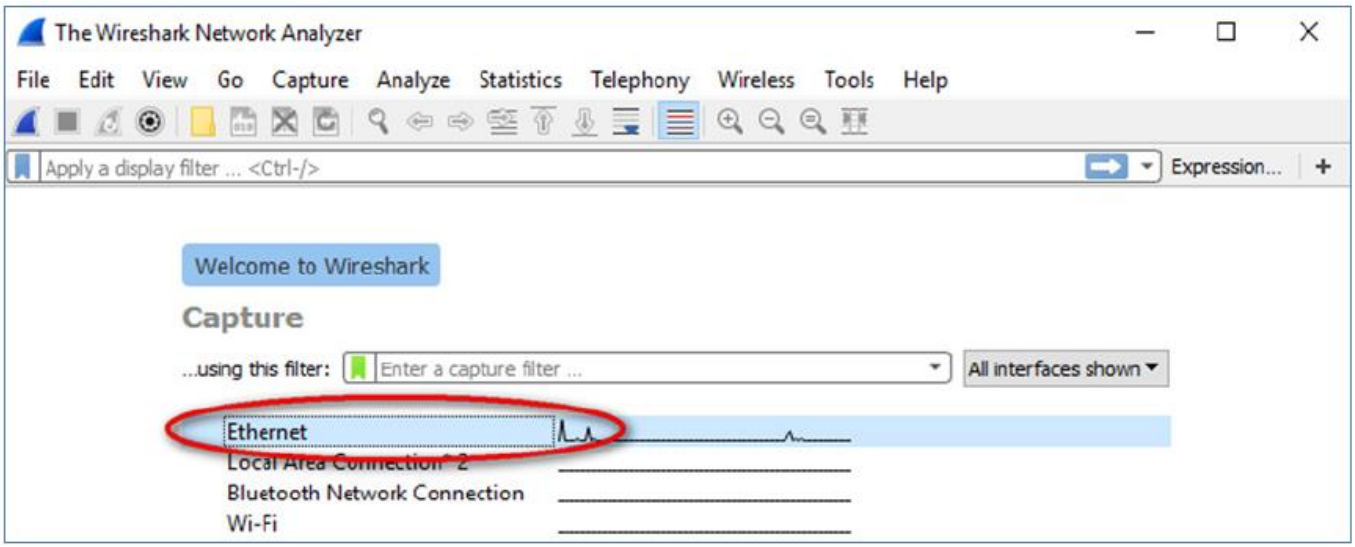
```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82577LM Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-26-B9-DD-00-91
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::d809:d939:110f:1b7f%20(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.147(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
```

b. Найти и записать MAC-адрес и IP-адрес сетевой интерфейсной платы своего ПК, IP-адрес указанного шлюза по умолчанию и IP-адрес DNS-сервера, указанного для ПК. Запишите эти данные в таблицу.

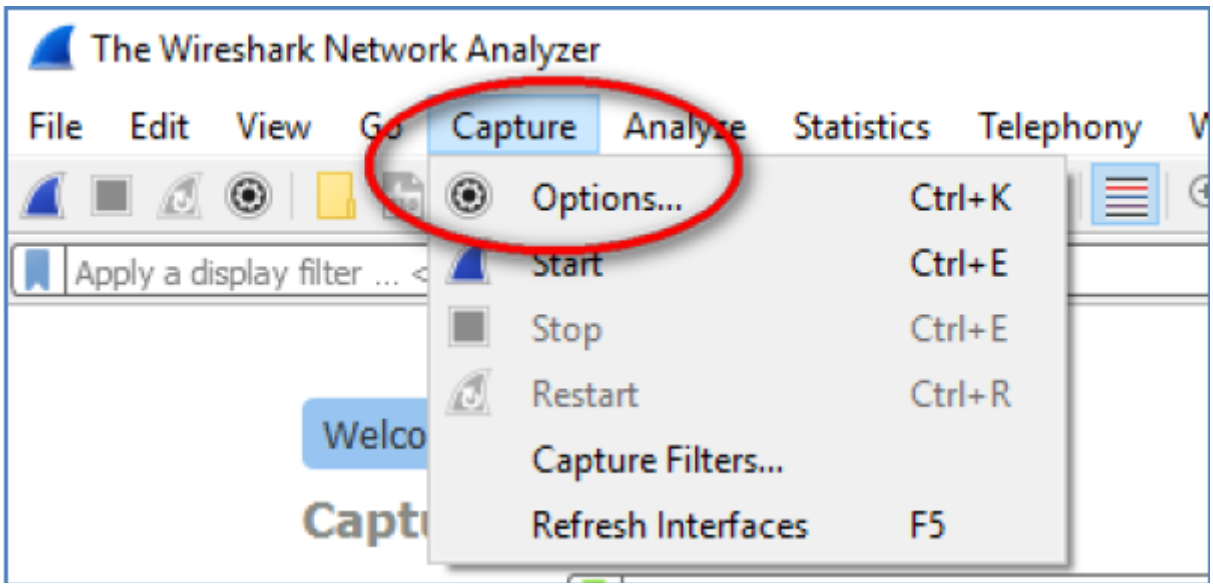
IP-адрес	
MAC-адрес	
IP-адрес шлюза по умолчанию	
IP-адрес DNS-сервера	

Шаг 2: Запустите программу Wireshark и начните сбор данных.

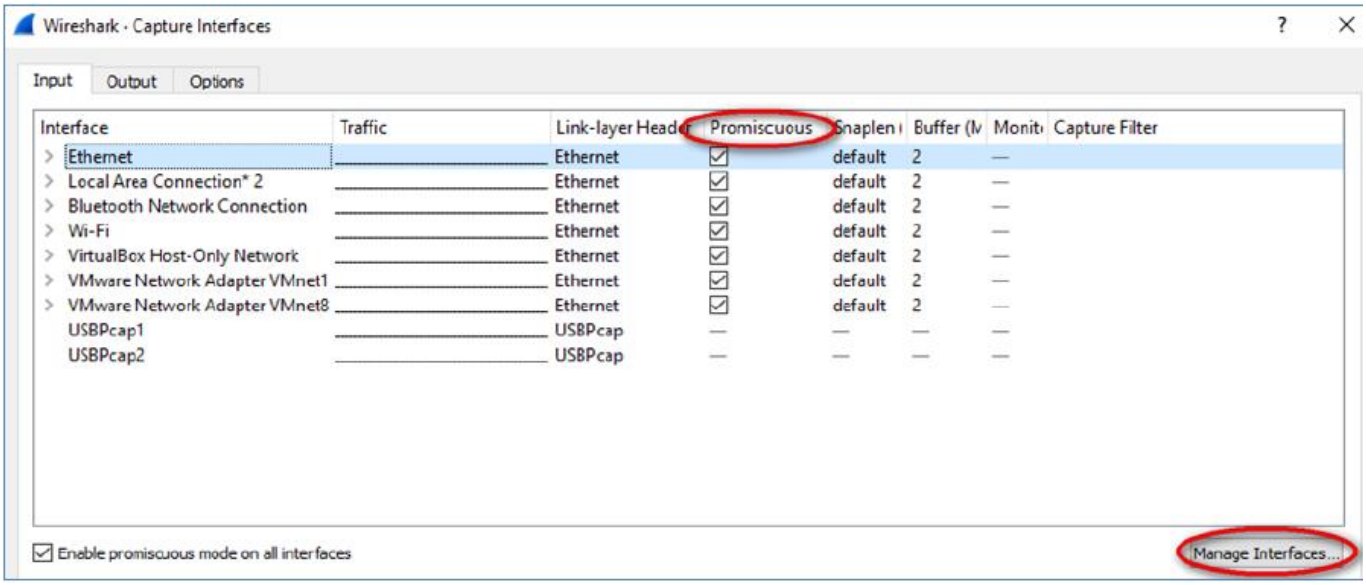
a. На своем ПК нажмите кнопку **Пуск** и найдите Wireshark в списке программ. Дважды нажмите на **Wireshark**.
b. После запуска Wireshark выберите интерфейс захвата трафика. Если на ПК используется подключение к проводной Ethernet-сети, выберете вариант Ethernet.



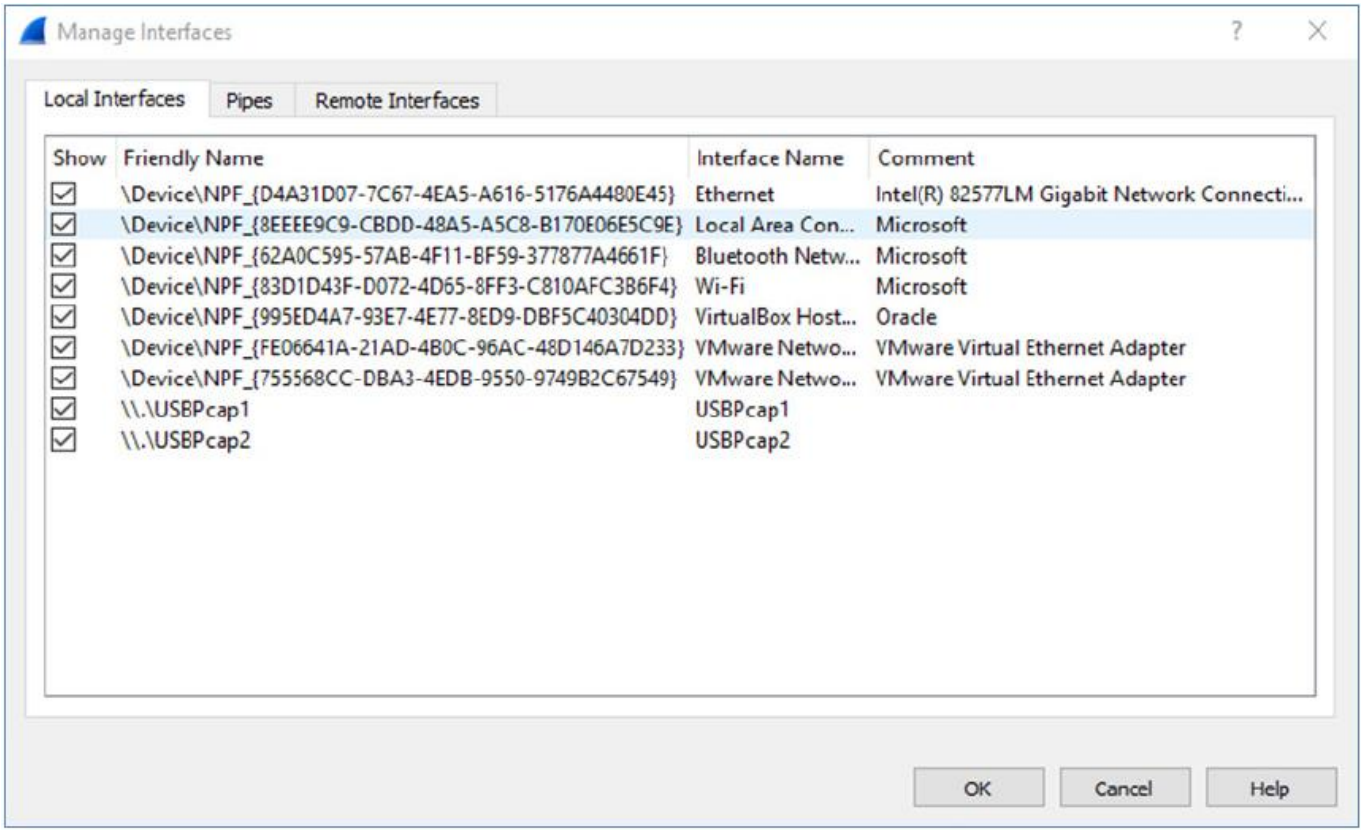
Для управления интерфейсом захвата трафика щелкните **Capture** (Захват), а затем **Options** (Параметры).



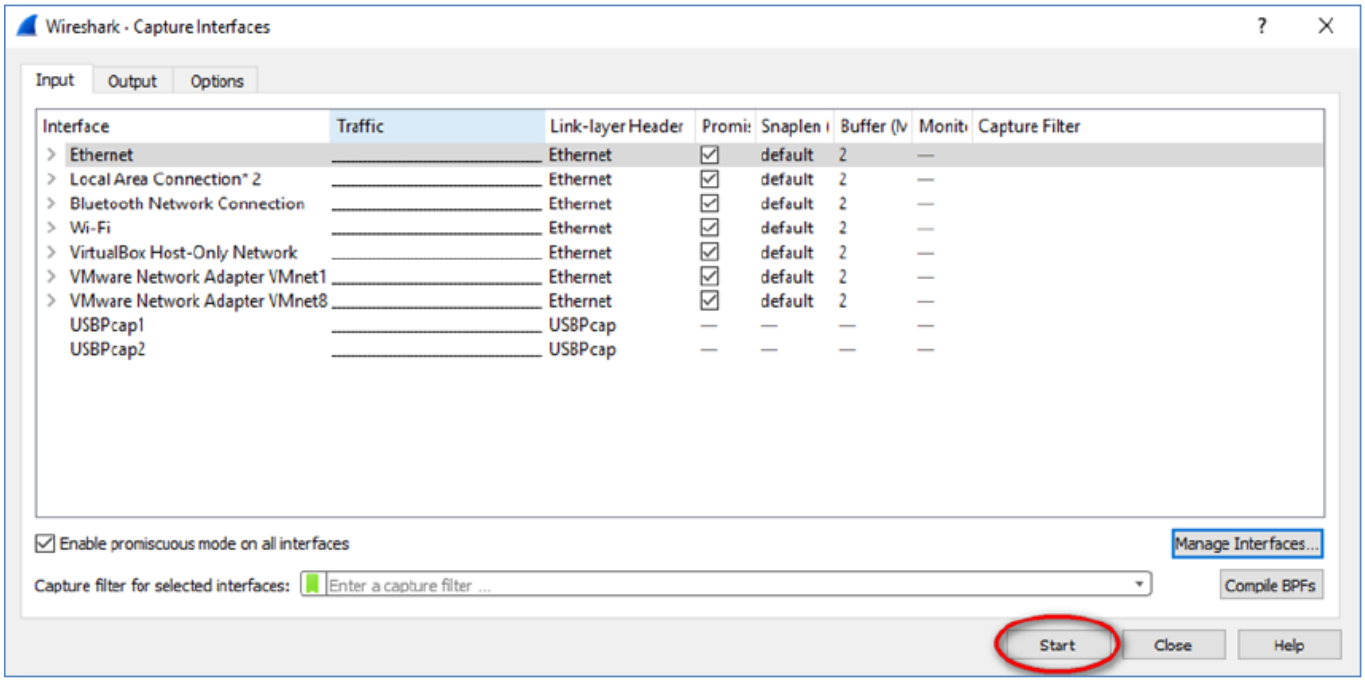
c. Отобразится список интерфейсов. Убедитесь, что в разделе **Promiscuous** (Неизбирательный) отмечен интерфейс захвата трафика.



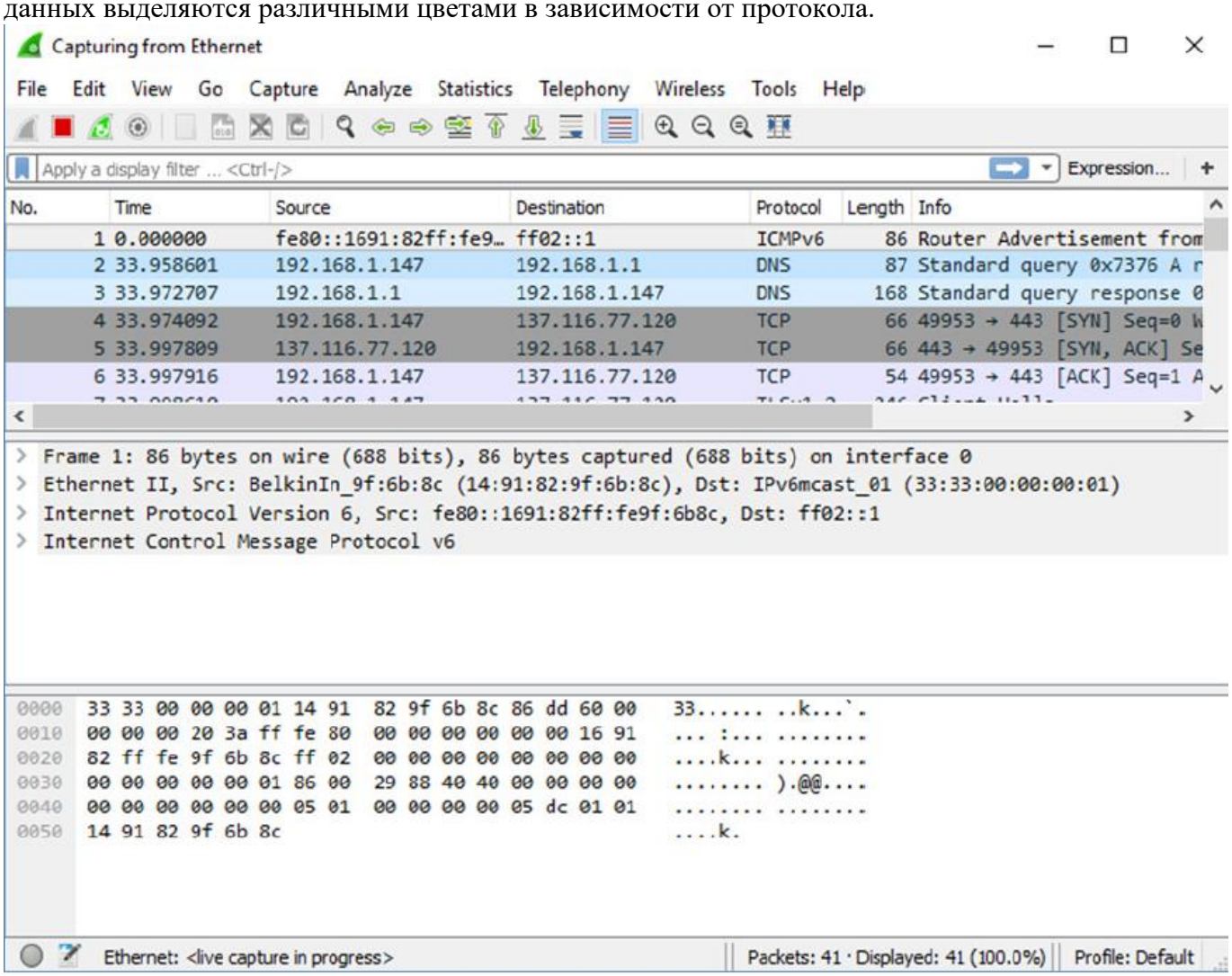
Примечание. Далее можно управлять интерфейсами на ПК, щелкнув **Manage Interfaces** (Управление интерфейсами). Убедитесь в том, что описание соответствует результату, который вы получили на шаге 1Б. Убедившись в правильности интерфейса, закройте окно **Manage Interfaces** (Управление интерфейсами).



d. После этого нажмите кнопку **Start** (Начать), чтобы начать захват данных.

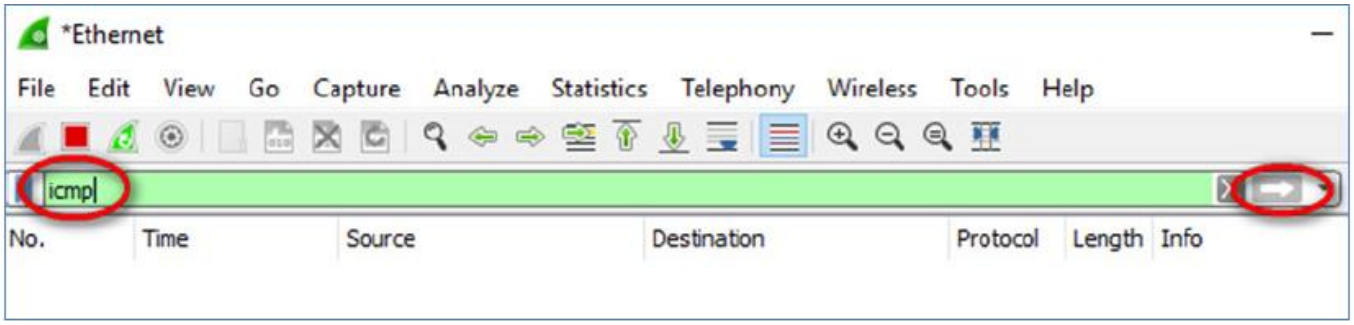


В верхней части окна программы Wireshark начнет прокручиваться информация. Строки данных выделяются различными цветами в зависимости от протокола.



е. Информация может прокручиваться очень быстро. Скорость прокрутки зависит от типа связи между ПК и сетью. Чтобы облегчить просмотр и работу с данными, собранными

программой Wireshark, можно применить фильтр. Например, для того чтобы вывести на экран только единицы данных протокола ICMP (ping-запрос), в поле **Filter** (Фильтр) в верхней части окна программы Wireshark введите **icmp** и нажмите клавишу **Enter** (Ввод) или кнопку **Apply** (Применить) (кнопка со значком стрелки).



f. После этого все данные в верхнем окне исчезнут, однако захват трафика в интерфейсе продолжится. Откройте окно командной строки, которое вы открывали ранее, и отправьте эхо-запрос с помощью команды ping на IP-адрес сайта Яндекса.

Обратите внимание на то, что в верхней части окна программы Wireshark снова появятся данные.

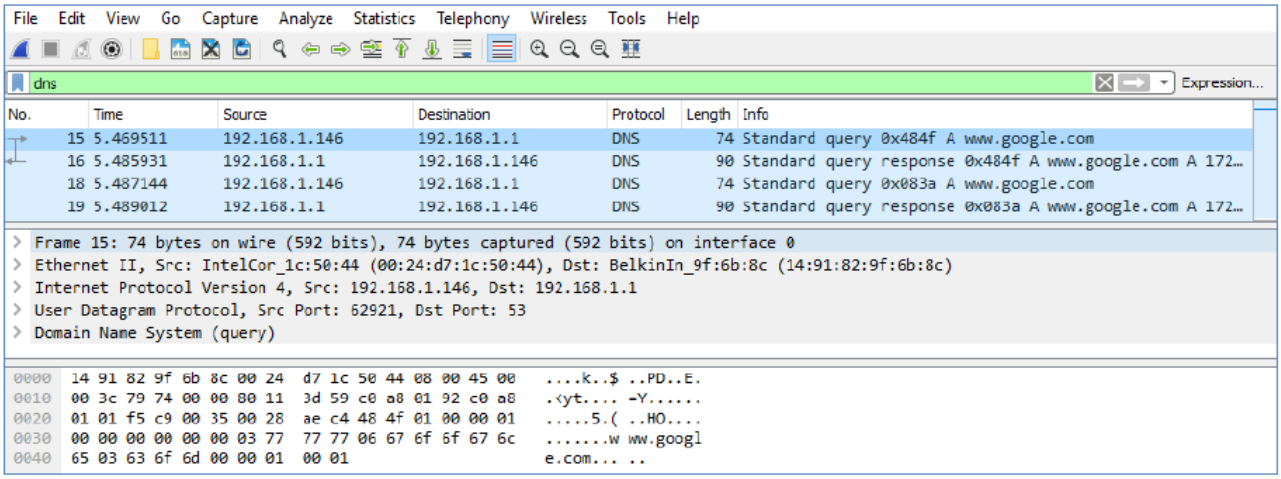
g. Остановите захват данных, нажав на значок **Stop Capture** (Остановить захват).

Изучение захваченных пакетов DNS и UDP с помощью программы Wireshark

Если вы хотя бы однажды выходили в Интернет, то пользовались системой доменных имен (DNS). DNS — это распределенная сеть серверов, которая преобразует понятные человеку имена доменов, например www.google.com, в IP-адреса. При вводе в браузере URL-адреса какого-либо веб-сайта компьютер отправляет DNS-запрос на IP-адрес DNS-сервера. При запросе компьютером DNS-сервера и ответе DNS-сервера в качестве протокола транспортного уровня используется протокол пользовательских датаграмм (UDP). В отличие от TCP, UDP является протоколом без установления соединения и не требует установления сеанса. Запросы и ответы DNS имеют чрезвычайно малый объем и не требуют использования служебной информации TCP.
В ходе лабораторной работы вы будете обмениваться данными с DNS-сервером, отправляя DNS-запросы с помощью транспортного протокола UDP. Для анализа обмена данными с сервером доменных имен будет использоваться программа Wireshark.

Шаг 1: Отфильтруйте DNS-пакеты. а. В главном окне программы Wireshark введите **dns** в поле **Filter** (Фильтр) инструментальной панели и нажмите **Enter** (Ввод).

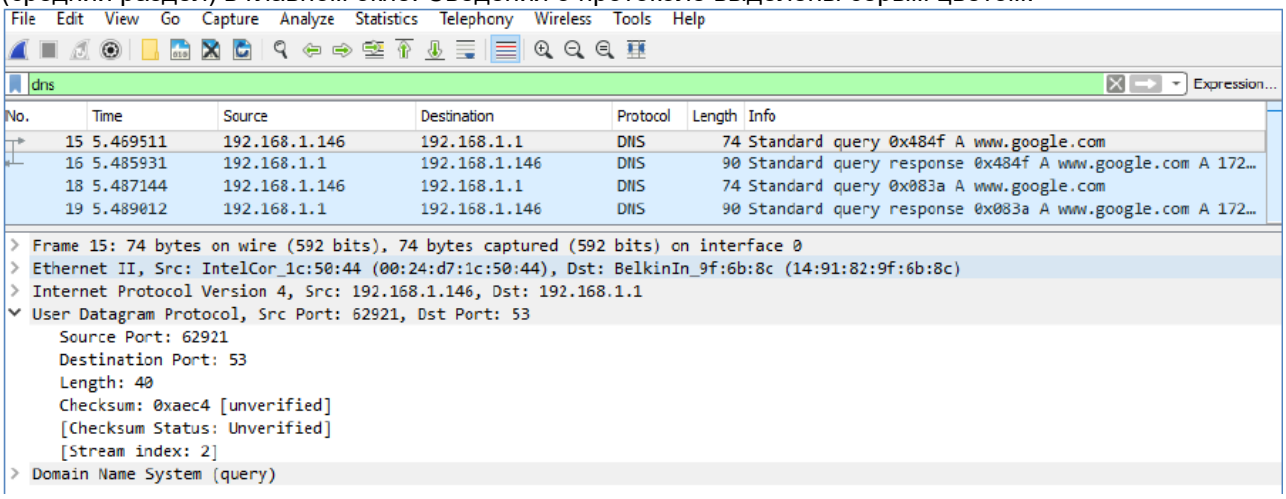
Примечание. Если после применения фильтра DNS вы не видите никаких результатов, закройте браузер. В окне командной строки введите **ipconfig /flushdns** для удаления всех предыдущих результатов DNS. Перезапустите захват данных программой Wireshark и повторите шаги 2Б — 2Д. Если таким образом решить проблему не удалось, то вместо использования браузера введите в окне командной строки команду**nslookup** www.google.com.



b. На панели списка пакетов (верхний раздел) в главном окне программы найдите пакет с информацией **Standard query** (Стандартный запрос) и **A www.google.com** (Запрос сайта google.com). В качестве примера можно взять кадр 15.

Шаг 2: Изучите сегмент UDP с помощью DNS-запроса.

Изучите данные UDP, используя DNS-запрос для адреса www.google.com, захваченный программой Wireshark. В данном примере для анализа выбран захваченный программой Wireshark кадр 15 на панели списка пакетов. Протоколы в этом запросе отображаются на панели сведений о пакетах (средний раздел) в главном окне. Сведения о протоколе выделены серым цветом.



a. Как показано в первой строке на панели сведений о пакетах, кадр 15 содержал 74 байта данных во время передачи. Это количество байтов нужно отправить в качестве DNS-запроса на сервер, который запрашивает IP-адреса сайта www.google.com.

b. Строка Ethernet II содержит MAC-адреса источника и места назначения. MAC-адрес источника принадлежит вашему локальному ПК как источнику DNS-запроса. MAC-адрес назначения — это шлюз по умолчанию, поскольку это последняя остановка перед выходом запроса из локальной сети. Совпадает ли MAC-адрес источника с адресом, записанным в части 1 для локального ПК?

c. В строке Internet Protocol Version 4 захваченные данные IP-пакета показывают, что IP-адрес источника данного DNS-запроса — 192.168.1.146, а IP-адрес назначения — 192.168.1.1. В данном примере адрес назначения — это шлюз по умолчанию. В данной сети шлюзом по умолчанию является маршрутизатор.

Можете ли вы указать IP-адрес и MAC-адрес для устройств источника и назначения?

Устройство	**IP-адрес**	**MAC-адрес**
Локальный ПК		
Шлюз по умолчанию		

СЕГМЕНТ UDP

0	16 31
ПОРТ ИСТОЧНИКА UDP	ПОРТ НАЗНАЧЕНИЯ UDP
ДЛИНА СООБЩЕНИЯ UDP	КОНТРОЛЬНАЯ СУММА UDP
ДАННЫЕ	
ДАННЫЕ...	

Разверните узел User Datagram Protocol на панели сведений о пакетах, нажав на значок «плюс» (+). Обратите внимание на то, что отображаются всего четыре поля. Номер порта источника в данном примере — 60868. Порт источника был случайно сгенерирован локальным ПК с использованием незарезервированных номеров портов. Порт назначения — 53. Порт 53 — это «хорошо известный порт», зарезервированный для использования с DNS. DNS-серверы прослушивают порт 53 для получения DNS-запросов от клиентов.

```
User Datagram Protocol, Src Port: 62921, Dst Port: 53
    Source Port: 62921
    Destination Port: 53
    Length: 40
    Checksum: 0xaec4 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 2]
```

Задание 2.

Перехват DNS-запроса, HTTP-запрос и DNS-ответа

Шаг 1: Вызвать меню настроек. Следующие опции должны быть активированы:

- Capture packets in promiscuous mode.
- Update list of packets in real time
- Automatic scrolling in live capture
- Enable MAC name resolution
- Enable network name resolution

В качестве интерфейса, используемого для захвата трафика выбрать физический (не виртуальный) адаптер и установить тип адаптера **Local**.

Шаг 2: Запустить процесс захвата трафика.

Для запуска процесса необходимо нажать кнопку **Start** в меню настроек.

Шаг 3: Настроить фильтрацию вывода по протоколам DNS и HTTP.

Для настройки фильтрации необходимо:

a. Ввести в поле фильтра выражение: “**dns || http**”.

b. Нажать кнопку **Apply.**

Шаг 4: Запустить обновление для вашего антивируса.

Шаг 5: Остановить захват трафика.

Для того чтобы остановить захват трафика, необходимо нажать кнопку **Stop** на панели инструментов, либо нажать **Capture** > **Stop**.

Шаг 4: Проанализировать трафик, захваченный программой.

При анализе трафика необходимо произвести следующие действия:

a. Среди PDU, захваченных программой, найти **DNS-запрос** (query) и **DNS-ответ** (query response).

```
DNS      Standard query A personal.avira-update.com
DNS      Standard query response A 80.190.143.236 A 80.190.143.233
```

b. Посмотрев содержимое DNS-запроса и DNS-ответа выяснить и записать в отчёт следующую информацию:

• DNS имя сервера обновлений антивируса.

• Любые 5 сетевых адресов сервера обновлений.

c. Среди PDU, захваченных программой, найти **HTTP-запрос** (HTTP GET).

d. Посмотрев содержимое PDU выяснить и записать в отчёт следующую информацию:

• Сетевой адрес сервера обновлений.

• Данные о вашем компьютере, которые программа обновления передала на сервер: версию Windows, месторасположение компьютера (Страна).

e. Изучив содержимое **DNS-запроса, HTTP-запрос** и **DNS-ответа** выяснить и записать в отчёт следующую информацию:

• Сетевой адрес компьютера.

• MAC-адрес компьютера.

• Сетевой адрес шлюза.

• MAC-адрес шлюза.

• IP-адрес прокси-сервера

• DNS имя прокси-сервера.

• Сетевой адрес DNS-сервера.

• Протокол транспортного уровня, который использует сервис DNS.

• Порт, на который осуществляется DNS-запрос.

• Протокол транспортного уровня, который использует протокол HTTP.

• Порт, на который осуществляется запрос обновления антивируса по протоколу HTTP.

Задание 3.

Перехват ftp-запроса

Шаг 1: Заново запустить захват трафика.

Для того, чтобы сохранить захваченный трафик, необходимо нажать кнопку **Restart** на панели инструментов, либо нажать **Capture** > **Restart**.

Шаг 2: Настроить фильтрацию вывода по протоколу FTP.

Для настройки фильтрации необходимо:

a. Ввести в поле фильтра выражение: "**ftp || ftp-data**".

b. Нажать кнопку **Apply.**

Шаг 3: Скачать файл с FTP-сервера.

Найдите адрес любого ftp сервера и введите в окне браузера его адрес:

ПРИМЕР: ftp:// --адрес-- /file.zip

Шаг 4: Проанализировать трафик, захваченный программой.

При анализе трафика необходимо произвести следующие действия:

a. Среди PDU, захваченных программой, найти **FTP Data**, содержащие скачиваемые с FTP-сервера данные.

b. Посмотрев содержимое **FTP Data** выяснить и записать в отчёт следующую информацию:

- Сколько байт данных содержится в одном PDU
- Сетевой адрес FTP-сервера.
- MAC-адрес FTP-сервера
- Протокол транспортного уровня, который использует протокол FTP.
- Порт, который используется при передаче данных по протоколу FTP.

Протокол TCP, как правило, используется во время сеанса связи для управления доставкой датаграмм, проверки их получения и регулировки размера окна. Для каждого обмена данными между FTP-клиентом и FTP-сервером запускается новый сеанс TCP. По завершении передачи данных сеанс TCP закрывается. По завершении сеанса FTP протокол TCP выполняет плановое отключение и прекращение работы.

Программа Wireshark отображает подробные данные TCP на панели сведений о пакетах (средний раздел). Выделите первую датаграмму TCP с узлового компьютера и разверните ее. Откроется развернутая датаграмма TCP аналогично показанной ниже панели сведений о пакетах.

```
> Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
> Ethernet II, Src: IntelCor_1c:50:44 (00:24:d7:1c:50:44), Dst: BelkinIn_9f:6b:8c (14:91:82:9f:6b:8c)
> Internet Protocol Version 4, Src: 192.168.1.146, Dst: 198.246.117.106
v Transmission Control Protocol, Src Port: 54712, Dst Port: 21, Seq: 0, Len: 0
    Source Port: 54712
    Destination Port: 21
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Acknowledgment number: 0
    1000 .... = Header Length: 32 bytes (8)
  v Flags: 0x002 (SYN)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...0 .... = Acknowledgment: Not set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
    > .... .... ..1. = Syn: Set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ··********S·]
    Window size value: 8192
    [Calculated window size: 8192]
    Checksum: 0x13e8 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
```

На приведенном выше изображении показана схема датаграммы TCP. Для большей ясности к каждому полю приводится пояснение.

• Поле **TCP Source Port Number** (Номер порта источника TCP) относится к хосту сеанса TCP, который открыл соединение. В качестве значения обычно используется произвольное число больше 1023.

• Поле **TCP Destination Port Number** (Номер порта назначения TCP) используется для идентификации протокола верхнего уровня или приложения на удаленном сайте. Значения в диапазоне от 0 до 1023 соответствуют «хорошо известным портам» и связаны с популярными сервисами и приложениями (как описано в документе RFC 1700), например Telnet, FTP и HTTP. Комбинация IP-адреса источника, порта источника, IP-адреса назначения и порта назначения однозначно определяет сеанс как для отправителя, так и для получателя.

Примечание. В приведенных ниже данных, захваченных программой Wireshark, указан порт назначения 21, который используется для FTP. FTP-серверы прослушивают порт 21 для подключений FTP-клиентов.

Используя данные, захваченные программой Wireshark при запуске первого сеанса TCP (бит SYN установлен в значение 1), заполните информацию о заголовке TCP.

От ПК к серверу CDC (только бит SYN установлен в значение 1):

№	Поле	Значение
1.	IP-адрес источника	
2.	IP-адрес назначения	
3.	Номер порта источника	
4.	Номер порта назначения	
5.	Порядковый номер	
6.	Длина заголовка	

ЛИТЕРАТУРА

Основная:

1) Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. — СПб.: Питер, 2012. — 960 с.

2) Короуз Д. Компьютерные сети. Нисходящий подход. – М. : Издательство «Э», 2016 г. – 912 с.

3) Олейник П. Корпоративные информационные системы. Учебник для вузов. Стандарт третьего поколения. – СПб. : Питер, 2011 г. – 176 с.

4) Величко В. В. Основы инфокоммуникационных технологий: учеб. пособие для вузов / В. В. Величко, Г. П. Катунин, В. П. Шувалов. - М.: Горячая линия - Телеком, 2015.