ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Иркутский государственный университет путей сообщения»
Сибирский колледж транспорта и строительства

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

К ПРАКТИЧЕСКИМ РАБОТАМ

ПМ.01 ВЫПОЛНЕНИЕ РАБОТ ПО ПРОЕКТИРОВАНИЮ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

МДК.01.01 Компьютерные сети
Тема 1.1. Введение в сетевые технологии

по специальности
09.02.06 Сетевое и системное администрирование

базовая подготовка среднего профессионального образования

Иркутск 2022

РАССМОТРЕНО:
Цикловой методической
комиссией специальности 09.02.06
Сетевое и системное
администрирование
«08» июня 2022 г.
Председатель: _____/Саквенко Т.В.

СОГЛАСОВАНО:
Заместитель директора по УВР
_____/А.П.Ресельс
«09» июня 2022 г.

Разработчики: Фитисова Н.Н., преподаватель высшей категории Сибирского колледжа транспорта и строительства ФГБОУ ВО «Иркутский государственный университет путей сообщения».

Практическая работа 1: составление карты сети Интернет

Задачи

Часть 1. Проверка подключения к сети с помощью эхо-запроса с помощью команды ping

Часть 2. Отслеживание маршрута к удалённому серверу с помощью утилиты Windows «traceroute»

Часть 3. Отслеживание маршрута к удалённому серверу с помощью программных и веб- средств

Часть 4. Сравнение результатов трассировки Исходные данные

Программное обеспечение для трассировки маршрута — это утилита, содержащая списки сетей, по которым должны пройти данные от отправляющего оконечного устройства пользователя до удалённой сети назначения.

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 этой функции существует несколько средств.

Инструмент traceroute (или 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 «полно связным» характером взаимно подключённых сетей, состоящих из возможностей Интернета и протоколов Интернета выбирать различные кабельные каналы для отправки пакетов.

Средства трассировки маршрута с использованием командной строки обычно заложены в операционную систему оконечного устройства.

Другие инструменты, такие как Visual Route™, являются пропри

VisualRoute Lite Edition	Windows XP\2003\Vista\7	4.0Mb	Downloa
	Mac OS X (dmg) 10.3+, universal binary	2.0Mb	Downloa

тарными программами и позволяют получать более подробную информацию. Visual Route формирует графическое отображение маршрута, используя доступную информацию в сети.

Для выполнения данной лабораторной работы необходима программа Visual Route. Если на вашем компьютере программа Visual Route не установлена, загрузите её по следующей ссылке:

http://www.visualroute.com/download.htm

Сценарий

Используя интернет-подключение и три различных утилиты трассировки маршрута, вы должны будете отследить путь прохождения пакетов данных через Интернет к сетям назначения. Для этого вам потребуется компьютер, подключение к Интернету и доступ к командной строке. Сначала вы воспользуетесь утилитой «tracert», встроенной в ОС Windows, затем веб-средством для трассировки маршрута (http://www.subnetonline.com/pages/network-tools/online-traceroute.php) и, наконец, программой Visual Route.

Необходимые ресурсы

1 ПК (Windows 7, Vista или XP с выходом в Интернет)

Часть 1: Проверка подключения к сети посредством эхо-запроса с помощью команды ping

Шаг 1: Определите, доступен ли удалённый сервер.

Для трассировки маршрута к удалённой сети используемый ПК должен быть подключён к Интернету.

a. Сначала мы воспользуемся эхо-запросом с помощью команды ping. 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.

b. Нажмите кнопку Пуск на экране компьютера, введите команду cmd в поле Найти программы и файлы и нажмите клавишу ВВОД.

c. 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
```

d. В первой строке полученных данных отображается полное доменное имя (FQDN) e144.dscb.akamaiedge.net. Затем следует IP-адрес 23.1.48.170. Веб-узлы компании Cisco, содержащие одну и ту же

```
C:\>ping www.apnic.net

Pinging www.apnic.net [202.12.29.194] with 32 bytes of data:
Reply from 202.12.29.194: bytes=32 time=286ms TTL=49
Reply from 202.12.29.194: bytes=32 time=287ms TTL=49
Reply from 202.12.29.194: bytes=32 time=286ms TTL=49
Reply from 202.12.29.194: bytes=32 time=286ms TTL=49

Ping statistics for 202.12.29.194:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 286ms, Maximum = 287ms, Average = 286ms
```

Результат будет выглядеть следующим образом.

```
Ping statistics for 23.45.0.170:
    Packets: Sent = 100, Received = 100, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 46ms, Maximum = 53ms, Average = 49ms
```

```
C:\>ping -n 100 www.cisco.com
```

информацию, размещаются на различных серверах (так называемых зеркалах) по всему миру. Это значит, что имя FQDN и IP-адрес будут отличаться в зависимости от вашего местонахождения.

e. Возьмём приведённую ниже часть полученных результатов.

Из неё видно, что были отправлены четыре эхо-запроса с помощью команды ping, на каждый из которых был получен ответ. Ответ поступил на все эхо-запросы с помощью команды ping, значит, потери пакетов нет (0 % потерь). В среднем для передачи пакетов по сети требуется 54 мс (миллисекунды). Миллисекунда — это 1/1000 секунды.

От потери пакетов или медленного сетевого подключения в первую очередь страдает качество потокового видео и онлайн-игр. Чтобы

```
C:\>ping www.afrinic.net

Pinging www.afrinic.net [196.216.2.136] with 32 bytes of data:
Reply from 196.216.2.136: bytes=32 time=314ms TTL=111
Reply from 196.216.2.136: bytes=32 time=312ms TTL=111
Reply from 196.216.2.136: bytes=32 time=313ms TTL=111
Reply from 196.216.2.136: bytes=32 time=313ms TTL=111

Ping statistics for 196.216.2.136:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 312ms, Maximum = 314ms, Average = 313ms
```

Австралия:

C:\> ping www.apnic.net

определить скорость интернет-подключения более точно, можно отправить не 4 эхо-запроса с помощью команды ping, предусмотренных по

Европа:

C:\> ping www.ripe.net

```
C:\>ping www.ripe.net

Pinging www.ripe.net [193.0.6.139] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 193.0.6.139:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
Reply from 200.3.14.147: bytes=32 time=158ms TTL=51
Reply from 200.3.14.147: bytes=32 time=158ms TTL=51
Reply from 200.3.14.147: bytes=32 time=157ms TTL=51

Ping statistics for 200.3.14.147:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 157ms, Maximum = 158ms, Average = 157ms
```

умолчанию, а 100. Для этого используется указанная ниже команда.

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

Африка:

C:\> ping www.afrinic.net

Южная Америка:

C:\> ping lacnic.net

Все эти эхо-запросы с помощью команды ping были отправлены с компьютера, расположенного в США. Что происходит со средним временем эхо-запроса (в миллисекундах), когда данные передаются в пределах одного континента (Северной Америки), по сравнению с ситуацией, когда данные из Северной Америки пересылаются на другие континенты?

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

Часть 2: Отслеживание маршрута к удалённому серверу с помощью утилиты «traceroute»

Шаг 1: Определите, какой маршрут из всего интернет-трафика направлен к удалённому серверу.

Проверив достижимость с помощью утилиты «ping», стоит более внимательно рассмотреть каждый сегмент сети, через который проходят данные. Для этого воспользуемся утилитой tracert.

a. В командной строке введите tracert www.cisco.com.

```
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.
```

b. 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) Откройте Блокнот Windows. Для этого нажмите кнопку Пуск и выберите Все программы > Стандартные > Блокнот.

4) Чтобы вставить данные в Блокнот, выберите в меню Правка команду Вставить.

5) В меню Файл выберите команду Сохранить как и сохраните файл Блокнота на рабочий стол с названием tracert1.txt.

c. Запустите утилиту tracert для каждого веб-сайта назначения и сохраните полученные результаты в последовательно пронумерованные файлы.

C:\> tracert www.afrinic.net C:\> tracert www.lacnic.net

d. 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 к www.cisco.com. Ниже представлен весь маршрут трассировки.

```
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  delrouter.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 «tracer!», 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-провайдера способны обеспечить одинаковую скорость передачи данных. Как определить, является ли alter.net тем же самым или другим Интернет-провайдером?

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

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. Как видно из следующих примеров, чаще всего в пересылке данных участвуют два и более интернет- провайдеров.

f. Теперь рассмотрим пример с пересылкой интернет-трафика через несколько интернет-

провайдеров. Ниже представлены результаты применения утилиты «tracert» к узлу www.afrinic.net.

```
C:\>tracert www.afrinic.net

Tracing route to www.afrinic.net [196.216.2.136]
over a maximum of 30 hops:

  1     1 ms    <1 ms    <1 ms  dslrouter.westell.com [192.168.1.1]
  2    39 ms    38 ms    37 ms  10.18.20.1
  3    40 ms    38 ms    39 ms  G4-0-0-2204.ALBYNY-LCR-02.verizon-gni.net [130.8
1.197.182]
  4    44 ms    43 ms    43 ms  so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81
.22.46]
  5    43 ms    43 ms    42 ms  0.so-4-0-0.XT2.NYC4.ALTER.NET [152.63.9.249]
  6    43 ms    71 ms    43 ms  0.ae4.BR3.NYC4.ALTER.NET [152.63.16.185]
  7    47 ms    47 ms    47 ms  te-7-3-0.edge2.NewYork2.level3.net [4.68.111.137
]
  8    43 ms    55 ms    43 ms  vlan51.ebr1.NewYork2.Level3.net [4.69.138.222]
  9    52 ms    51 ms    51 ms  ae-3-3.ebr2.Washington1.Level3.net [4.69.132.89]

 10   130 ms   132 ms   132 ms  ae-42-42.ebr2.Paris1.Level3.net [4.69.137.53]
 11   139 ms   145 ms   140 ms  ae-46-46.ebr1.Frankfurt1.Level3.net [4.69.143.13
7]
 12   148 ms   140 ms   152 ms  ae-91-91.csw4.Frankfurt1.Level3.net [4.69.140.14
]
 13   144 ms   144 ms   146 ms  ae-92-92.ebr2.Frankfurt1.Level3.net [4.69.140.29
]
 14   151 ms   150 ms   150 ms  ae-23-23.ebr2.London1.Level3.net [4.69.148.193]

 15   150 ms   150 ms   150 ms  ae-58-223.csw2.London1.Level3.net [4.69.153.138]

 16   156 ms   156 ms   156 ms  ae-227-3603.edge3.London1.Level3.net [4.69.166.1
54]
 17   157 ms   159 ms   160 ms  195.50.124.34
 18   353 ms   340 ms   341 ms  168.209.201.74
 19   333 ms   333 ms   332 ms  csw4-pkl-gi1-1.ip.isnet.net [196.26.0.101]
 20   331 ms   331 ms   331 ms  196.37.155.180
 21   318 ms   316 ms   318 ms  fa1-0-1.ar02.jnb.afrinic.net [196.216.3.132]
 22   332 ms   334 ms   332 ms  196.216.2.136

Trace complete.
```

Что происходит в переходе 7? Является ли level3.net тем же самым Интернет-провайдером, что и в переходах 2-6? Чтобы ответить на этот вопрос, воспользуйтесь сервисом who is.

Как меняется время, необходимое для пересылки пакета данных между Вашингтоном и Парижем в переходе 10 по сравнению с предыдущими переходами 1-9?

Что происходит в переходе 18? С помощью сервиса who is выполните поиск по адресу 168.209.201.74. Кто является владельцем этой сети?

g. Введите команду tracert www.lacnic.net.

```
C:\>tracert www.lacnic.net

Tracing route to www.lacnic.net [200.3.14.147]
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    38 ms    38 ms    39 ms  G3-0-9-2204.ALBYNY-LCR-02.verizon-gni.net [130
1.196.190]
  4    42 ms    43 ms    42 ms  so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.
.22.46]
  5    82 ms    47 ms    47 ms  0.ae2.BR3.NYC4.ALTER.NET [152.63.16.49]
  6    46 ms    47 ms    56 ms  204.255.168.194
  7   157 ms   158 ms   157 ms  ge-1-1-0.100.gw1.gc.registro.br [159.63.48.38]
  8   156 ms   157 ms   157 ms  xe-5-0-1-0.core1.gc.registro.br [200.160.0.174

  9   161 ms   161 ms   161 ms  xe-4-0-0-0.core2.nu.registro.br [200.160.0.164

 10   158 ms   157 ms   157 ms  ae0-0.ar3.nu.registro.br [200.160.0.249]
 11   176 ms   176 ms   170 ms  gw02.lacnic.registro.br [200.160.0.213]
 12   158 ms   158 ms   158 ms  200.3.12.36
 13   157 ms   158 ms   157 ms  200.3.14.147

Trace complete.
```

Что происходит в переходе 7?

Часть 3: Отслеживание маршрута к удалённому серверу с помощью программных и веб-средств

Шаг 1: Воспользуйтесь веб-средством для трассировки маршрута.

a. С помощью сайта http://www.subnetonline.com/pages/network-tools/online-tracepath.php отследите маршрут к следующим веб-сайтам:

www.cisco.com

www.afrinic.net

Скопируйте данные и сохраните их в файл Блокнота.

Как меняется трассировка маршрута при переходе на www.cisco.com из командной строки (см. часть 1), а не через веб-сайт? (Полученные результаты могут изменяться в зависимости от местонахождения и того, с каким Интернет-провайдером работает ваше учебное заведение.)

Сравните результаты трассировки маршрута в Африку из части 1 с результатами трассировки того же маршрута через веб-интерфейс. Какую разницу вы заметили?

В некоторых результатах трассировки маршрута можно увидеть сокращение «asymm». Есть идеи, что оно может означать? В чём его смысл?

Шаг 2: Работа с программой Visual Route Lite Edition

Visual Route — это пропри тарная программа, позволяющая отобразить результаты трассировки маршрута наглядно.

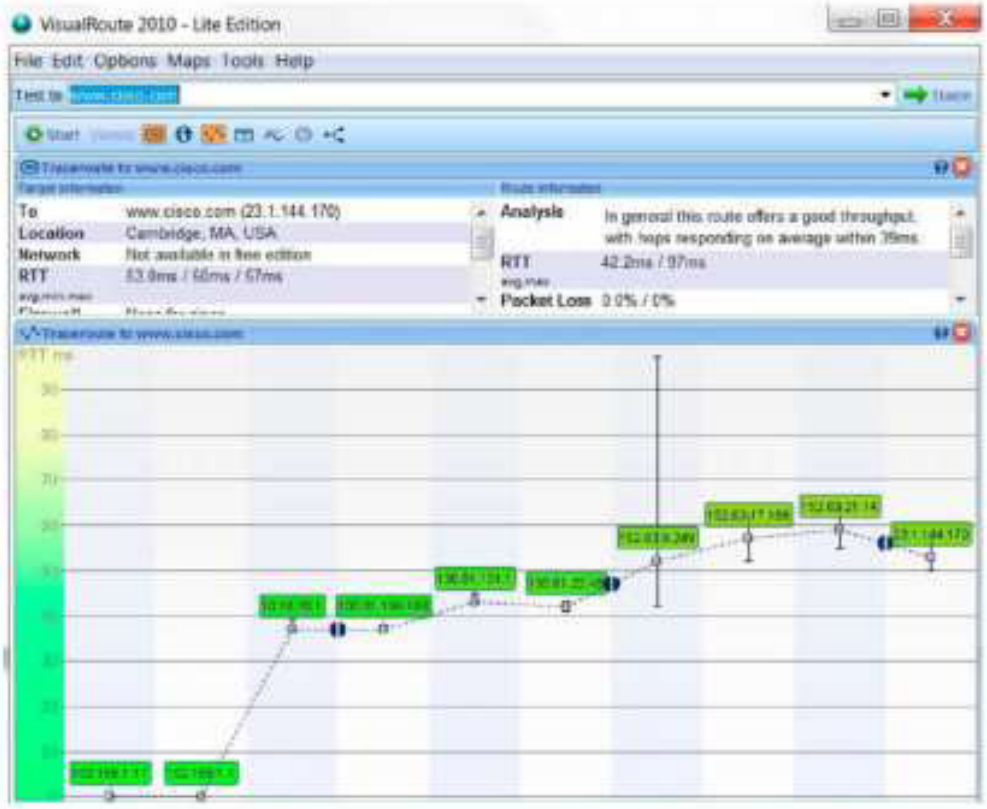
a. Если программа Visual Route Lite Edition на вашем компьютере не установлена, загрузите ее по следующей ссылке:

http://www.visualroute.com/download.html

Если с загрузкой или установкой программы Visual Route возникнут проблемы, обратитесь за помощью к инструктору. Убедитесь, что выполняется загрузка Lite Edition.

b. С помощью программы Visual Route 2010 Lite Edition отследите маршруты к www.cisco.com.

c. Сохраните полученные IP-адреса в файле Блокнота.



Часть 4: Сравнение результатов трассировки

Сравните результаты трассировки маршрута к www.cisco.com, полученные в частях 2 и 3.

Шаг 1: Перечислите адреса на маршруте к www.cisco.com, полученные с помощью утилиты «tracert».

Шаг 2: Перечислите адреса на маршруте к www.cisco.com, полученные с помощью веб- сервиса subnetonline.com.

Шаг 3: Перечислите адреса на маршруте к www.cisco.com, полученные с помощью программы Visual Route Lite Edition.

Все ли инструменты для трассировки использовали одни и те же маршруты к www.cisco.com? Поясните свой ответ.

Вопросы на закрепление

Вы воспользовались тремя различными средствами для трассировки маршрута (утилита «tracert», веб-интерфейс и программа Visual Route). Можно ли считать, что программа Visual Route позволяет получить какие-либо сведения, не предоставляемые двумя другими инструментами?

Практическая работа 2: создание простой сети
Топология

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
S1	VLAN 1	Недоступно	Недоступно	Недоступно
S2	VLAN 1	Недоступно	Недоступно	Недоступно
ПК-А	Сетевой адаптер	192.168.1.10	255.255.255.0	Недоступно
ПК-Б	Сетевой адаптер	192.168.1.11	255.255.255.0	Недоступно

Задачи

Часть 1. Настройка топологии сети (только Ethernet)

- Укажите, какие кабели и порты должны использоваться в сети.
- Проложите кабели между устройствами. **Часть 2. Настройка узлов ПК**
- Настройте на узлах статический IP-адрес на интерфейсах, которые подключены к локальной сети.
- **Проверьте связь между компьютерами с помощью утилиты** ping. Часть 3. Настройка и проверка основных параметров коммутатора
- Настройте имя узла, локальные пароли и баннер входа в систему для каждого коммутатора.
- Сохраните текущие конфигурации.
- Отобразите текущую конфигурацию коммутатора.
- Отобразите версию IOS текущего коммутатора.
- Отобразите статус интерфейсов.

Исходные данные/сценарий

Сети состоят из трёх основных компонентов: узлов, коммутаторов и маршрутизаторов. В этой лабораторной работе вам предстоит построить простую сеть с двумя узлами и двумя коммутаторами и настроить основные

параметры, включая имя узла, локальные пароли и баннер входа в систему. С помощью команды **show** отобразите текущую конфигурацию, версию IOS и состояние интерфейса. С помощью команды **copy** сохраните конфигурации устройств.

В данной лабораторной работе вам нужно применить к компьютерам IP-адресацию и обеспечить соединение между этими двумя устройствами. Для проверки подключения используйте утилиту **ping.**

Примечание. Используются коммутаторы: Cisco Catalyst 2960s с операционной системой Cisco IOS версии 15.0(2) (образ lanbasek9). Можно использовать другие коммутаторы и версии ПО Cisco IOS. В зависимости от модели и версии Cisco IOS выполняемые доступные команды и выводы могут отличаться от данных, полученных в ходе лабораторных работ.

Примечание. Коммутаторы необходимо очистить от данных и загрузочной конфигурации. Процедура инициализации и перезагрузки коммутатора описана в приложении А.

Необходимые ресурсы

- 2 коммутатора (Cisco 2960, ПО CISCO IOS версии 15.0(2), образ lanbasek9 или аналогичный)
- 2 ПК (Windows 7, Vista и XP с программой эмуляции терминала, например Tera Term)
- Консольные кабели для настройки устройств CISCO IOS через консольные порты
- Кабели Ethernet в соответствии с топологией

Часть 1: Настройка топологии сети (только Ethernet)

В части 1 вам необходимо проложить кабели между устройствами в соответствии с топологией сети.

Шаг 1: Включите устройства.

Включите все устройства в топологии. Коммутаторы не имеют кнопок включения и включаются при подключении шнура питания.

Шаг 2: Соедините два коммутатора.

Подключите один конец кабеля Ethernet к разъёму F0/1 на коммутаторе S1, а другой — к разъёму F0/1 на коммутаторе S2. Лампочки разъёмов F0/1 на обоих коммутаторах загорятся жёлтым, а потом зелёным цветом. Это означает, что коммутаторы подключены правильно.

Шаг 3: Подсоедините компьютеры к соответствующим коммутаторам.

a. Подключите один конец второго кабеля Ethernet к порту сетевого адаптера ПК-А. Другой конец кабеля подключите к разъёму F0/6 на коммутаторе S1. После подключения ПК к коммутатору лампочка разъёма F0/6 загорится сначала жёлтым, а затем зелёным цветом, означающим, что ПК- А подключён правильно.

b. Подключите один конец последнего кабеля Ethernet к порту сетевого адаптера ПК-Б. Подключите другой конец кабеля к разъёму F0/18 на коммутаторе S2. После подключения ПК к коммутатору лампочка

разъёма F0/18 загорится сначала жёлтым, а затем зелёным цветом, означающим, что ПК-Б подключён правильно.

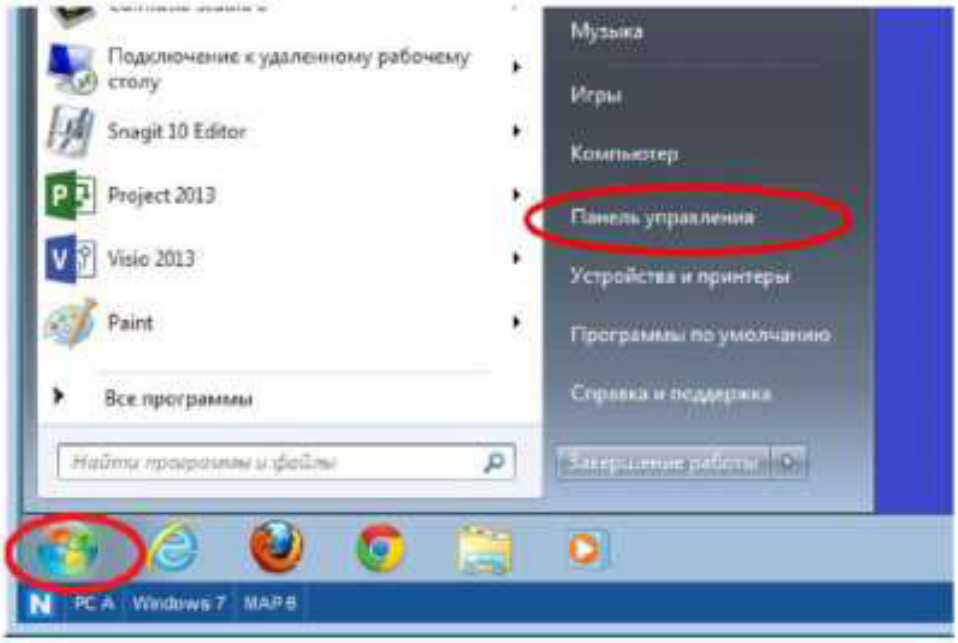
Шаг 4: Осмотрите сетевые соединения.

После подведения кабелей к сетевым устройствам тщательно проверьте соединения, чтобы впоследствии сократить время поиска и устранить неполадки с сетевым подключением.

Часть 2: Настройка узлов ПК

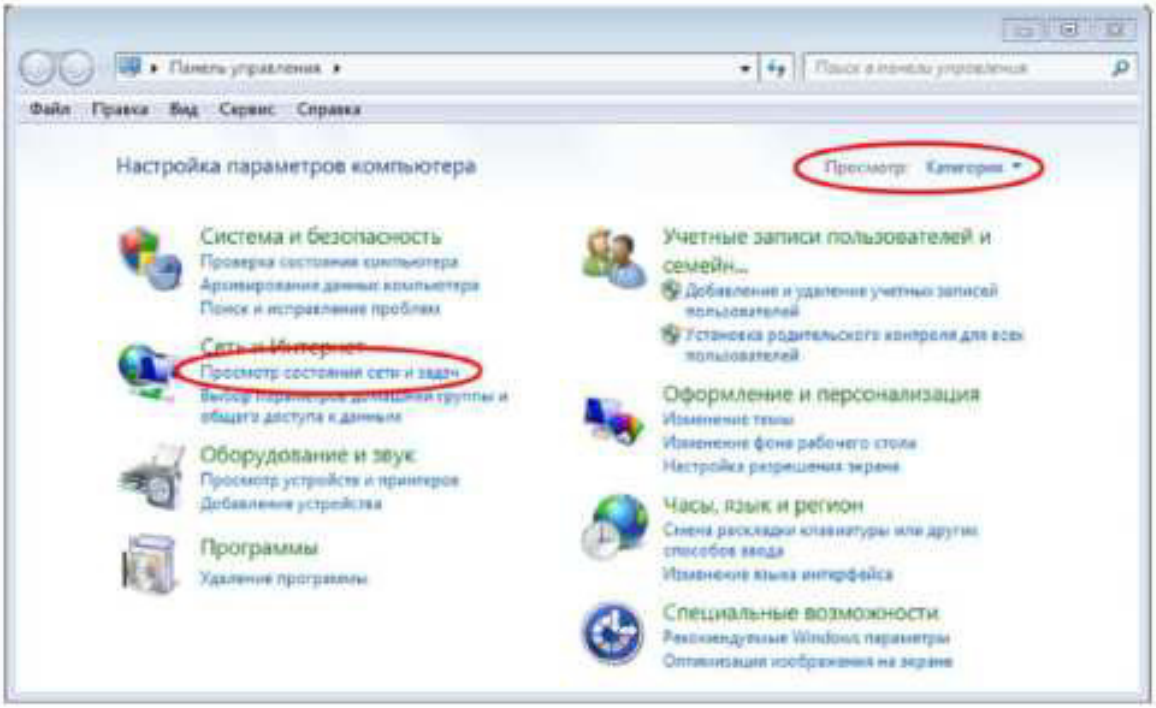
Шаг 1: Настройте статический IP-адрес на компьютерах.

a. В ОС **Windows** нажмите кнопку **Пуск** и зайдите в **Панель управления.**

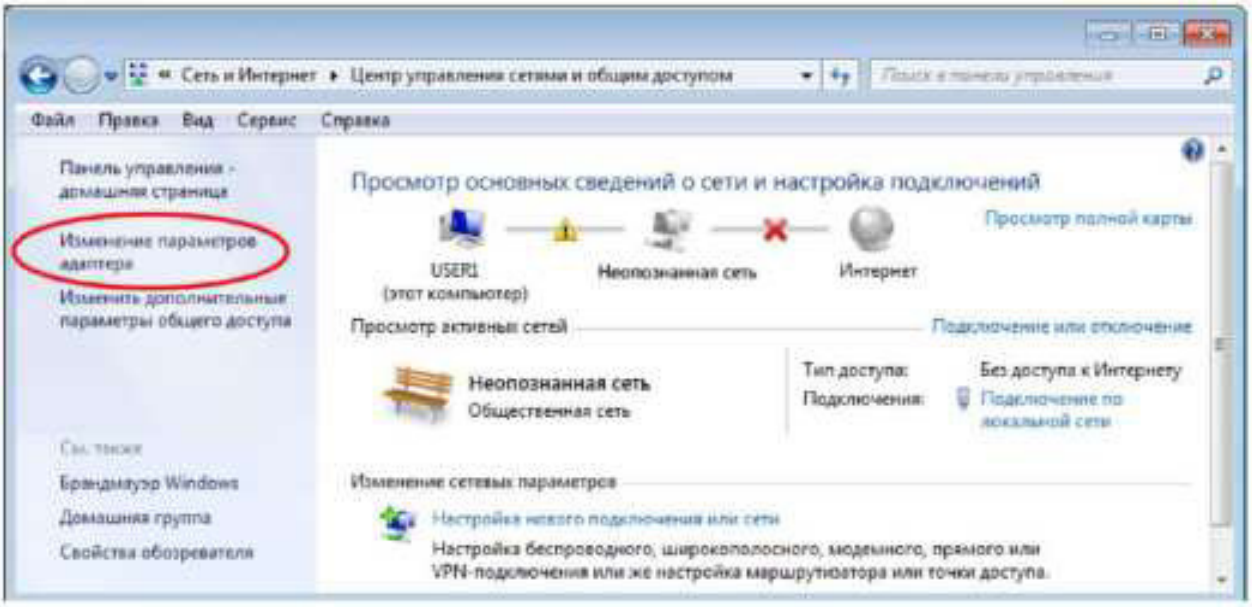


b. В разделе «Сеть и Интернет» нажмите на ссылку **Просмотр состояния сети и задач.**

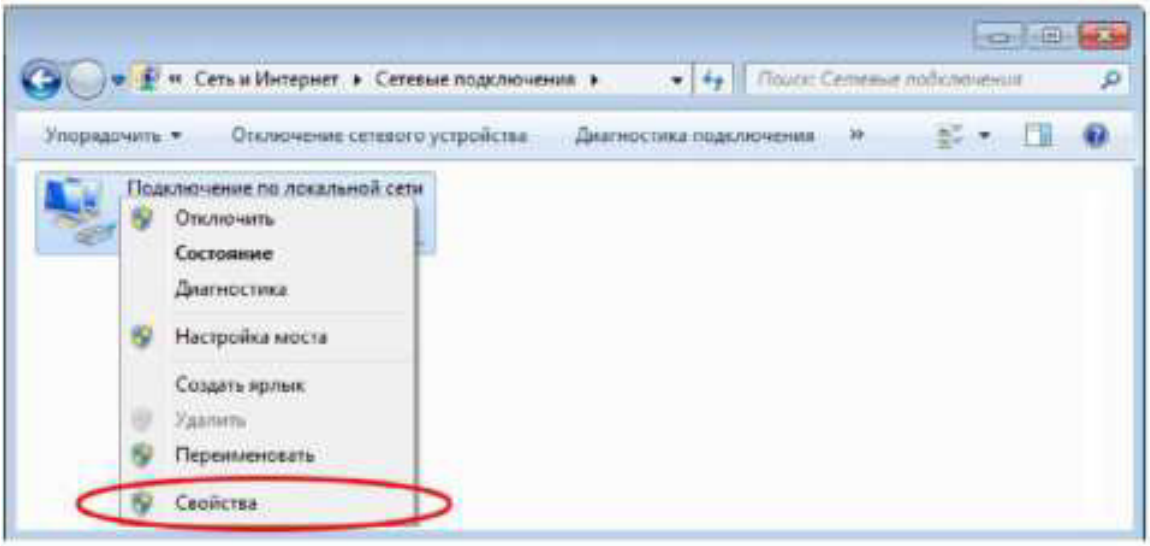
Примечание. Если в Панели управления отображается список значков, нажмите на раскрывающееся меню **Просмотр:** и выберите параметр **Категория.**



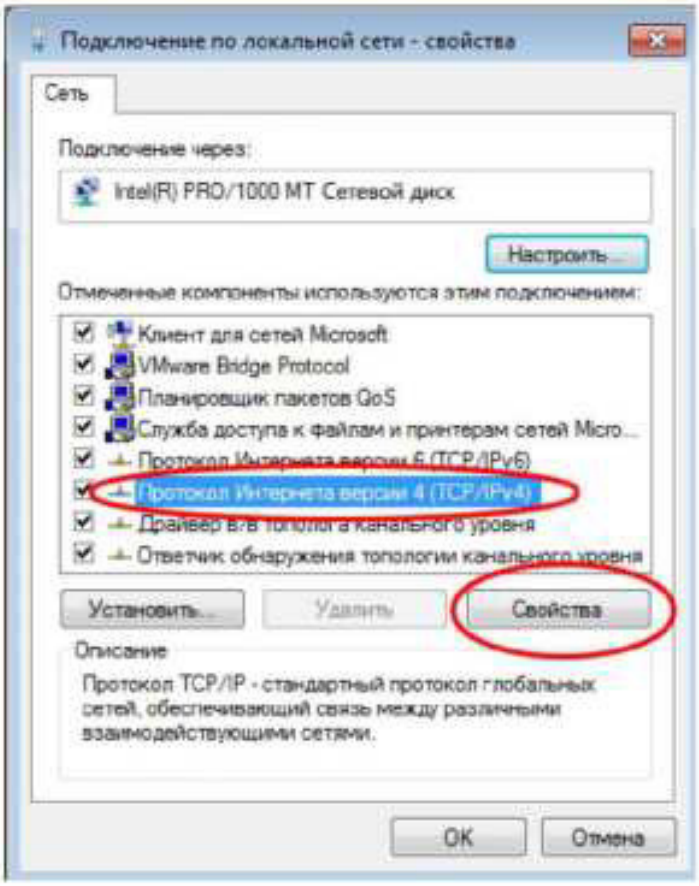
c. В левой части окна «Центр управления сетями и общим доступом» нажмите на ссылку Изменение параметров адаптера.



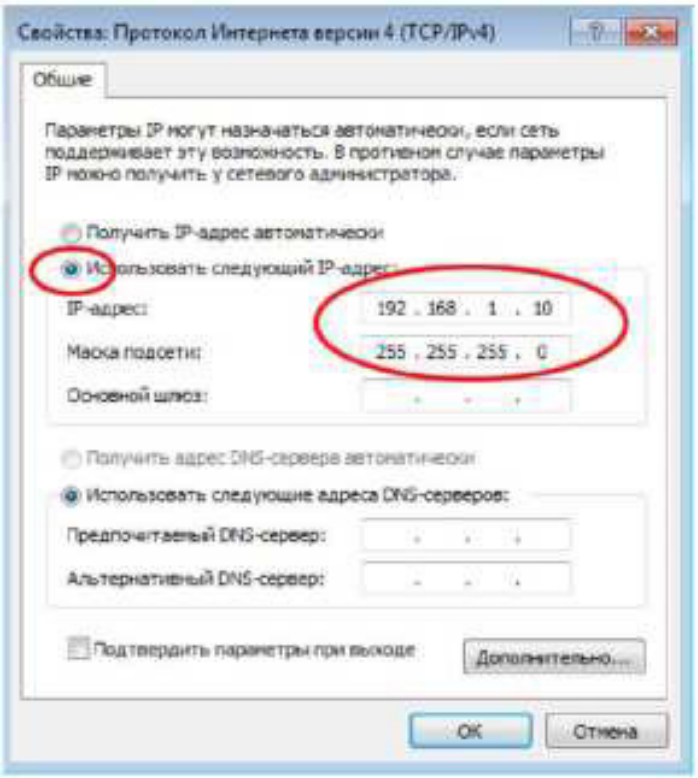
d. В окне «Сетевые подключения» отображаются доступные интерфейсы ПК. Нажмите правой кнопкой мыши на значок Подключение по локальной сети и выберите пункт Свойства.



. **Выберите опцию** Протокол Интернета версии 4 (TCP/IPv4) **и нажмите кнопку** Свойства.



Примечание. Чтобы открыть окно «Свойства», можно также дважды нажать кнопкой мыши на Протокол Интернета версии 4 (TCP/IPv4).f. Чтобы настроить IP-адрес, маску подсети и шлюз по умолчанию вручную, установите переключатель **Использовать следующий IP-адрес.**



Примечание. В рассмотренном выше примере введены IP-адрес и маска подсети для ПК-А. Шлюз по умолчанию не указан, поскольку к сети не подключён ни один маршрутизатор. В таблице адресации на стр. 1 указаны данные IP-адреса для ПК-Б.

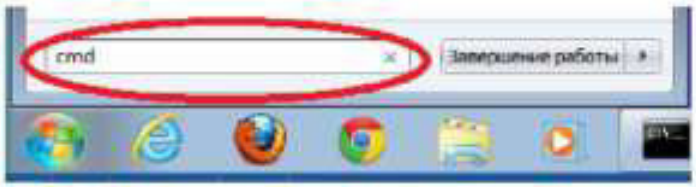
g. Указав все данные IP, нажмите кнопку OK. Нажмите кнопку OK в окне «Свойства подключения по локальной сети», чтобы присвоить IP-адрес адаптеру локальной сети.

h. Повторите перечисленные выше действия, чтобы ввести данные IP-адреса для ПК-Б.

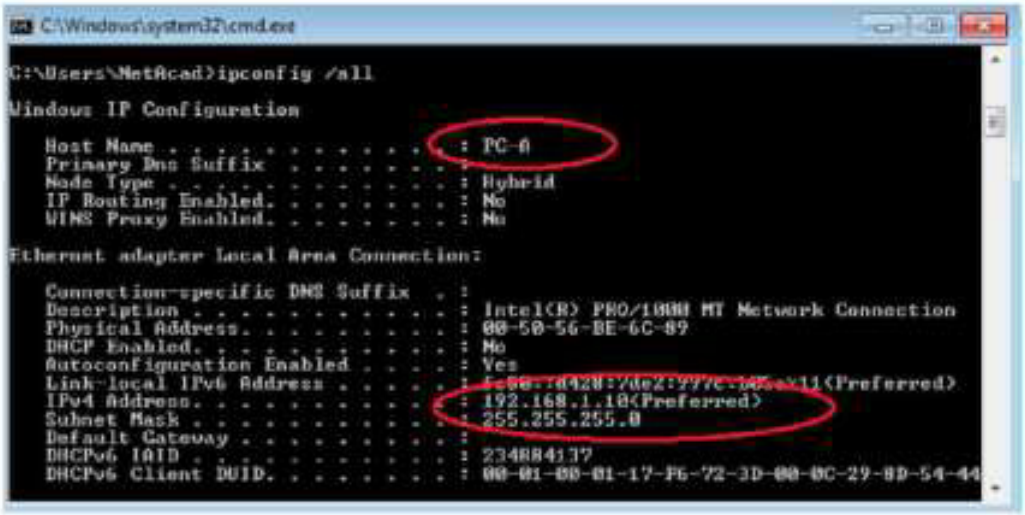
Шаг 2: Проверьте настройки и соединение ПК.

Для проверки настроек и соединения ПК используйте окно командной строки **(cmd.exe).**

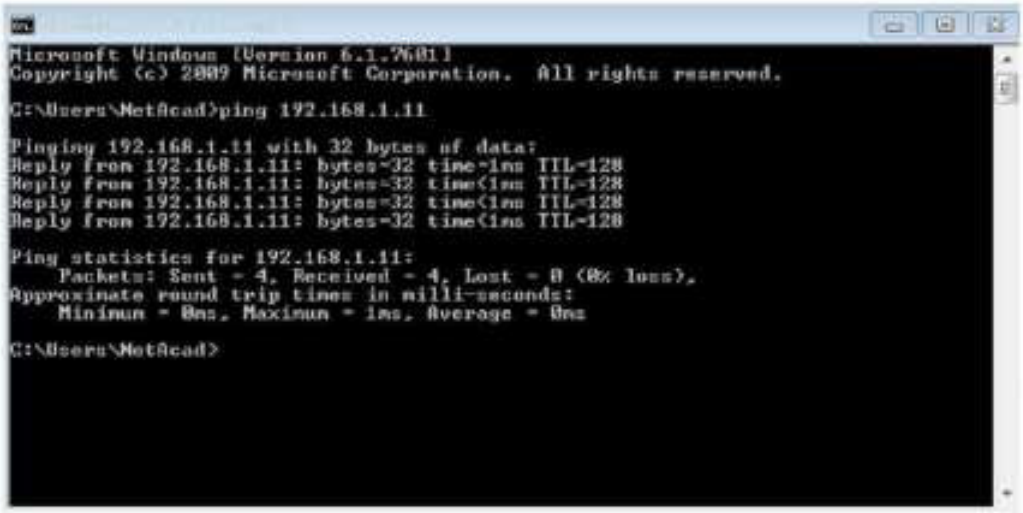
a. На ПК-Анажмите кнопку **Пуск,** введите **cmd** в строке **Найти программы и файлы и** нажмите клавишу ВВОД.



b. В окне ^d.exe можно вводить команды сразу в компьютер и тут же просматривать их результаты. Проверьте настройки ПК с помощью команды ipconfig /all. Эта команда отображает имя ПК и сведения об ^4-адресе.



c. Введите ping 192.168.1.11 и нажмите клавишу ВВОД.
C:\Window5\5y5tern32\cind,exe



Успешно ли выполнен эхо-запрос с помощью команды ping? Если нет, попытайтесь найти и устранить неполадку.

Примечание. Если вы не получили ответ от ПК-Б, попробуйте отправить эхо-запрос с помощью команды ping на ПК-Б ещё раз. Если ответа от ПК-Б по-прежнему нет, попробуйте отправить эхо- запрос с помощью команды ping с ПК-Б на ПК-А. Если ответ от удалённого ПК не поступает, обратитесь за помощью к инструктору.Часть 3: Настройка и проверка основных параметров коммутатора

Шаг 1: Подключитесь к коммутатору через консоль.

С помощью программы Tera Term установите консольное подключение ПК-А к коммутатору.

Шаг 2: Войдите в привилегированный режим.

Привилегированный режим даёт доступ ко всем командам коммутатора. К привилегированному набору команд относятся те, которые содержатся в пользовательском режиме, а также команда **configure,** при

помощи которой выполняется доступ к остальным командным режимам. Перейдите в привилегированный режим, введя команду **enable.**

Switch**>enable** Switch#

Приглашение в командной строке изменится с **Switch >** на **Switch #**, что указывает на привилегированный режим.

Шаг 3: Войдите в режим конфигурации.

Для входа в режим конфигурации используйте команду **configuration terminal.** Switch# **configure terminal**

Enter configuration commands, one per line. End with CNTL/Z. Switch (config) |

Приглашение в командной строке изменится в соответствии с режимом глобальной конфигурации.

Шаг 4: Присвойте коммутатору имя.

С помощью команды **hostname**измените имя коммутатора на **S1.**

Switch(config)# **hostname S1** S1(config)#

Шаг 5: Запретите нежелательные поиски в DNS.

Отключите поиск в DNS, чтобы предотвратить попытки коммутатора преобразовывать введённые команды таким образом, как будто они являются именами узлов.

S1(config)# no ip domain-lookup

S1(config)#

Шаг 6: Введите локальные пароли.

Для предотвращения несанкционированного доступа к коммутатору необходимо настроить пароли. S1(config)# **enable secret class**

S1(config)# **line con 0** S1(config-line)# **password cisco** S1(config-line)# **login** S1(config-line)# **exit** S1(config)#

Шаг 7: Введите сообщение дня (MOTD).

Баннер входа в систему, называемый также сообщением дня (MOTD), предупреждает о том, что любые попытки несанкционированного доступа к коммутатору запрещены.

Для использования команды **banner motd**необходимы разграничители, чтобы можно было распознать содержимое баннерного сообщения. Разграничительным символом может быть любой символ, которого нет в данном сообщении. По этой причине часто используются такие символы, как #.

```
S1(config)# banner motd #
Enter TEXT message.End with the character '#'.
Unauthorized access is strictly prohibited and prosecuted to the full
of the law. #
S1(config)# exit
S1#
```

Шаг 8: Сохраните конфигурацию.

С помощью команды сорусохраните текущую конфигурацию в файл загрузочной конфигурации, который хранится в энергонезависимой памяти(NVRAM).

```
S1# copy running-config startup-config
Destination filename [startup-config]? [Enter]
Building configuration...
[OK]
S1#
```

Шаг 9: Отобразите текущую конфигурацию.

Команда **show running-config** отображает всю текущую конфигурацию постранично. Для пролистывания страниц используйте клавишу ПРОБЕЛ. Команды, выполненные в пунктах 1-8, выделены ниже.

```
S1# show running-config
Building configuration...

Current configuration : 1409 bytes
!
! Last configuration change at 03:49:17 UTC Mon Mar 1 1993
!
version 15.0
no service pad
service timestamps debug datetimemsec
service timestamps log datetimemsec
no service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGholQM5EnRtoyr8cHAUg.2
!
noaaa new-model
```

```
systemmtu routing 1500
!
!
no ip domain-lookup
!

<outputomitted>

!
banner motd ^C
Unauthorized access is strictly prohibited and prosecuted to the full extent of the
law. ^C
!
line con 0
password cisco
login
line vty 0 4
login
line vty 5 15
login
!
end

S1#
```

Шаг 10: Отобразите версию IOS и другие необходимые данные коммутатора.

```
Switch Ports Model              SW Version            SW Image
------ ----- -----              ----------            ----------
*    1 26    WS-C2960-24TT-L    15.0(2)SE             C2960-LANBASEK9-M
```

```
Compiled Sat 28-Jul-12 00:29 by prod_rel_team
Configuration register is 0xF
S1#
```

Ш

Дл

show ip

```
BOOTLDR: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(53r)SEY3, RELEASE SOFTWARE
(fc1)

S1 uptime is 1 hour, 38 minutes
System returned to ROM by power-on
System image file is "flash:/c2960-lanbasek9-mz.150-2.SE.bin"


This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
```

С помощью команды show version отобразите версию IOS коммутатора, а также другую полезную информацию. Здесь для пролистывания отображаемых данных также используется клавиша ПРОБЕЛ.

S1# show ip interface brief					
Interface	IP-Address	OK?	Method	Status	Protocol
Vlanl	unassigned	YES	unset	up	up
FastEthernet0/1	unassigned	YES	unset	up	up
FastEthernet0/2	unassigned	YES	unset	down	down
FastEthernet0/3	unassigned	YES	unset	down	down
FastEthernet0/4	unassigned	YES	unset	down	down
FastEthernet0/5	unassigned	YES	unset	down	down
FastEthernet0/6	unassigned	YES	unset	up	up
FastEthernet0/7	unassigned	YES	unset	down	down
FastEthernet0/8	unassigned	YES	unset	down	down
FastEthernet0/9	unassigned	YES	unset	down	down
FastEthernet0/10	unassigned	YES	unset	down	down
FastEthernet0/11	unassigned	YES	unset	down	down
FastEthernet0/12	unassigned	YES	unset	down	down
FastEthernet0/13	unassigned	YES	unset	down	down
FastEthernet0/14	unassigned	YES	unset	down	down
FastEthernet0/15	unassigned	YES	unset	down	down
FastEthernet0/16	unassigned	YES	unset	down	down
FastEthernet0/17	unassigned	YES	unset	down	down
FastEthernet0/18	unassigned	YES	unset	down	down
FastEthernet0/19	unassigned	YES	unset	down	down
FastEthernet0/2 0	unassigned	YES	unset	down	down
FastEthernet0/21	unassigned	YES	unset	down	down
FastEthernet0/22	unassigned	YES	unset	down	down
FastEthernet0/23	unassigned	YES	unset	down	down
FastEthernet0/2 4	unassigned	YES	unset	down	down

S1# show ip interface brief					
Interface	IP-Address	K?	ethod	Status	Protocol
Vlanl	unassigned	ES	nset	up	up
FastEthernet 0/1	unassigned	ES	nset	up	up
FastEthernet 0/2	unassigned	ES	nset	down	down
FastEthernet 0/3	unassigned	ES	nset	down	down
FastEthernet 0/4	unassigned	ES	nset	down	down
FastEthernet 0/5	unassigned	ES	nset	down	down
FastEthernet 0/6	unassigned	ES	nset	up	up
FastEthernet 0/7	unassigned	ES	nset	down	down
FastEthernet 0/8	unassigned	ES	nset	down	down
FastEthernet 0/9	unassigned	ES	nset	down	down
FastEthernet 0/10	unassigned	ES	nset	down	down
FastEthernet 0/11	unassigned	ES	nset	down	down
FastEthernet 0/12	unassigned	ES	nset	down	down
FastEthernet 0/13	unassigned	ES	nset	down	down
FastEthernet 0/14	unassigned	ES	nset	down	down
FastEthernet 0/15	unassigned	ES	nset	down	down
FastEthernet 0/16	unassigned	ES	nset	down	down
FastEthernet 0/17	unassigned	ES	nset	down	down
FastEthernet 0/18	unassigned	ES	nset	down	down
FastEthernet 0/19	unassigned	ES	nset	down	down
FastEthernet 0/2 0	unassigned	ES	nset	down	down
FastEthernet 0/21	unassigned	ES	nset	down	down
FastEthernet 0/22	unassigned	ES	nset	down	down
FastEthernet 0/23	unassigned	ES	nset	down	down
FastEthernet	unassig			down	down

Шаг 12: Повторите шаги 1-12 для настройки коммутатора S2.

В данном случае необходимо изменить имя узла на S2.

Шаг 13: Запишите состояние указанных ниже интерфейсов.

Интерфейс	S1		S2	
	Состояние	Протокол	Состояние	Протокол
F0/1				
F0/6				
F0/18				
VLAN 1				

Почему одни порты Fast Ethernet коммутаторов включены, а другие — отключены?

Вопросы на закрепление

Что может препятствовать передаче эхо-запроса с помощью команды ping между компьютерами?

Примечание. Для отправки эхо-запроса с помощью команды ping между компьютерами может потребоваться отключение брандмауэра ПК.

Приложение А. Инициализация и перезагрузка коммутатора

Шаг 1: Подключитесь к коммутатору.

Подключите консоль к коммутатору и войдите в привилегированный режим.

```
Switch>enable
Switch#
```

Шаг 2: Определите, были ли созданы виртуальные локальные сети (VLAN).

Воспользуйтесь командой **show flash,** чтобы определить, были ли созданы сети VLAN на коммутаторе.

```
Switch# show flash

Directory of flash:/

32514048 bytes total (20886528 bytes free)
Switch#
```

Шаг 3: Удалите файл виртуальной локальной сети (VLAN).

а. Ес

```
Switch# delete vlan.
Delete filename [vlan.
```

бнаружен во флэш-памяти, удалите это

	rwx	- 9	191	ar		993	0:	6:	3	00:	0	private-config.text
	rwx	- 2	163	ar		993	0:	6:	3	00:	0	config.text
	rwx	- 36	133	ar		993	0:	6:	3	00:	0	multiple-fs
	rwx	- 07161	116	ar		993	2:	37 :	6	00:	0	c2960-lanbasek9-mz.150-2.SE.bin
	rwx	-	616	ar		993	0:	07 :	3	00:	0	vlan.dat

Будет предложено проверить имя файла. На данном этапе можно изменить имя файла или нажать клавишу ВВОД, если имя введено верно.

b. При запросе удаления этого файла нажмите клавишу ВВОД, чтобы подтвердить удаление. (Чтобы отменить удаление, нажмите любую другую кнопку.)

```
Delete flash:/vlan.dat? [confirm]
Switch#
```

Шаг 4: Удалите файл загрузочной конфигурации.

Введите команду **erase startup-config,** чтобы удалить файл загрузочной конфигурации из NVRAM. При необходимости удаления файла конфигурации нажмите клавишу ВВОД, чтобы подтвердить удаление. (Чтобы отменить операцию, нажмите любую другую кнопку.)

```
Switch# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
Switch#
```

Шаг 5: Перезагрузить коммутатор.

Перезагрузите коммутатор, чтобы удалить из памяти всю информацию о предыдущей конфигурации. При необходимости

```
Switch# reload
Proceed with reload? [con
```

Примечание. Возможно, появится запрос о сохранении текущей конфигурации перед перезагрузкой коммутатора. Введите **no**и нажмите клавишу ВВОД.

```
System configuration has been modified. Save? [yes/no]: no
```

Шаг 6: Пропустите диалоговое окно начальной конфигурации.

перезагрузки коммутатора нажмите клавишу ВВОД, чтобы продолжить перезагрузку. (Чтобы отменить перезагрузку, нажмите любую другую клавишу.)

После перезагрузки коммутатора появится запрос о входе в диалоговое окно начальной конфигурации. Введите **no** в окне запроса и нажмите клавишу ВВОД.

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

Практическая работа 3. Запуск сеанса консоли с помощью программы Tera Term

Топология

Задачи

Часть 1. Получение доступа к коммутатору Cisco через последовательный консольный порт Часть 2. Отображение и настройка основных параметров устройства

Часть 3. Получение доступа к маршрутизатору Cisco с помощью консольного кабеля mini-USB (дополн ительно)

Примечание. Пользователи NetLab или другого оборудования для удаленного доступа должны выполнить только часть 2.

Общие сведения/сценарий

Во всех типах сетей используют различные модели маршрутизаторов и коммутаторов Cisco. Для управления этими устройствами используется локальное консольное подключение или удаленное подключение. Практически все устройства Cisco оснащены консольным портом последовательного подключения. На некоторых новых моделях, например на маршрутизаторе с интегрированными сетевыми сервисами (ISR) 1941 G2, который используется в этой лабораторной работе, также есть консольный порт USB.

В этой лабораторной работе вы узнаете, как получить доступ к устройству Cisco через прямое локальное подключение к консольному порту, используя программу эмуляции терминала Tera Term. Вы также научитесь настраивать последовательный порт для консольного подключения Tera Term. Установив консольное подключение к устройству Cisco, можно отобразить или настроить параметры устройства. В этой лабораторной работе вы только отобразите параметры и настроите часы.

Примечание. В лабораторных работах CCNA используются маршрутизаторы Cisco ISR 1941 с Cisco IOS версии 15.2(4)M3 (образ universalk9). В лабораторных работах используются коммутаторы Cisco Catalyst 2960 с Cisco IOS версии 15.0(2) (образ lanbasek9). Можно использовать другие маршрутизаторы, коммутаторы и версии Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и результаты их выполнения могут отличаться от тех, которые показаны в лабораторных работах. Правильные идентификаторы интерфейса см. в сводной таблице по интерфейсам маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что все настройки коммутатора и маршрутизатора удалены, и загрузочная конфигурация отсутствует. Если вы не уверены, обратитесь к инструктору.

Необходимые ресурсы

- 1 маршрутизатор (Cisco 1941 с ПО Cisco IOS версии 15.2(4)M3 с универсальным образом или аналогичная модель)
- 1 коммутатор (Cisco 2960 с ПО Cisco IOS версии 15.0(2) с образом lanbasek9 или аналогичная модель)
- 1 ПК (под управлением Windows 7 или 8 с программой эмуляции терминала, например, Tera Term)
- Rollover-консольный кабель (DB-9-RJ-45) для настройки коммутатора или маршрутизатора через консольный порт RJ-45
- Кабель mini-USB для настройки маршрутизатора через консольный порт USB

Часть 1: Получение доступа к коммутатору Cisco через консольный порт последовательного подключения

Вы подключите ПК к коммутатору Cisco 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 Cisco и компьютер с помощью rollover-консольного кабеля.

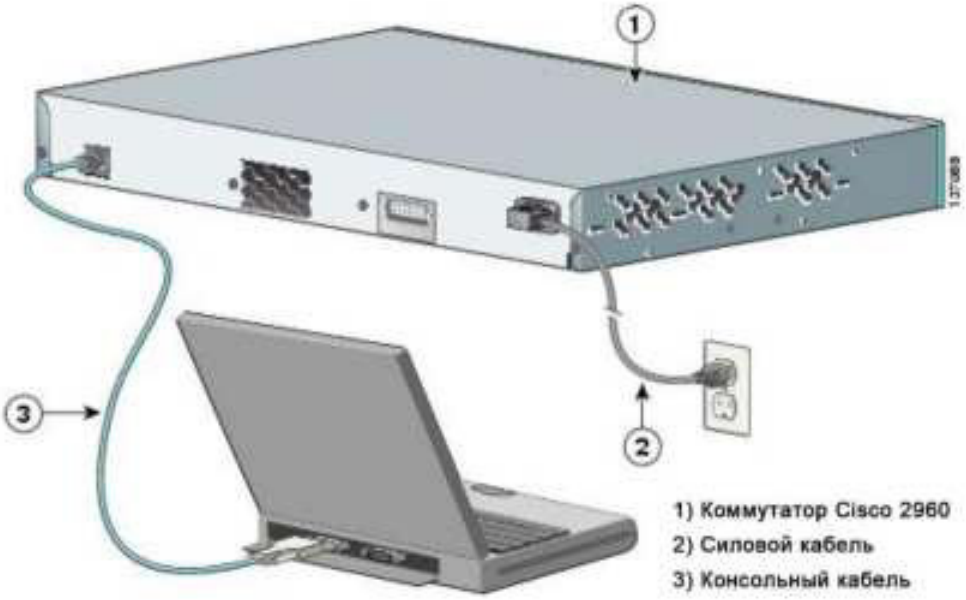
a. Подключите один конец rollover-консольного кабеля к консольному порту RJ-45 на коммутаторе.

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 Cisco 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 Cisco IOS при помощи эмулятора терминала в шаге 2.

c. Включите коммутатор Cisco и компьютер.



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

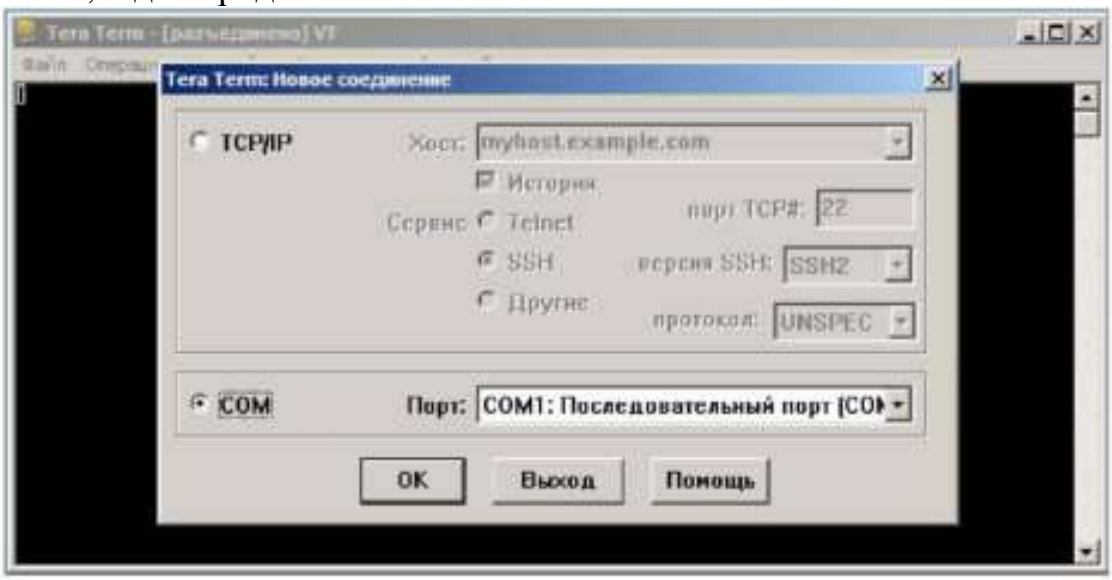
Tera Term — это программа эмуляции терминала. Она обеспечивает доступ к выходным данным терминала коммутатора, а также позволяет настроить коммутатор.

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

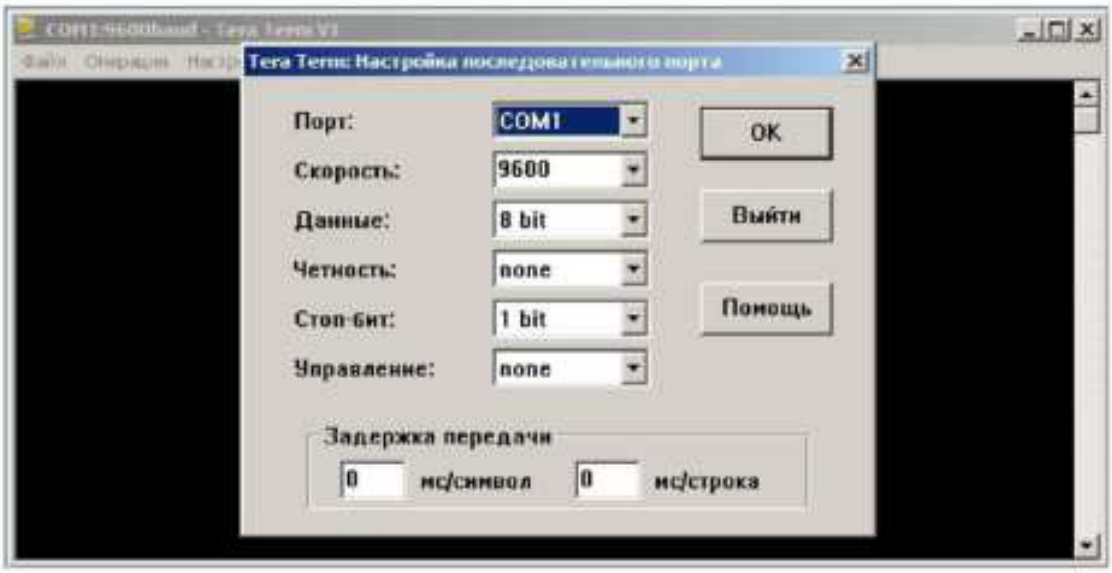
Примечание. Если программа Tera Term не установлена на компьютере, ее можно загрузить, перейдя по следующей ссылке и выбрав Tera Term:

<u>httpV/logmett.com/index.php?/download/free-downloads.html</u>

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 Cisco IOS.



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

Часть 2: Отображение и настройка основных параметров устройства

В этом разделе вы познакомитесь с пользовательским и привилегированным режимами EXEC. Вы определите версию IOS, отобразите параметры часов и настроите часы на коммутаторе.

Примечание. Если вышеуказанное сообщение не отображается, попросите инструктора сбросить настройки вашего коммутатора.

Шаг 1: 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]:
```

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

a. Отобразите текущие настройки часов.

```
Switch> show clock
*00:30:05.261 UTC Mon Mar 1 1993
```

Какая версия образа IOS используется на коммутаторе? c2960-lanbase-mz.122-25.FX.bin

Шаг 2: Настройте часы.

```
Switch> enable
```

Узнавая о сетях все больше, вы поймете, что настройка правильного времени на коммутаторе Cisco может упростить поиск и устранение неполадок. Далее описан порядок настройки внутренних часов коммутатора вручную.

b. Часы можно настроить в привилегированном режиме EXEC. Перейдите в привилегированный режим EXEC, введя enable в командной строке пользовательского режима EXEC.

c. Настройте часы. При вводе вопросительного знака (?) отображается справка, помогающая

определить, какие данные нужно ввести для настройки текущего

```
Switch# clock set ?
  hh:mm:ss  Current Time

Switch# clock set 15:08:00 ?
  <1-31>  Day of the month
  MONTH   Month of the year
```

времени, даты и года. Нажмите клавишу ввода для завершения настройки часов.

Часть 3: Получение доступа к маршрутизатору Cisco с помощью консольного кабеля mini-USB (дополнительно)

Если вы используете маршрутизатор Cisco 1941 или другие устройства под управлением Cisco IOS с консольным портом mini-USB, то для доступа к консольному порту устройства можно использовать кабель mini-USB, подключенный к порту USB на компьютере.

Примечание. Консольный кабель mini-USB аналогичен кабелям mini-USB, которые используются с другими электронными устройствами,

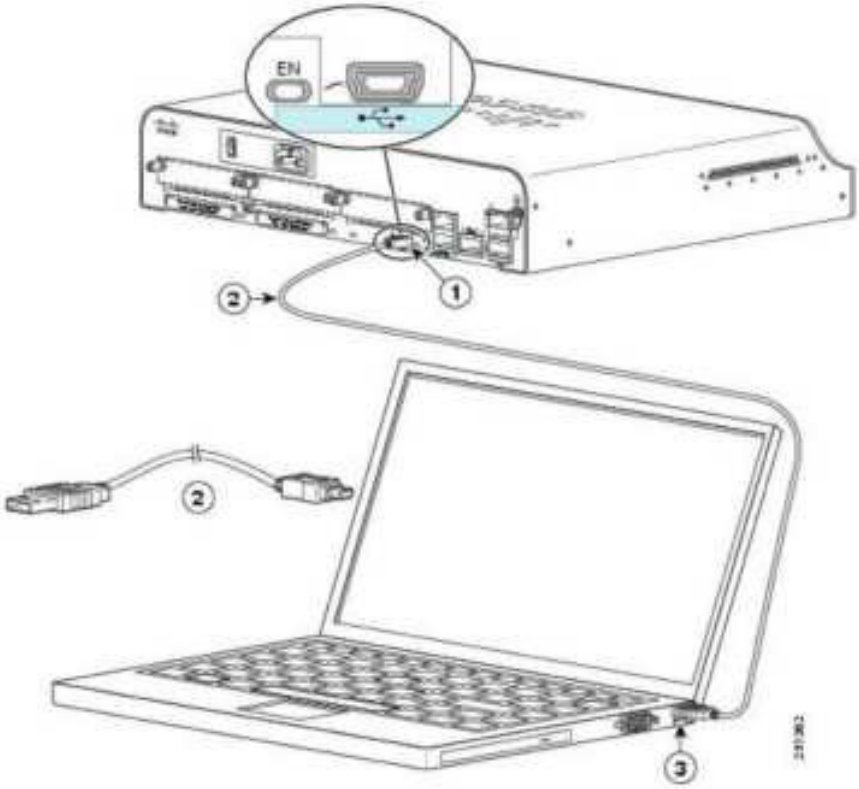
такими как жесткие диски USB, принтеры USB и концентраторы USB. Эти кабели mini-USB можно приобрести в корпорации Cisco Systems или у других поставщиков. Убедитесь, что вы используете именно кабель mini-USB, а не micro-USB для подключения к консольному порту mini-USB на устройстве с Cisco IOS.

Примечание. Необходимо использовать либо порт USB, либо порт RJ-45. Нельзя использовать оба порта одновременно. Если используется порт USB, он имеет приоритет над консольным портом RJ-45Шаг 1: Создайте физическое подключение с помощью кабеля mini-USB.

a. Подключите один конец кабеля mini-USB к консольному порту mini-USB на маршрутизаторе.

b. Другой конец кабеля подключите к порту USB на компьютере.

c. Включите маршрутизатор Cisco и компьютер.



1) Консольный USB-порт, 5 контактов, тип B mini

2) Консольный USB-кабель, 5 контактов, тип B mini-USB, к консольному USB-кабелю типа A

3) Разъем USB, тип A

Шаг 2: Проверьте готовность консоли USB.

Если вы используете ПК под управлением Microsoft Windows и индикатор консольного порта USB (с маркировкой EN) не горит зеленым, установите драйвер Cisco для консоли USB.

Перед подключением ПК с Microsoft Windows к устройству под управлением Cisco IOS при помощи кабеля USB необходимо установить драйвер USB. Драйвер для соответствующего устройства под управлением Cisco IOS можно найти на сайте www.cisco.com. Драйвер USB можно загрузить по следующей ссылке:

http://www.cisco.com/cisco/software/release.html?mdfid=282774238&flowid=714&softwareid=282855122&release=3.1&relind=AVAILABLE&rellifecycle=&reltype=latest

Примечание. Для загрузки этого файла требуется действительная учетная запись Cisco Connection Online (CCO).

Примечание. Эта ссылка относится к маршрутизатору Cisco 1941. Однако драйвер консоли USB не зависит от модели устройства под управлением Cisco IOS. Этот драйвер работает только с маршрутизаторами и коммутаторами Cisco. По завершении установки драйвера USB необходимо перезагрузить компьютер.

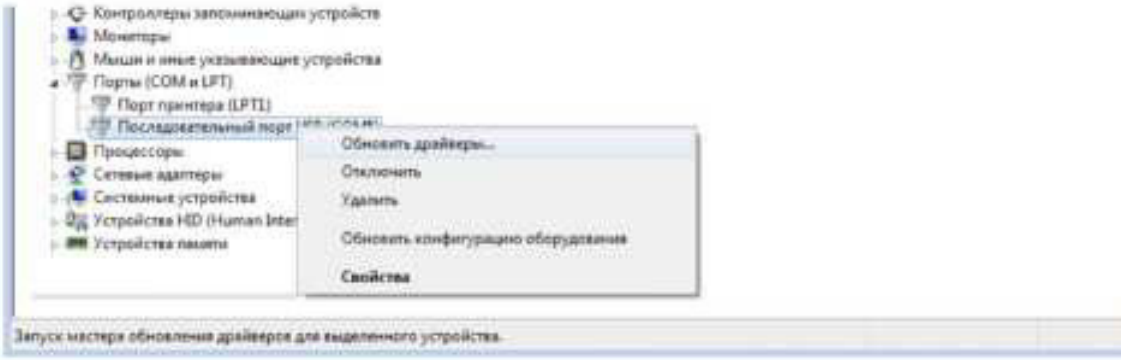
Примечание. После извлечения файлов папка будет содержать инструкции по установке и удалению, а также необходимые драйверы для разных операционных систем и архитектур. Выберите подходящую версию для своей системы.

Когда индикатор консольного порта USB загорится зеленым, порт доступен.

Шаг 3: Включите порт COM для ПК под управлением Windows 7 (дополнительно).

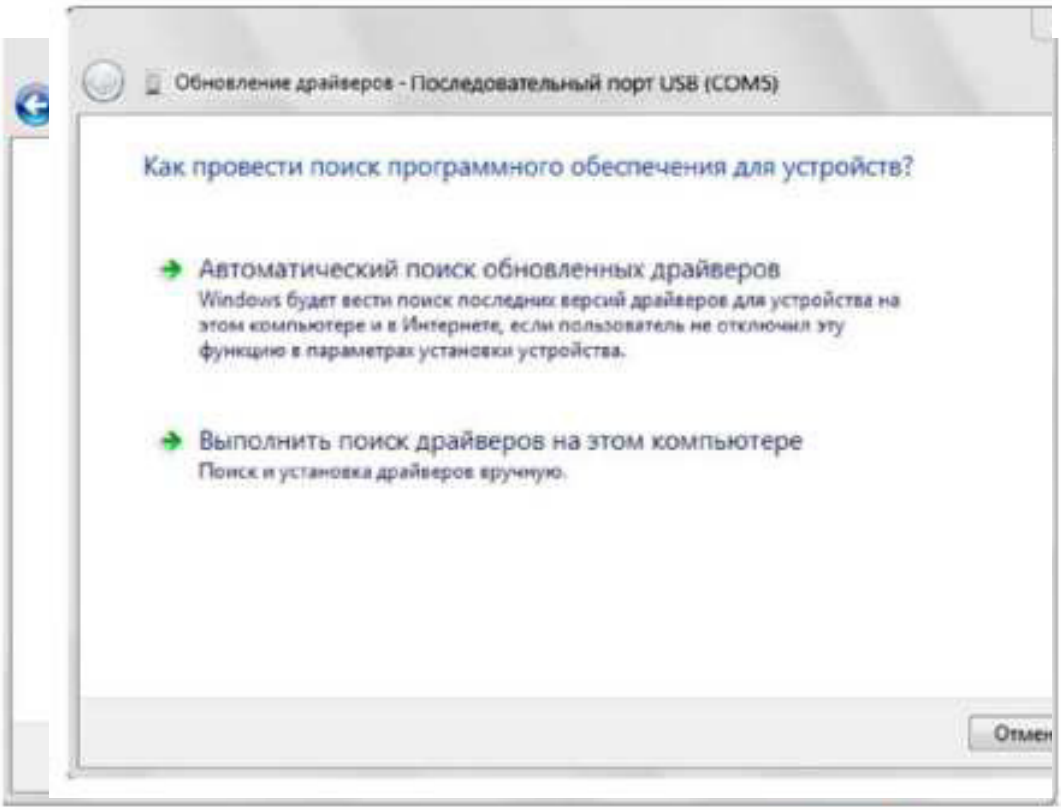
На ПК под управлением Microsoft Windows 7 могут потребоваться следующие действия для включения порта COM.

a. Нажмите кнопку Пуск, чтобы открыть Панель управления.
b. Откройте Диспетчер устройств.
c. Щелкните Порты (COM и LPT), чтобы развернуть древовидную



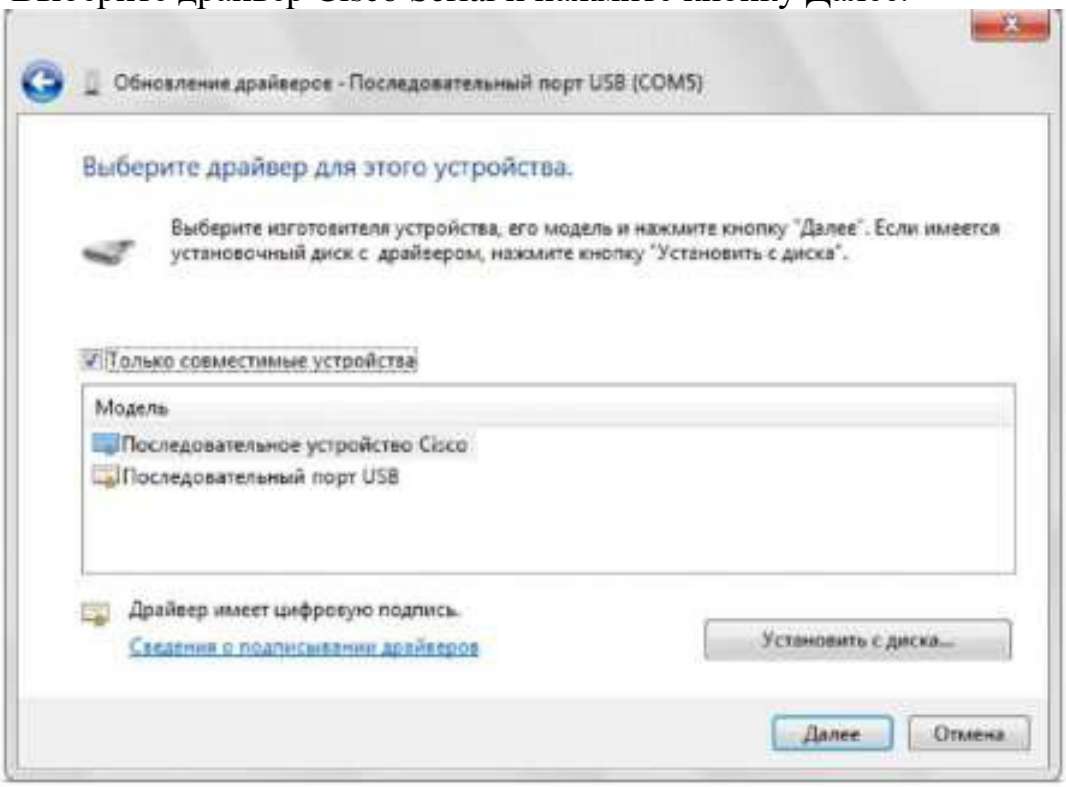
d. Выберите Выполнить поиск драйверов на этом компьютере.

структуру. Щелкните правой кнопкой мыши значок Последовательный порт USB и выберите Обновить драйверы

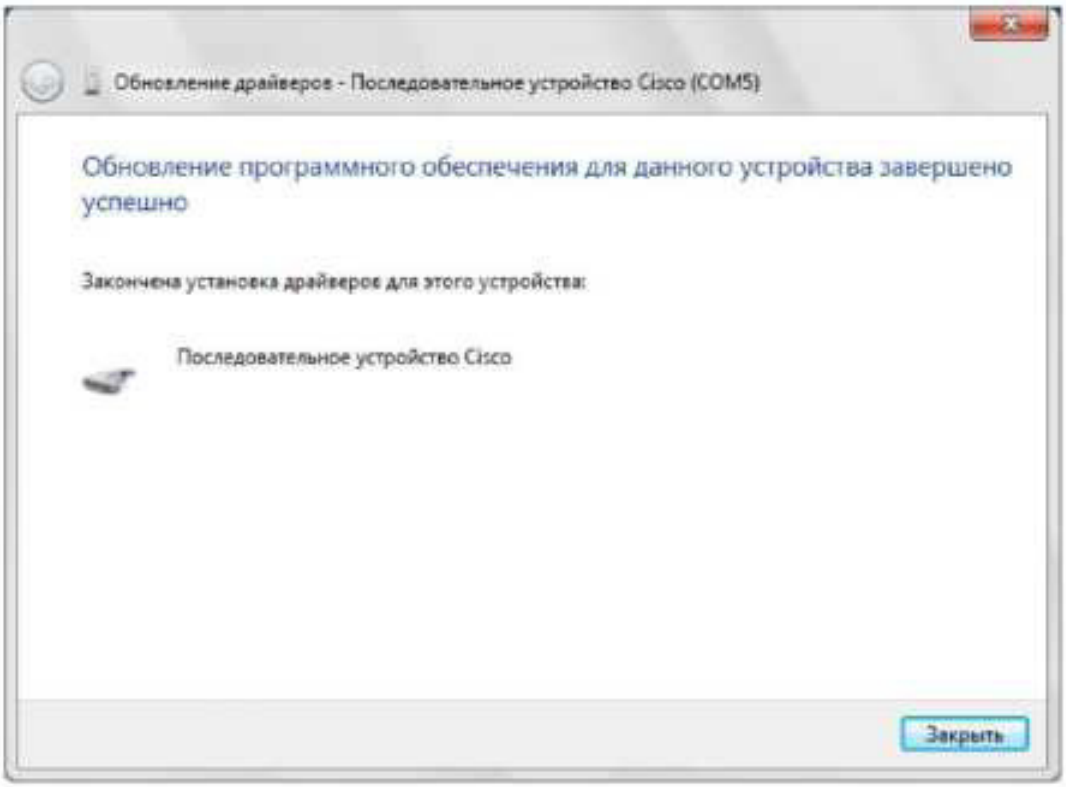


e. Выберите Выбрать драйвер из списка уже установленных драйверов и нажмите кнопку Далее.

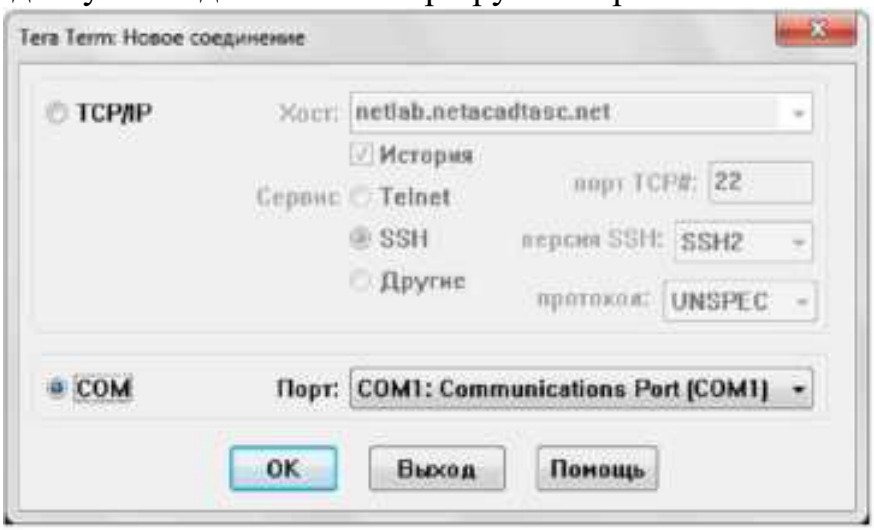
f. Выберите драйвер Cisco Serial и нажмите кнопку Далее.



g. Запишите назначенный номер порта, который отображается вверху окна. В данном примере для связи с маршрутизатором используется порт COM 5. Нажмите Закрыть.



h. Откройте программу Tera Term. Установите переключатель Serial (Последовательное) и выберите соответствующий последовательный порт. В данном примере это Port COM5: Cisco Serial (COM 5). Теперь этот порт должен стать доступным для связи с маршрутизатором. Нажмите OK.



Вопросы для повторения

1. Как предотвратить несанкционированный доступ к устройству Cisco через консольный порт?

2. Назовите достоинства и недостатки использования последовательного консольного подключения по сравнению с консольным подключением USB к маршрутизатору или коммутатору Cisco.

Сводная таблица по интерфейсам маршрутизаторов

Сводная таблица по интерфейсам маршрутизаторов				
Модель маршрутизатора	Интерфейс Ethernet 1	Интерфейс Ethernet 2	Последовательный интерфейс 1	Последовательный интерфейс 2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Примечание. Чтобы определить конфигурацию маршрутизатора, можно посмотреть на интерфейсы и установить тип маршрутизатора и количество его интерфейсов. Перечислить все комбинации конфигураций для каждого класса маршрутизаторов невозможно. Эта таблица содержит идентификаторы для возможных комбинаций интерфейсов Ethernet и последовательных интерфейсов на устройстве. Другие типы интерфейсов в таблице не представлены, хотя они могут присутствовать в данном конкретном маршрутизаторе. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это официальное сокращение, которое можно использовать в командах Cisco IOS для обозначения интерфейса.				

Практическая работа 4: настройка адреса управления коммутатором

Топология

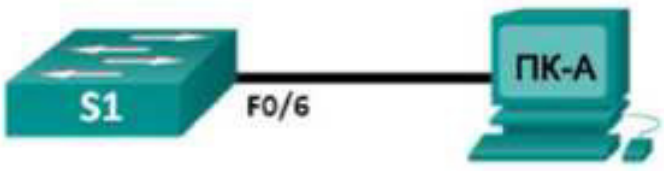


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
S1	VLAN 1	192.168.1.2	255.255.255.0	Недоступно
ПК-А	Сетевой адаптер	192.168.1.10	255.255.255.0	Недоступно

Задачи

Часть 1. Настройка основных параметров сетевого устройства

- Создайте сеть в соответствии с изображенной на схеме топологией.
- Настройте основные параметры коммутатора, включая имя узла, адрес управления и доступ по протоколу Telnet.
- Настройте IP-адрес ПК.

Часть 2. Проверка и тестирование подключения к сети

- Отобразите конфигурацию устройства.
- Проверьте сквозное подключение с помощью эхо-запроса с помощью команды ping.
- Проверьте возможность удалённого управления по протоколу Telnet.
- Сохраните файл текущей конфигурации коммутатора.

Исходные данные/сценарий

Коммутаторы Cisco имеют особый интерфейс, который называется виртуальным интерфейсом коммутатора (SVI). На SVI интерфейсе можно сконфигурировать IP-адрес, который обычно называют адресом управления. Он позволяет получить удалённый доступ к коммутатору для отображения и настройки параметров.

В ходе лабораторной работы вам необходимо создать простую сеть, используя кабель локальной сети Ethernet и получить доступ к коммутатору Cisco, используя консоль и методы удалённого доступа. Вы настроите основные параметры коммутатора и IP-адресацию, а также продемонстрируете использование IP-адреса управления для удалённого доступа к коммутатору. Топология состоит из одного коммутатора и одного узла, использующего только порты Ethernet и консоли.

Примечание. Используются коммутаторы: Cisco Catalyst 2960s с операционной системой Cisco IOS версии 15.0(2) (образ lanbasek9). Можно использовать другие коммутаторы и версии ПО Cisco IOS

В зависимости от модели и версии Cisco IOS выполняемые доступные команды и выводы могут отличаться от данных, полученных в ходе лабораторных работ.

Примечание. Коммутаторы необходимо очистить от данных и файлов начальной конфигурации. Если вы не уверены, что сможете это сделать, обратитесь к инструктору.

Необходимые ресурсы

- 1 коммутатор (серия Cisco 2960, с программным обеспечением Cisco IOS версии 15.0(2), образ lanbasek9 или аналогичный)
- 1 ПК (Windows 7, Vista или XP с программой эмулятора терминала, например Tera Term)
- Консольные кабели для настройки устройств CISCO IOS через консольные порты
- Кабели Ethernet в соответствии с топологией

Часть 1: Настройка основных параметров сетевого устройства

В части 1 вы должны настроить сеть и основные параметры, такие как IP-адреса интерфейсов и доступ к устройствам.

Шаг 1: Подключите кабели.

a. Создайте сеть в соответствии с изображенной на схеме топологией.

b. Создайте консольное подключение к коммутатору на ПК-А.

Шаг 2: Настройте основные параметры коммутатора.

На этом этапе вам необходимо настроить основные параметры коммутатора (такие как имя узла) и IP- адрес для SVI. Назначение IP-адреса на коммутаторе — это лишь первый шаг. Как сетевому администратору, вам следует выбрать способ управления коммутатором. Два наиболее распространённых метода управления — это Telnet и SSH, однако протокол Telnet не очень надёжен. Вся информация, передаваемая между двумя устройствами, отправляется в виде простого текста. Анализатор пакетов может легко перехватить, а также прочесть пароли и другие важные данные.

a. Если в энергонезависимой памяти (NVRAM) коммутатора нет сохранённых файлов конфигурации, воспользовавшись командой Switch>, вы перейдете в пользовательский режим. Войдите в привилегированный режим.

```
Switch> enable
Switch#
```

b. Проверьте чистый файл конфигурации с помощью команды привилегированного режима show running-config. Если файл конфигурации был ранее сохранён, его нужно удалить. В зависимости от модели коммутатора и версии IOS конфигурация может выглядеть по-разному. При

```
Switch# configure terminal
Switch(config)# hostname S1
S1(config)#
```

d. Настройте пароль доступа к коммутатору.

```
S1(config)# enable secret class
S1(config)#
```

e. Запретите нежелательные поиски в службе доменных имен (DNS).

```
S1(config)# no ip domain-lo
S1(config)#
```

f. Настройте сообщение дня (MOTD), которое будет отображаться перед входом в систему.

```
S1(config)# banner motd #
Enter Text message.  End with the character '#'.
Unauthorized access is strictly prohibited. #
```

этом настроенных ранее паролей или IP-адреса на коммутаторе быть не должно. Если ваш коммутатор не имеет конфигурации по умолчанию,

Примечание. Пароль не будет отображаться на экране в процессе ввода.

d. Войдите в режим глобальной конфигурации и настройте IP-адрес SVI для разрешения удалённого управления коммутатором.

```
S_# config t
S1#(config)# interface vlan 1
S1(config-if)# ip address 192.168.1.2 255.255.255.0
S1(config-if)# no shut
S_(config-if)# exit
S1(config)#
```

обратитесь за помощью к инструктору.

c. Войдите в режим глобальной конфигурации и назначьте имя узла коммутатора.

Какое сочетание клавиш используется для прямого перехода из режима глобальной конфигурации в привилегированный режим?

h. Вернитесь из пользовательского режима в привилегированный.

j. Ограничьте доступ к порту консоли. Конфигурация по умолчанию не требует пароля при консольных подключениях.

k. Настройте канал виртуального соединения для удалённого управления (VTY), чтобы

к коммутатору можно было подключаться по протоколу Telnet. Если вы не укажете пароль VTY, то не сможете подключаться к коммутатору по протоколу Telnet.

```
S1(config)# line vty 0 4
S1(config-line)# password cisco
S1(config-line)# login
```

```
S1(config-line)# end
S1#
*Mar  1 00:06:11.590: %SYS-5-CONFIG_I: Configured from console by console
```

Шаг 3: Настройте IP-адрес ПК-А.

a. Назначьте IP-адрес и маску подсети для ПК, как показано Addressing Table на стр. 1. Процедура присвоения IP-адреса на ПК под управлением ОС Windows 7 описана ниже.

1) Нажмите кнопку Пуск > Панель управления.
2) Нажмите кнопку Просмотр: > Категория.
3) Выберите вариант Просмотр состояния сети и задач > Изменение параметров адаптера.
4) Нажмите правой кнопкой мыши на вариант Подключение к локальной сети и выберите пункт Свойства.
5) Выберите вариант Протокол Интернета версии 4 (TCP/IPv4), далее щёлкните пункт Свойства > OK.
6) Установите переключатель Использовать следующий IP-адрес и введите IP-адрес и маску подсети.

Часть 2: Проверка и тестирование подключения сети

Теперь нужно проверить и зафиксировать конфигурацию коммутатора, протестировав сквозное подключение между ПК-А и коммутатором S1, а также возможность удалённого управления коммутатором.

Шаг 1: Отобразите конфигурацию коммутатора S1.

a. Воспользовавшись программой Tera Term на ПК, вернитесь к консольному подключению, чтобы отобразить и проверить конфигурацию коммутатора с помощью команды show. Ниже представлен пример конфигурации. Внесённые вами настройки выделены жёлтым цветом. Другие параметры конфигурации предусмотрены в IOS по умолчанию.

b. Проверьте состояние интерфейса управления SVI. Интерфейс VLAN 1 должен находиться в состоянии «up/up» и иметь назначенный IP-адрес. Обратите внимание на то, что порт коммутатора F0/6 также

```
S1# show run
Building configuration...

Current configuration : 1508 bytes
!
! Last configuration change at 00:06:11 UTC Mon Mar 1 1993
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
```

должен функционировать, так как к нему подключён ПК-А. Поскольку

все порты коммутатора по умолчанию входят в сеть VLAN 1, вы можете обмениваться данными с коммутатором по IP-адресу, который настроили для сети VLAN 1.

```
S1# show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
Vlanl	192.168.1.2	YES	manual	up	up
FastEthernet0/1	unassigned	YES	unset	down	down
FastEthernet0/2	unassigned	YES	unset	down	down
FastEthernet0/3	unassigned	YES	unset	down	down
FastEthernet0/4	unassigned	YES	unset	down	down
FastEthernet0/5	unassigned	YES	unset	down	down
FastEthernet0/6	unassigned	YES	unset	up	up
FastEthernet0/7	unassigned	YES	unset	down	down
FastEthernet0/8	unassigned	YES	unset	down	down
FastEthernet0/9	unassigned	YES	unset	down	down
FastEthernet0/10	unassigned	YES	unset	down	down
FastEthernet0/11	unassigned	YES	unset	down	down
FastEthernet0/12	unassigned	YES	unset	down	down
FastEthernet0/13	unassigned	YES	unset	down	down
FastEthernet0/14	unassigned	YES	unset	down	down
FastEthernet0/15	unassigned	YES	unset	down	down
FastEthernet0/16	unassigned	YES	unset	down	down
FastEthernet0/17	unassigned	YES	unset	down	down
FastEthernet0/18	unassigned	YES	unset	down	down
FastEthernet0/19	unassigned	YES	unset	down	down
FastEthernet0/2 0	unassigned	YES	unset	down	down
FastEthernet0/21	unassigned	YES	unset	down	down
FastEthernet0/22	unassigned	YES	unset	down	down
FastEthernet0/23	unassigned	YES	unset	down	down
FastEthernet0/2 4	unassigned	YES	unset	down	down
GigabitEthernet0/1	unassigned	YES	unset	down	down
GigabitEthernet0/2	unassigned	YES	unset	down	down

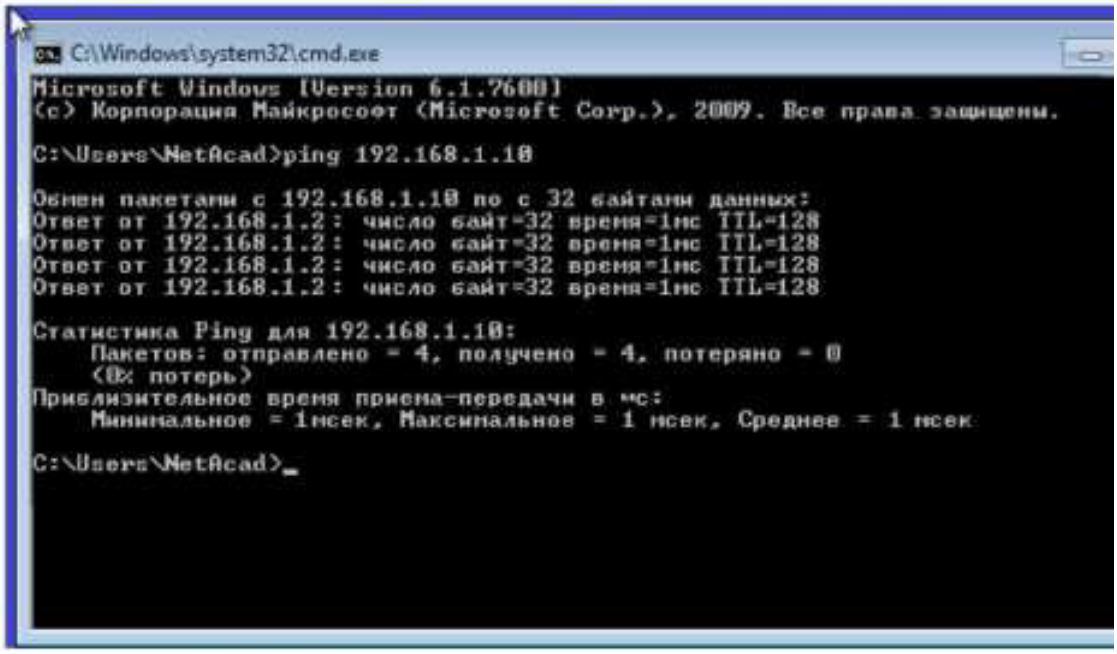
Шаг 2: Проверьте сквозное подключение.

Откройте диалоговое окно (cmd.exe) на ПК-А. Для этого нажмите кнопку Пуск и введите команду cmd в поле Найти программы и файлы. Проверьте IP-адрес ПК-А с помощью команды ipconfig /all. Эта команда отображает имя ПК и сведения об ^4-адресе. Отправьте эхо-запрос с помощью команды ping на собственный адрес ПК-А и адрес управления коммутатором S1.

C:\Users\NetAcad> ping 192.168

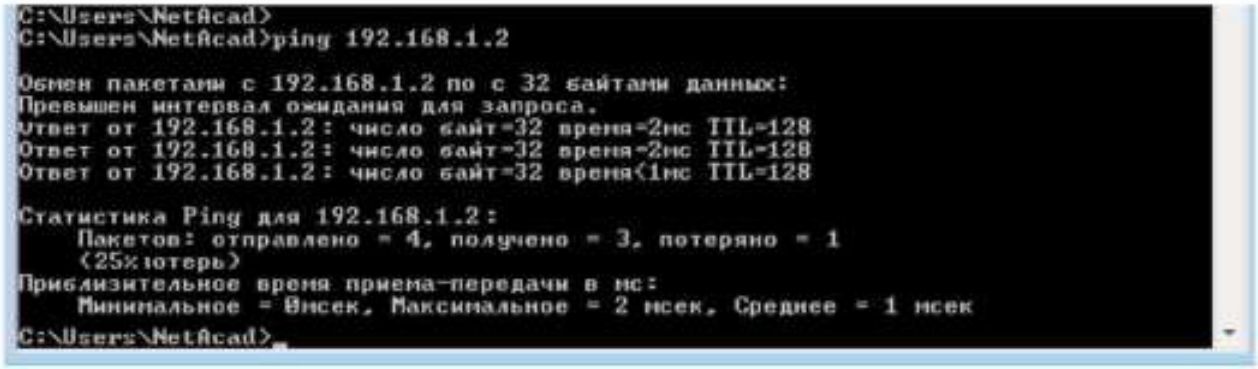
На экране должны появиться показанные ниже данные.

a. Сначала отправьте эхо-запрос с помощью команды ping на адрес ПК-А.



b. Отправьте эхо-запрос с помощью команды ping на адрес управления SVI коммутатора S1. C:\Users\NetAcad> ping 192.168.1.2

На экране должны появиться показанные ниже данные. Если эхо-запрос с помощью команды ping выполнить не удалось, попробуйте найти ошибку в основных параметрах устройства. При необходимости проверьте кабели и IP-адресацию.



Шаг 3: Проверьте удалённое управление коммутатором S1.

Сейчас вам предстоит получить удалённый доступ к коммутатору S1 по протоколу Telnet, используя адрес управления SVI. В данной лабораторной работе ПК-А и коммутатор S1 находятся рядом. В производственной сети коммутатор может находиться в коммутационном

шкафу на последнем этаже, а компьютер — на первом. Telnet не является безопасным протоколом, однако в данной лабораторной работе для проверки удалённого доступа вы будете использовать его. Вся информация по протоколу Telnet, включая пароли и команды, отправляется в виде простого текста. В последующих лабораторных работах для удалённого доступа к сетевым устройствам вы будете использовать протокол SSH.

Примечание. Изначально ОС Windows 7 не поддерживает Telnet. Протокол должен быть активирован администратором. Для установки клиента Telnet откройте окно командной строки и введите pkgmgr /iu: "TelnetClient".

C:\Users\NetAcad> pkgmgr /iu:"TelnetClient"

a. Для подключения к коммутатору S1 через адрес управления SVI в открытом окне командной строки на ПК-А введите команду Telnet. Пароль: cisco.

C:\Users\NetAcad> telnet 192.168.1.2

На экране должны появиться показанные ниже данные.

b. Указав пароль cisco, вы сможете перейти в командную строку пользовательского режима. При появлении приглашения введите enable. Введите пароль class, чтобы войти в привилегированный режим и выполнить команду show run.

Шаг 4: Сохраните файл конфигурации.

a. Открыв сеанс Telnet, введите в командную строку copy run start.

```
S1# copy run start
Destination filename [startup-config]? [Enter]
Building configuration ..
S1#
```

b. Введите quit, чтобы завершить сеанс Telnet. После этого вы вернётесь в командную строку Windows 7.

Вопросы на закрепление

Почему для начальной конфигурации коммутатора следует использовать подключение консоли? Почему нельзя подключиться к коммутатору по протоколу Telnet или SSH?

Практическая работа 5: просмотр сетевого трафика с помощью программы Wireshark

Топология

Задачи

Часть 1. Загрузка и установка программы Wireshark (необязательно)

Часть 2. Сбор и анализ данных протокола ICMP по локальным узлам в программе Wireshark

- Начните и остановите сбор данных трафика эхо-запросов с помощью команды ping к локальным узлам.
- Найдите данные об IP- и MAC-адресах в полученных PDU.

Часть 3. Сбор и анализ данных протокола ICMP по удалённым узлам в программе Wireshark

- Начните и остановите сбор данных трафика эхо-запросов с помощью команды ping к удалённым узлам.
- Найдите данные об IP- и MAC-адресах в полученных PDU.
- Поясните, почему MAC-адреса удалённых узлов отличаются от MAC-адресов локальных узлов.

Исходные данные/сценарий

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 перехватывает каждый протокольный блок данных (PDU), после чего расшифровывает или анализирует его 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 при выполнении большинства лабораторных работ в рамках курсов CCNA. В данной лабораторной работе содержатся

инструкции по загрузке и установке программы Wireshark. Воспользуйтесь ими, если программа не установлена. В ходе лабораторной работы вы научитесь пользоваться программой Wireshark для перехвата IP- адресов пакетов данных ICMP и MAC-адресов Ethernet-кадров.

Необходимые ресурсы

- 1 ПК (Windows 7, Vista или XP с выходом в Интернет)
- Дополнительные ПК в локальной сети будут использоваться для ответов на эхо-запросы.

Часть 1: Загрузка и установка программы Wireshark (необязательно)

Программа Wireshark стала стандартным анализатором пакетов, используемым сетевыми инженерами. Версии этой программы с открытым исходным кодом доступны для различных операционных систем, включая Windows, Mac и Linux. В части 1 этой лабораторной работы вам нужно будет загрузить и установить программу Wireshark на ПК.

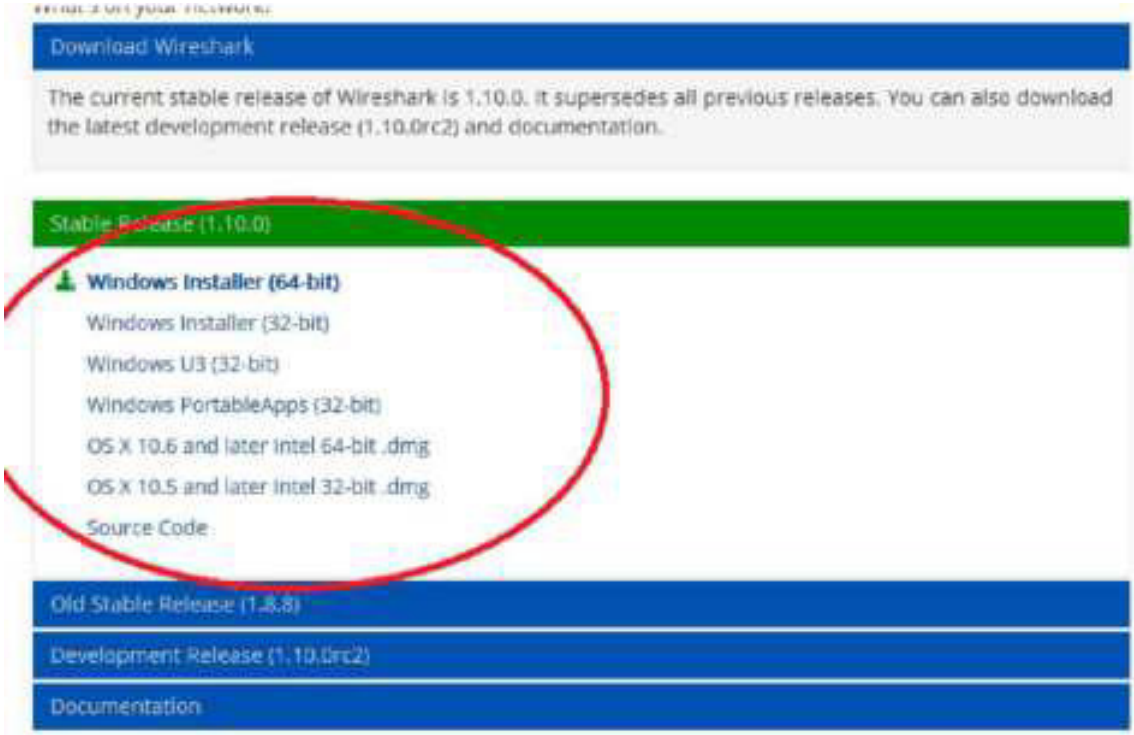
Примечание. Если программа Wireshark на вашем ПК уже установлена, вы можете пропустить часть 1 и перейти сразу к части 2. Если программа Wireshark на вашем ПК не установлена, узнайте у инструктора о правилах загрузки программного обеспечения в вашем учебном заведении.

Шаг 1: Загрузите программу Wireshark.

a. Программу Wireshark можно загрузить по адресу www.wireshark.org.

b. Нажмите Download Wireshark.

c. Выберите версию программы в соответствии с архитектурой и операционной системой вашего ПК. Например, если ваш ПК работает под управлением 64-разрядной ОС Windows, выберите Windows Installer (64-bit).

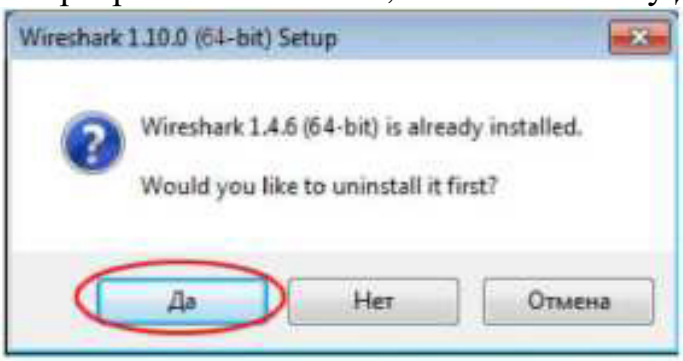


Сразу после этого начнётся загрузка. Местонахождение загруженного файла зависит от браузера и операционной системы, которыми вы пользуетесь. В ОС Windows загрузочные файлы по умолчанию находятся в папке Загрузки.

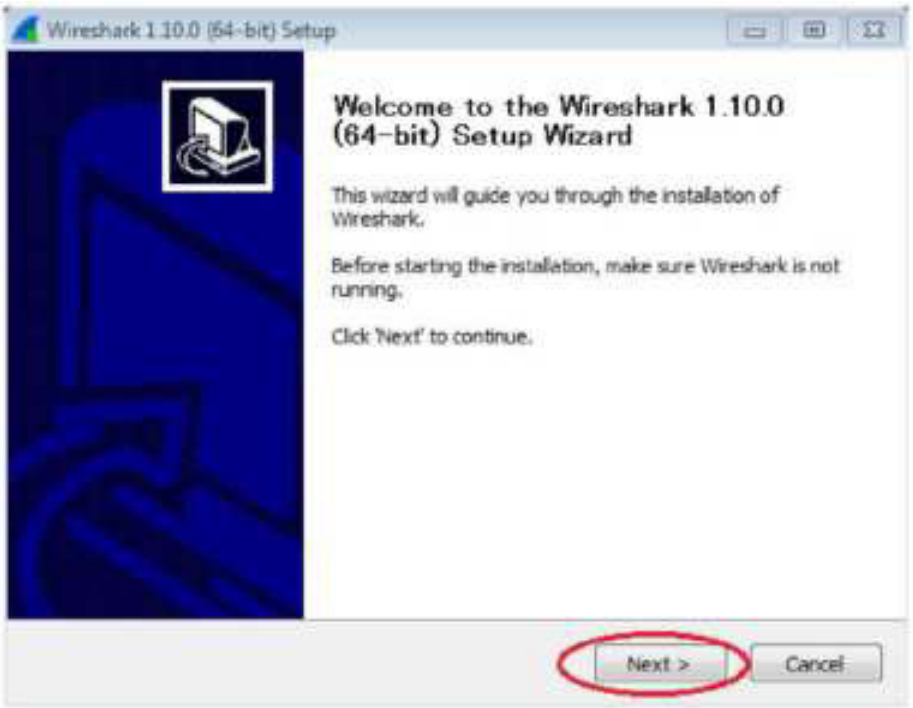
Шаг 2: Установите программу Wireshark.

a. Загруженный файл называется Wireshark-win64-x.x.x.exe, где «x» соответствует номеруверсии. Дважды нажмите на файл, чтобы начать установку.

b. Ответьте на все сообщения безопасности, которые появятся на экране. Если на вашем ПК уже имеется копия Wireshark, перед установкой программы появится запрос на удаление прежней версии. Рекомендуется удалить старую версию программы перед установкой новой. Чтобы удалить предыдущую версию программы Wireshark, нажмите кнопку Да.

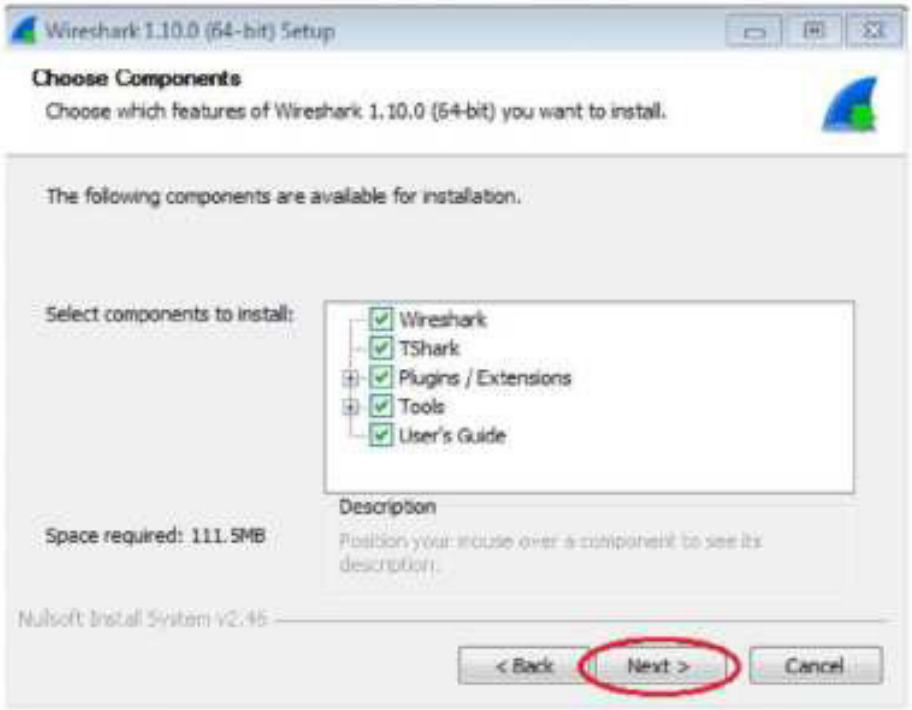


c. Если программа Wireshark устанавливается впервые или предыдущая версия была удалена, откроется мастер установки программы Wireshark. Нажмите кнопку Next (Далее).

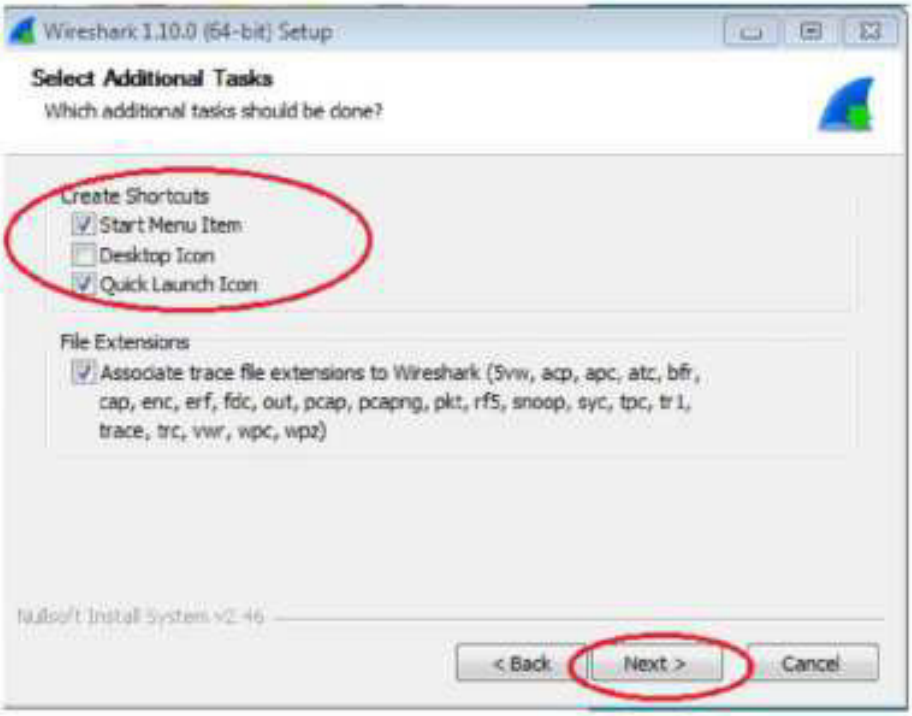


d. Выполните инструкции по установке. Когда откроется окно «License Agreement» (Лицензионное соглашение), нажмите кнопку I accept (Принять).

e. При выборе компонентов оставьте настройки по умолчанию и нажмите кнопку Next (Далее).



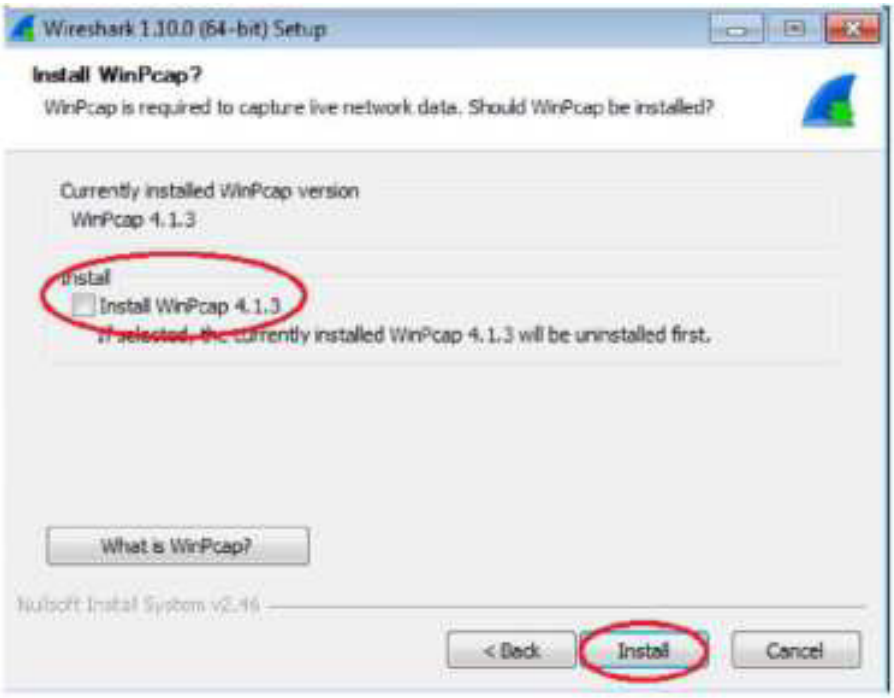
f. Выберите желаемые ярлыки и нажмите кнопку Next (Далее).



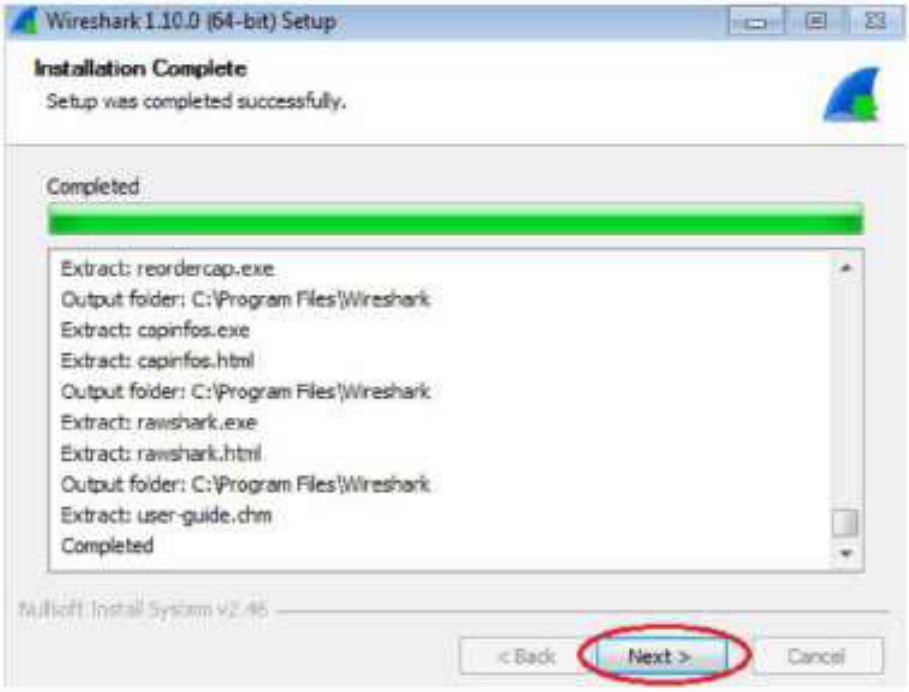
g. Если дисковое пространство ограничено, директорию установки можно изменить, в противном случае, оставьте адрес, указанный по умолчанию.

h. Для сбора сетевых данных на ваш ПК необходимо установить программу WinPcap. Если она уже установлена, флажок установки будет снят. Если установленная версия WinPcap старше версии, прилагаемой к программе Wireshark, рекомендуем установить более новую версию, нажав на флажок рядом с вариантом Install WinPcap x.x.x (Установить WinPcap x.x.x).

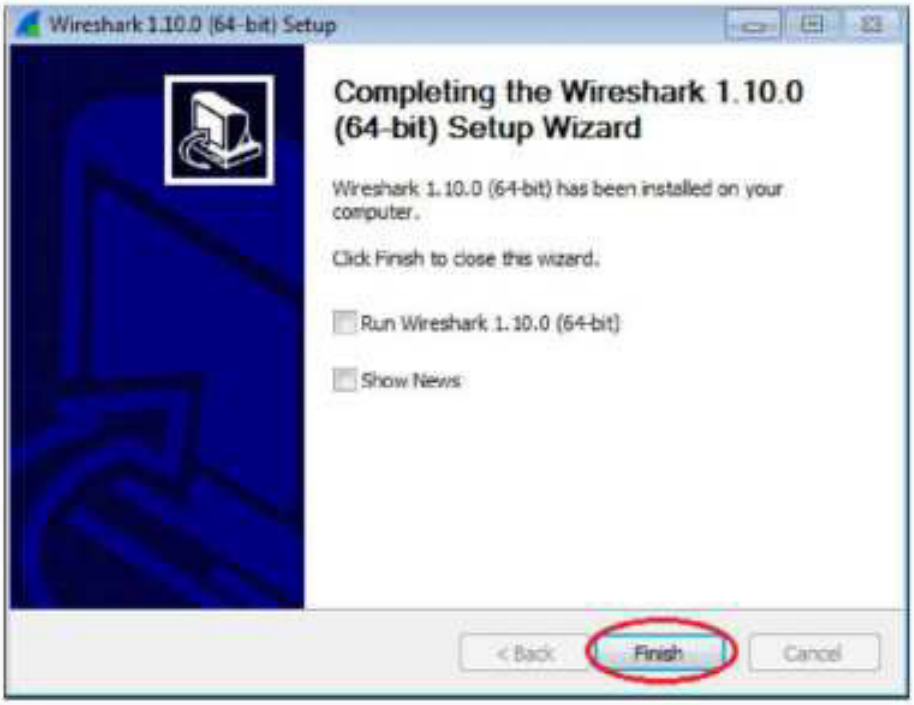
i. Если установка прошла успешно, закройте мастер установки WinPcap.



j. После этого начнётся установка программы Wireshark. Статус установки будет отображаться в отдельном окне. По завершении установки нажмите кнопку Next (Далее).



k. Для завершения процесса установки программы Wireshark нажмите Finish (Готово).



Часть 2: Сбор и анализ данных протокола ICMP по локальным узлам в программе Wireshark

В части 2 этой лабораторной работы вы должны отправить эхо-запрос с помощью команды ping на другой ПК в локальной сети и перехватить ICMP-запросы и отклики в программе Wireshark. Кроме того, вам нужно

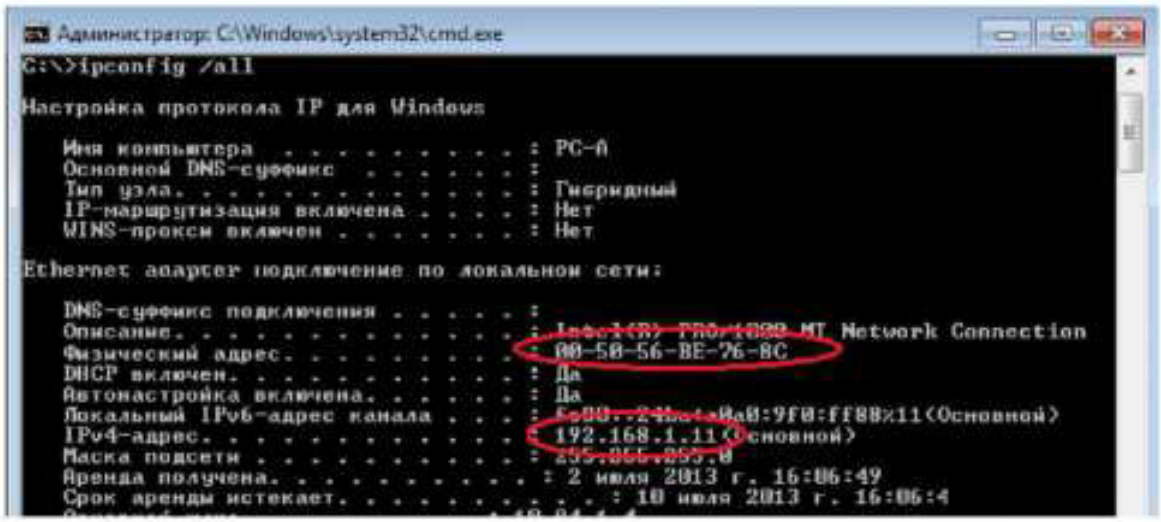
найти необходимую информацию в собранных кадрах. Этот анализ поможет понять, как используются заголовки пакетов для передачи данных по месту назначения.

Шаг 1: Определите адреса интерфейсов вашего ПК.

В данной лабораторной работе вам необходимо узнать IP-адрес компьютера и физический адрес сетевого адаптера, который называется MAC-адресом.

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

b. Запишите IP-адрес интерфейса ПК и MAC-адрес (физический адрес).

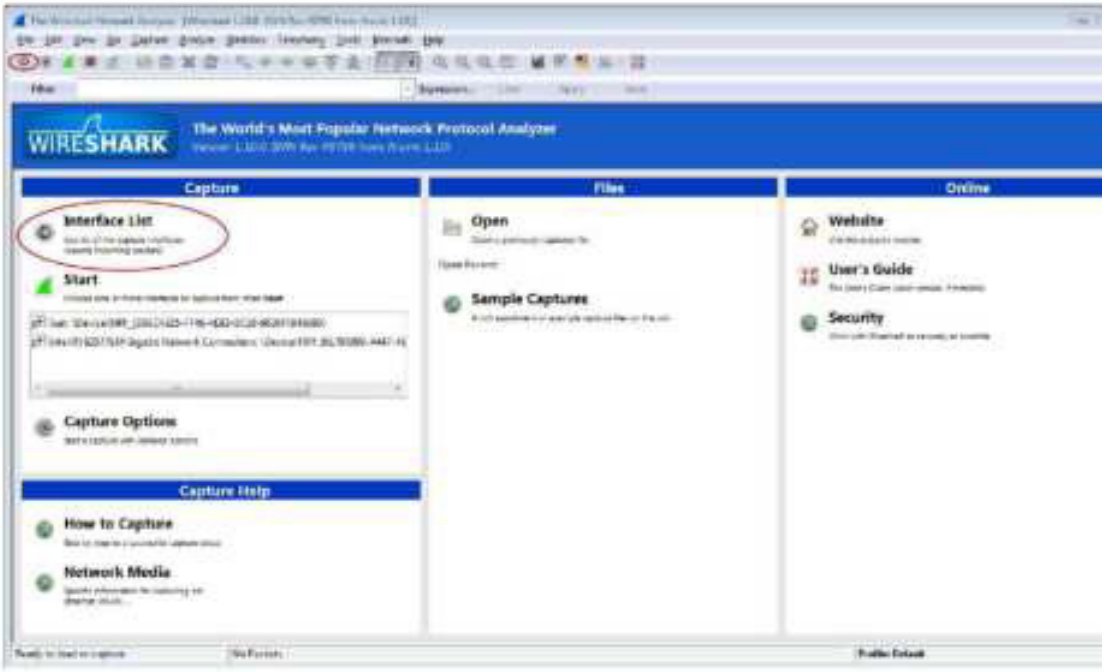


c. Обменяйтесь IP-адресами с другими учащимися, но пока что не сообщайте им свой MAC-адрес.

Шаг 2: Запустите программу Wireshark и начните перехват данных.

a. На своём ПК нажмите кнопку Пуск и найдите Wireshark в списке программ. Дважды нажмите на Wireshark.

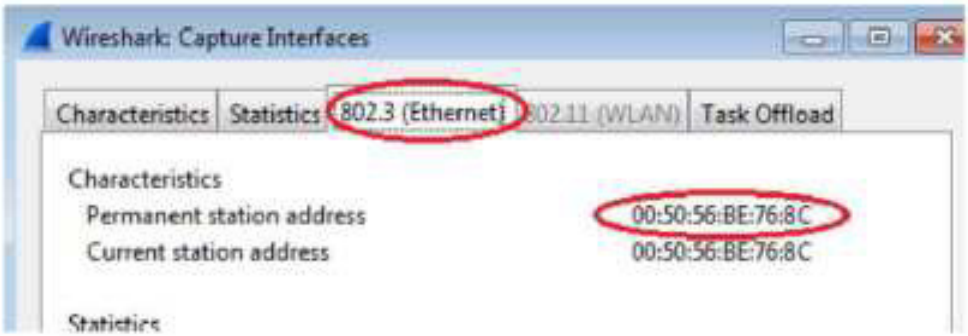
b. Запустив программу Wireshark, нажмите на параметр Interface list (Список интерфейсов).



Примечание. Список интерфейсов можно также открыть, нажав на значок первого интерфейса в ряду значков.

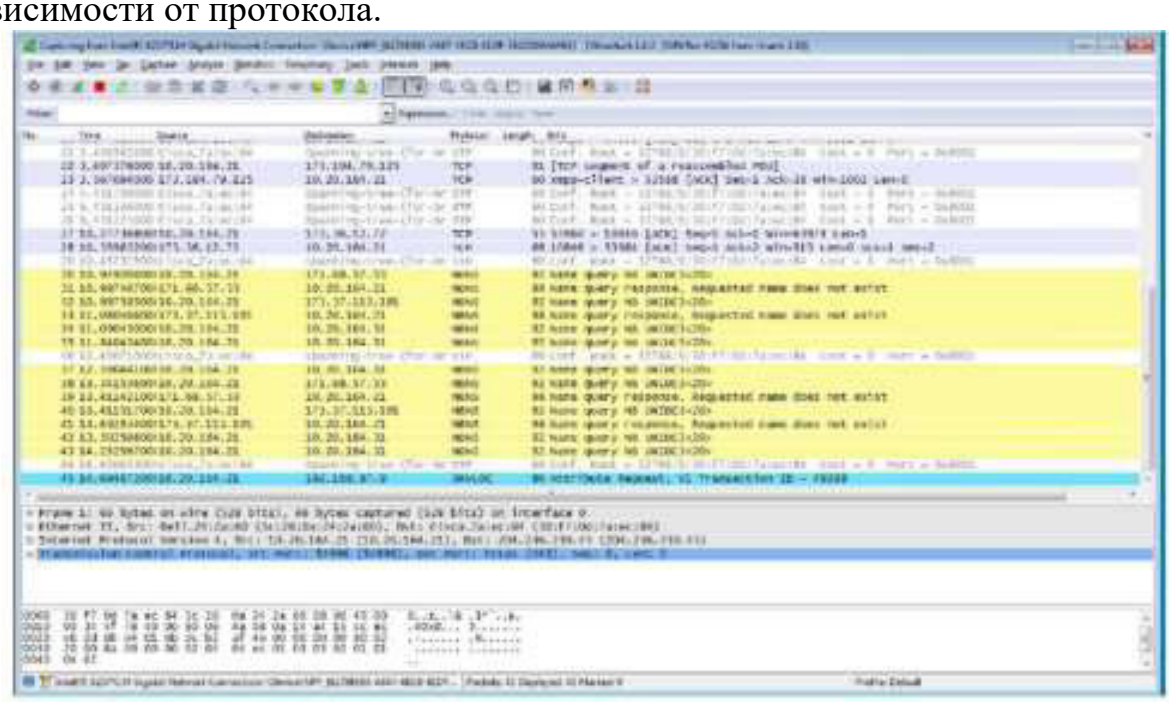
c. В окне «Capture Interfaces» (Перехват интерфейсов) программы Wireshark установите флажок рядом с интерфейсом, подключённым к вашей локальной сети.

Примечание. Если перечислено несколько интерфейсов и вы не уверены в том, какой из них нужно выбрать, нажмите кнопку Details (Подробнее) и откройте вкладку 802.3 (Ethernet). Убедитесь в том, что MAC-адрес соответствует результату, который вы получили в шаге 1b. Убедившись в правильности интерфейса, закройте окно информации.

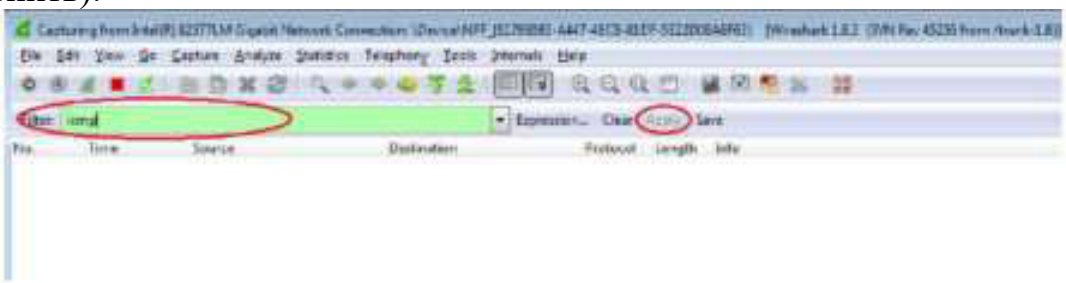


d. После этого нажмите кнопку Start (Начать), чтобы начать перехват данных.

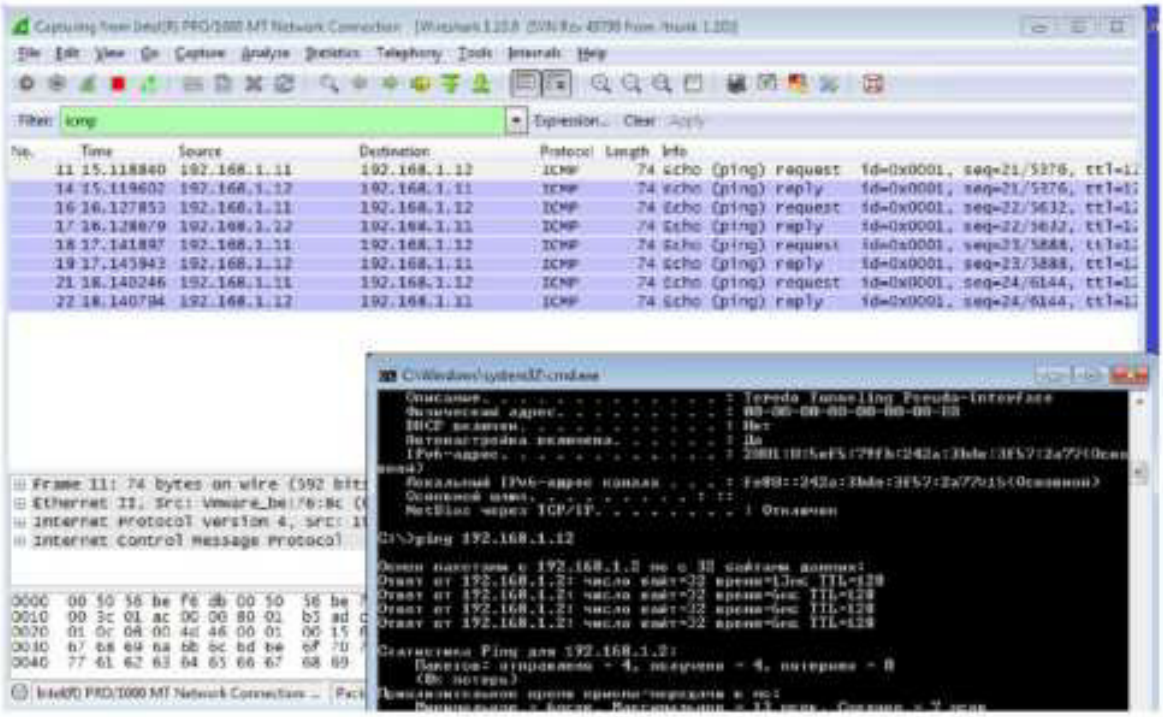
В верхней части окна программы Wireshark начнёт прокручиваться информация. Строки данных выделяются различными цветами в зависимости от протокола.



e. Информация может прокручиваться очень быстро в зависимости от типа связи между ПК и локальной сетью. Чтобы облегчить просмотр и работу с данными, собранными программой Wireshark, можно применить фильтр. В этой лабораторной работе нам нужны только протокольные блоки данных (PDU) ICMP (эхо-запрос с помощью команды ping). Чтобы вывести на экран только протокольные блоки данных ICMP (эхо-запрос с помощью команды ping), в поле фильтра в верхней части окна программы Wireshark введите icmp и нажмите клавишу ВВОД или кнопку Apply (Применить).

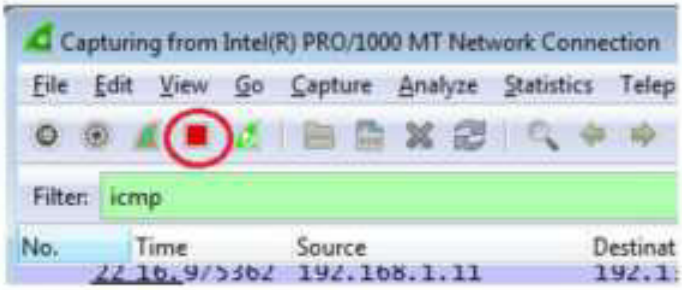


f. После этого все данные в верхнем окне исчезнут, однако перехват трафика в интерфейсе продолжится. Откройте окно командной строки, которое вы открывали ранее, и отправьте эхо- запрос с помощью команды ping на IP-адрес, полученный от другого учащегося. Обратите внимание на то, что в верхней части окна программы Wireshark снова появятся данные.



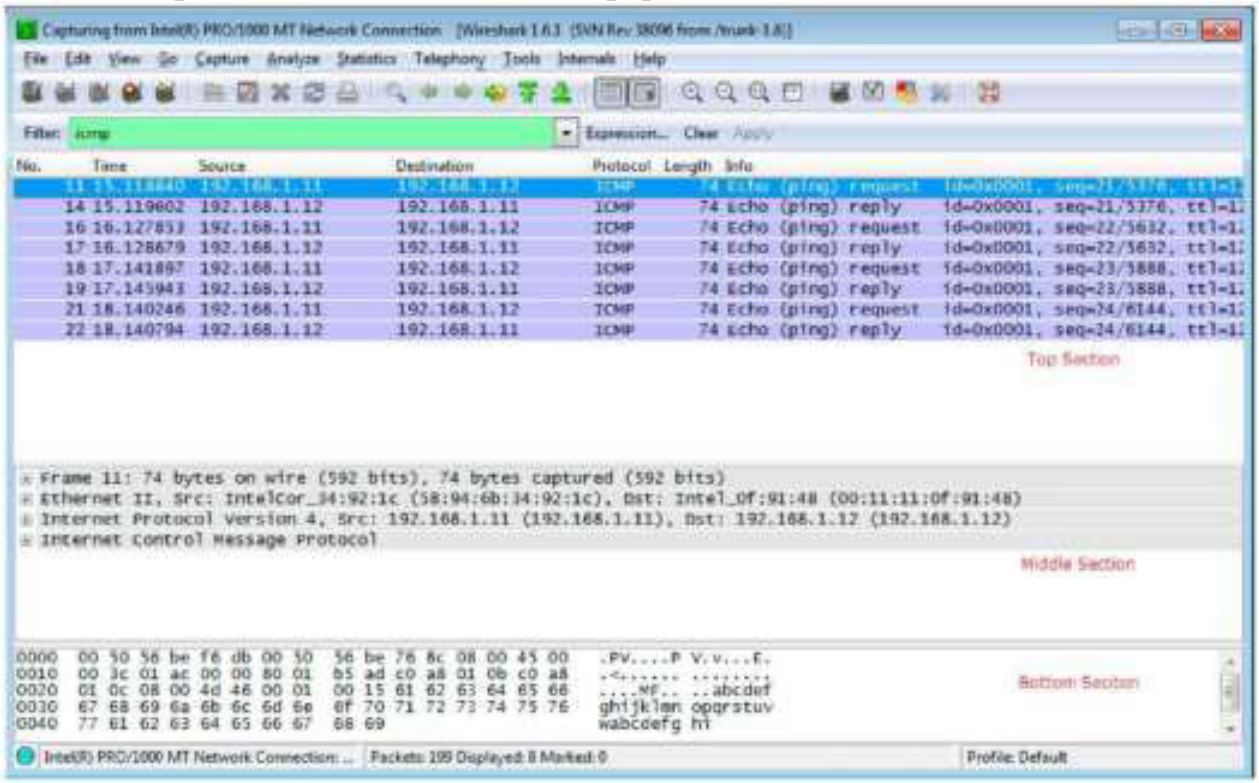
Примечание. Если компьютеры других учащихся не отвечают на ваши эхо-запросы, это может быть вызвано тем, что брандмауэры их компьютеров блокируют эти запросы. Информацию о том, как пропустить трафик ICMP через брандмауэр на ПК с ОС Windows 7, содержит Приложение А. Пропуск трафика ICMP через брандмауэр.

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

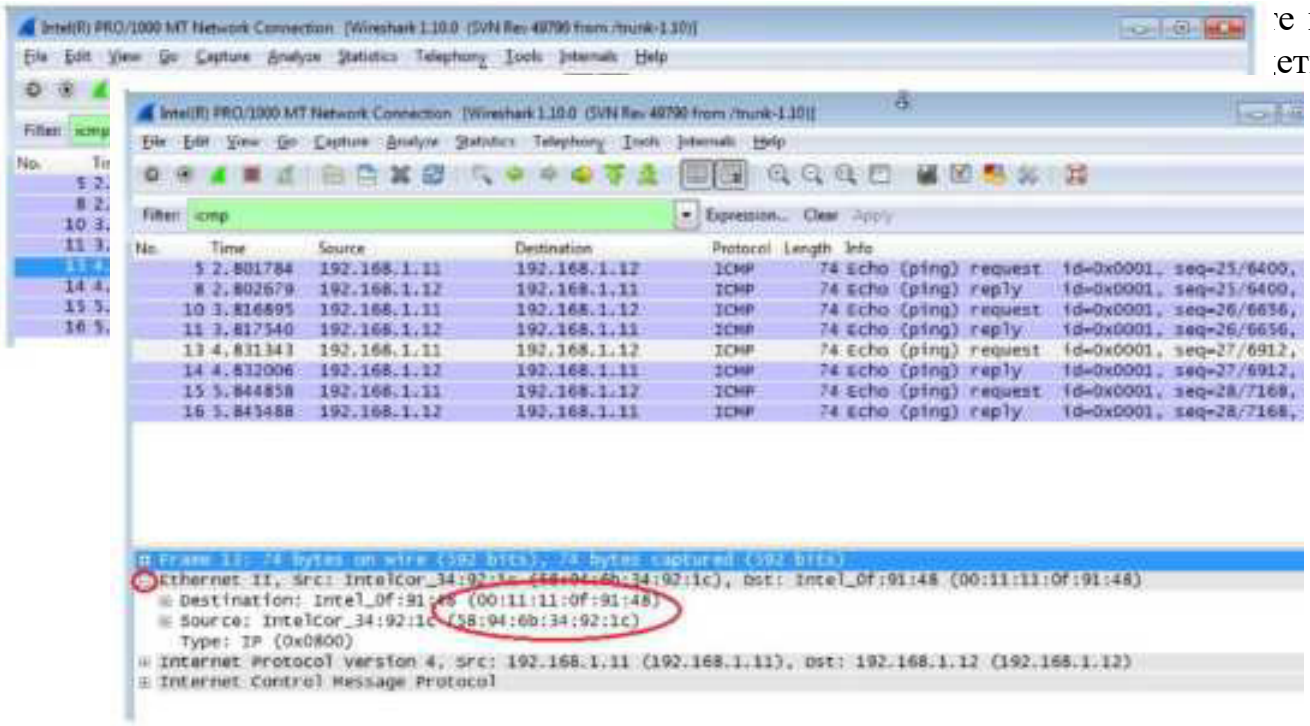


Шаг 3: Изучите полученные данные.

В шаге 3 необходимо проверить данные, сформированные эхо-запросами с помощью команды ping ПК других учащихся. Программа Wireshark отображает данные в трёх разделах: 1) в верхнем разделе отображается список полученных кадров PDU со сводной информацией об IP-пакетах; 2) в среднем разделе приводится информация о PDU для кадра, выбранного в верхнем разделе экрана, и деление кадра PDU на слои протоколов; 3) в нижнем разделе показываются необработанные данные каждого уровня. Необработанные данные отображаются как в шестнадцатеричном, так и десятичном форматах.



a. Выберите PDU-кадры первого запроса ICMP в верхнем разделе окна программы Wireshark. Обратите внимание на то, что в столбце Source (Источник) указывается IP-адрес вашего компьютера, а в столбце «Destination» (Назначение) — IP-адрес ПК, которому вы отправили эхо-запрос с помощью команды ping.



Совпадает ли MAC-адрес источника с интерфейсом вашего компьютера?

Совпадает ли MAC-адрес назначения в программе Wireshark с MAC-адресом другого учащегося?

Как ваш ПК вычислил MAC-адрес ПК, на который был отправлен эхо-запрос с помощью команды ping?

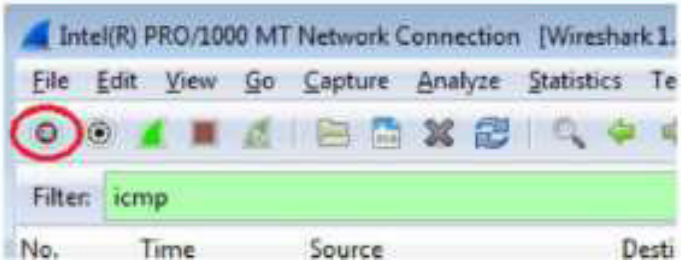
Примечание. В предыдущем примере перехваченного ICMP-запроса данные протокола ICMP инкапсулируются внутри PDU-пакета IPv4 (заголовка IPv4), который затем инкапсулируется в пакете кадра Ethernet II (заголовок Ethernet II) для передачи по локальной сети.

Часть 3: Сбор и анализ данных протокола ICMP по удалённым узлам в программе Wireshark

В части 3 вы должны будете отправить эхо-запросы с помощью команды ping на удалённые узлы (узлы за пределами локальной сети) и изучить данные, сформированные этими запросами. Затем вы определите различия между этими данными и данными, изученными в части 2.

Шаг 1: Запустите перехват данных в интерфейсе.

а. Нажмите на значок Interface List (Список интерфейсов), чтобы снова открыть список интерфейсов ПК

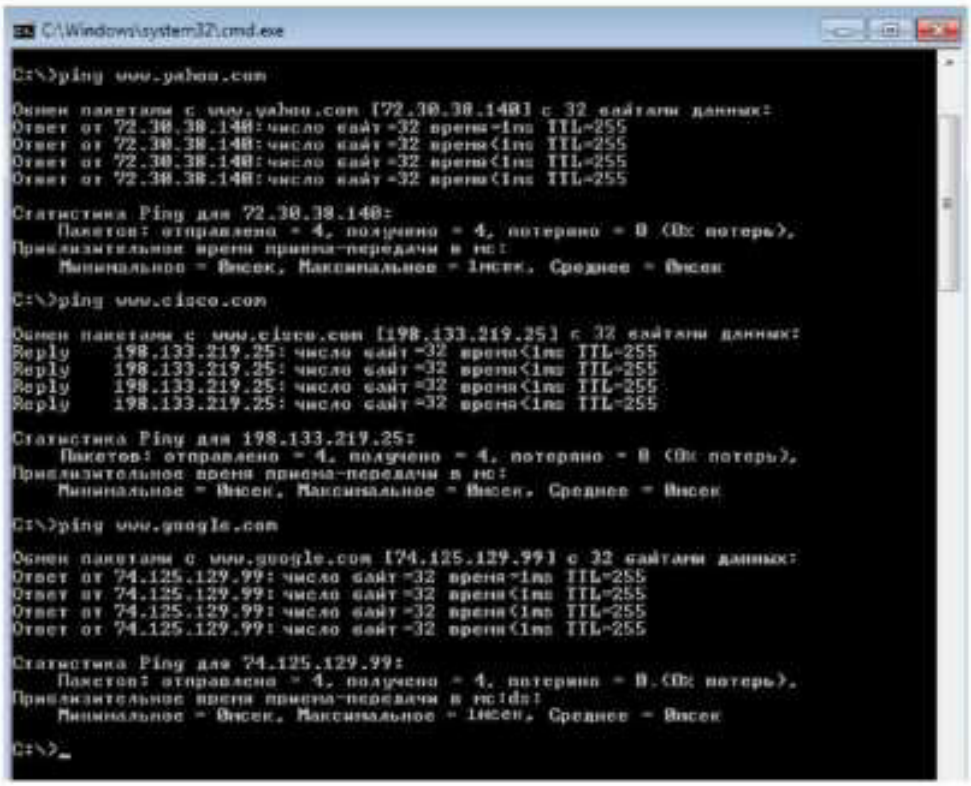


b. Убедитесь в том, что напротив интерфейса локальной сети установлен флажок, и нажмите кнопку Start (Начать).

c. Появится окно с предложением сохранить полученные ранее данные перед началом нового перехвата. Сохранять эти данные необязательно. Нажмите кнопку Continue withoutSaving (Продолжить без сохранения).

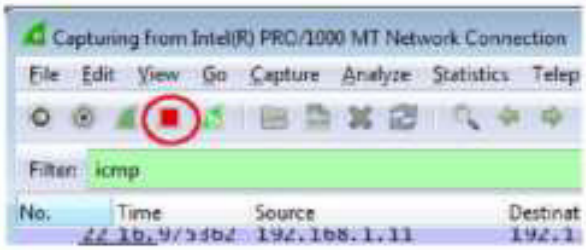
d. Активировав перехват данных, отправьте эхо-запрос с помощью команды ping на следующие три URL-адреса:

1) www.yahoo.com
2) www.cisco.com
3) www.google.com



Примечание. При отправке эхо-запросов с помощью команды ping на указанные URL-адреса обратите внимание на то, что служба доменных имен (DNS) преобразует URL в IP-адрес. Запишите IP-адреса, полученные для каждого URL-адреса.

e. Остановите перехват данных, нажав на значок Stop Capture (Остановить перехват).



Шаг 2: Изучите и проанализируйте данные, полученные от удалённых узлов.

a. Просмотрите собранные данные и изучите IP- и MAC-адреса трёх запрошенных веб-сайтов. Ниже укажите IP- и MAC-адреса назначения для всех трех веб-сайтов.

1адрес:P: MAC:

2адрес:P: MAC:

3адрес:P:MAC:Какова особенность этих данных?

b. Как эта информация отличается от данных, полученных в результате эхо-запросов локальных узлов в части 2?

Вопросы на закрепление

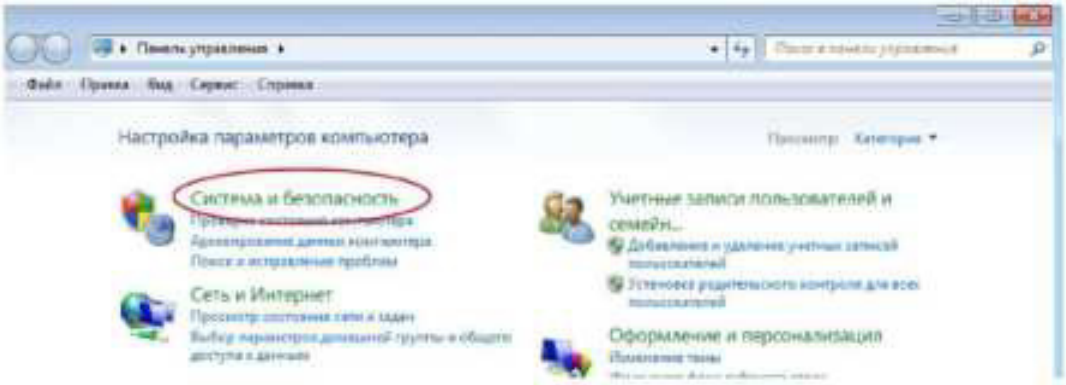
Почему программа Wireshark показывает фактический MAC-адрес локальных узлов, но не фактический MAC-адрес удалённых узлов?

Приложение А. Пропуск трафика ICMP через брандмауэр

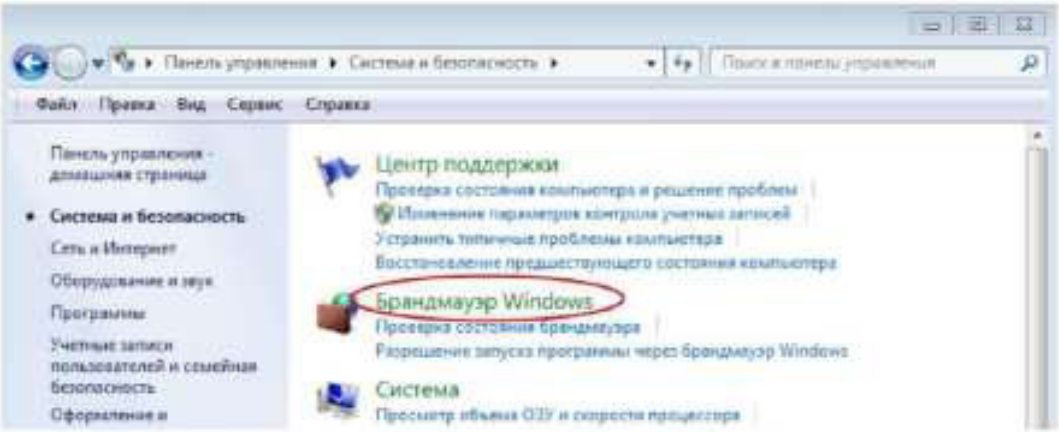
Если эхо-запросы с помощью команды ping с других компьютеров не проходят на ваш ПК, возможно, их блокирует брандмауэр. В этом приложении описывается, как пропустить эхо-запросы с помощью команды ping через брандмауэр и отменить новое правило брандмауэра по завершении лабораторной работы.

Шаг 1: Создайте новое правило, разрешающее прохождение ICMP-трафика через брандмауэр.

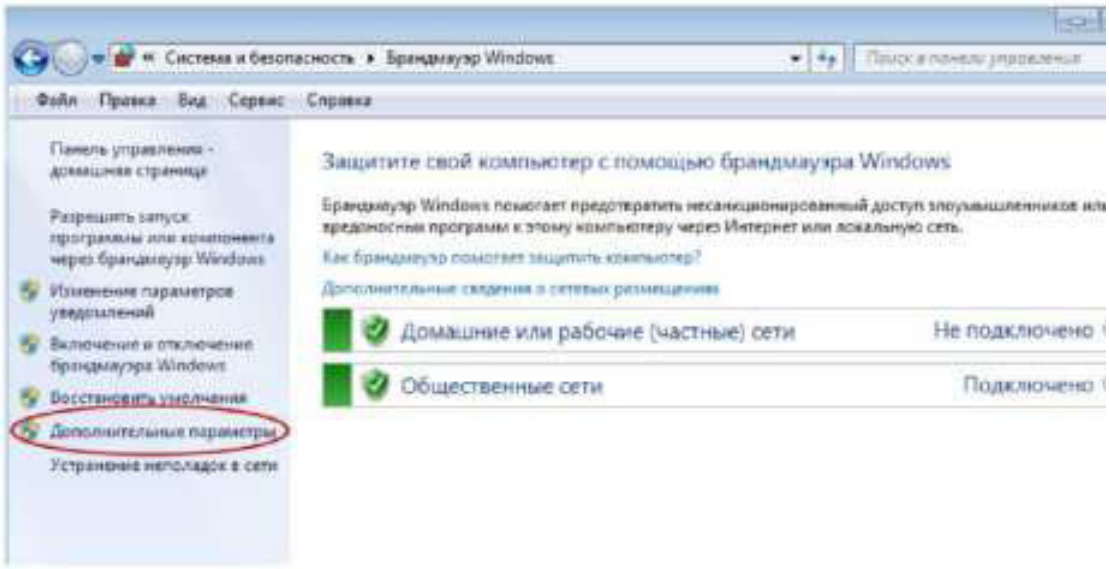
a. В панели управления выберите пункт Система и безопасность.



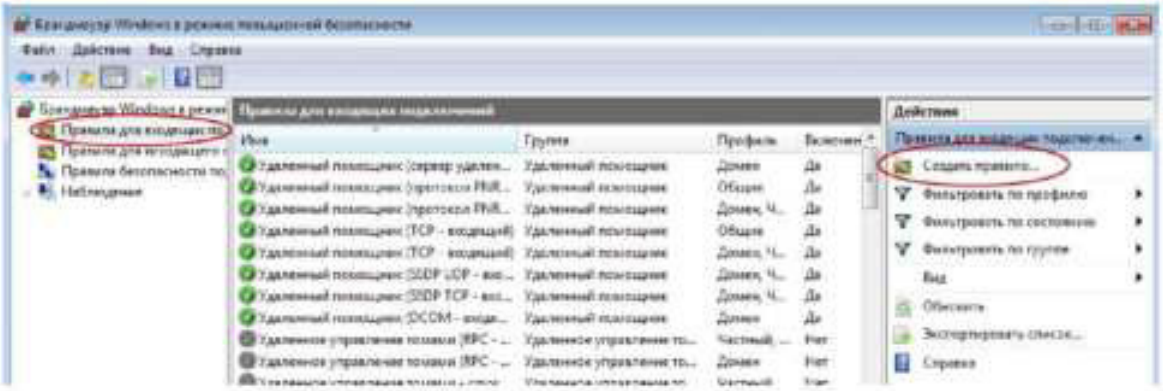
b. В окне «Система и безопасность» выберите Брандмауэр Windows.



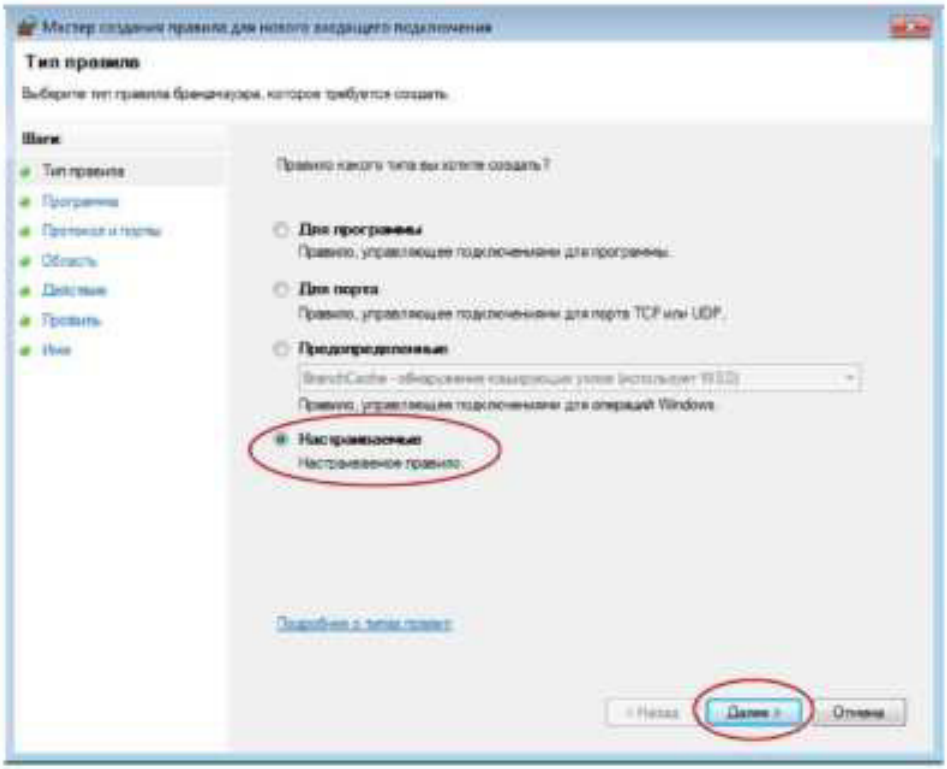
c. В левой части окна «Брандмауэр Windows» выберите Дополнительные параметры.



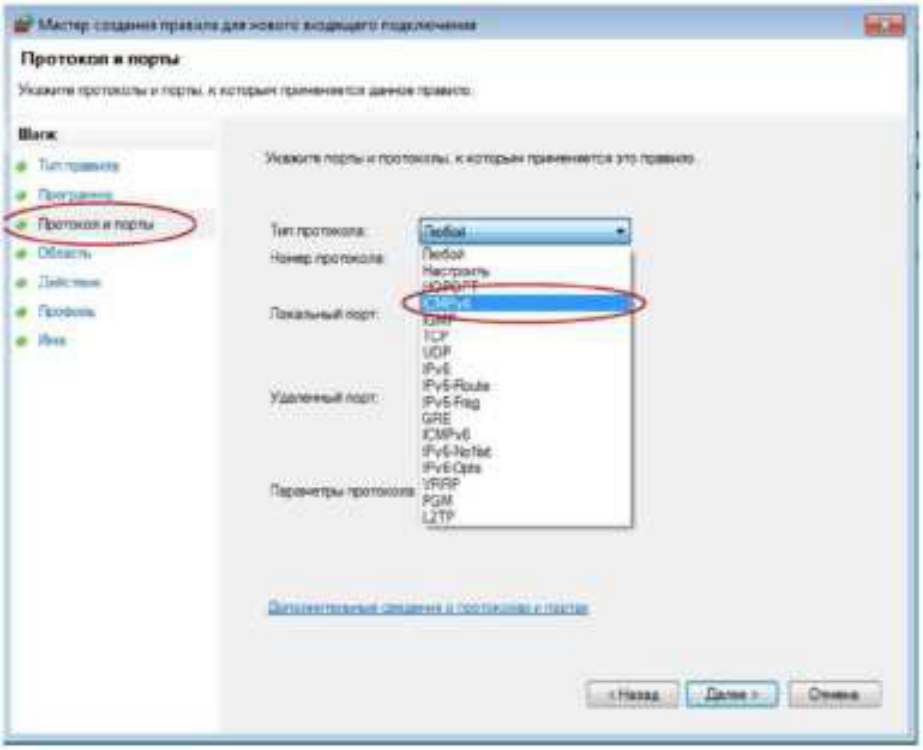
d. В окне «Дополнительные параметры» выберите в левой боковой панели Правила для входящих подключений, а затем Создать правило... в правой боковой панели.



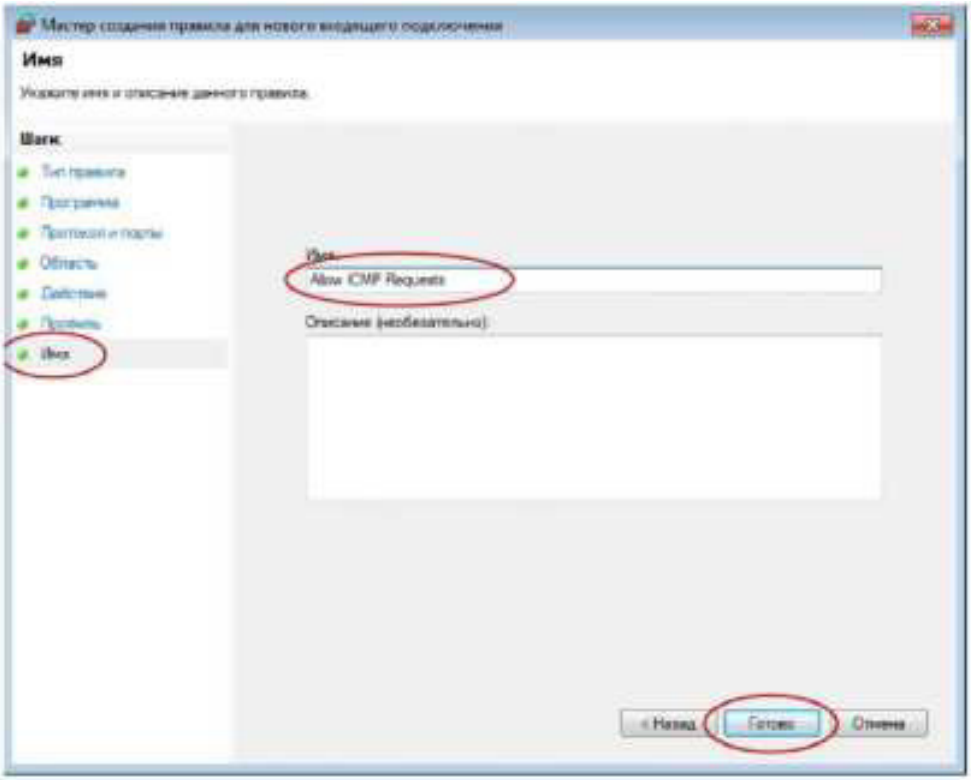
e. Откроется мастер создания новых правил для входящих подключений. В окне «Тип правила» установите переключатель Настраиваемые, и нажмите кнопку Далее.



f. В левой панели выберите Протоколы и порты и выберите пункт ICMPv4 в раскрывающемся меню типов протокола. После этого нажмите кнопку Далее.



g. В левой панели выберите Имя и введите в соответствующее поле Allow ICMP Requests. Нажмите кнопку Finish (Готово).

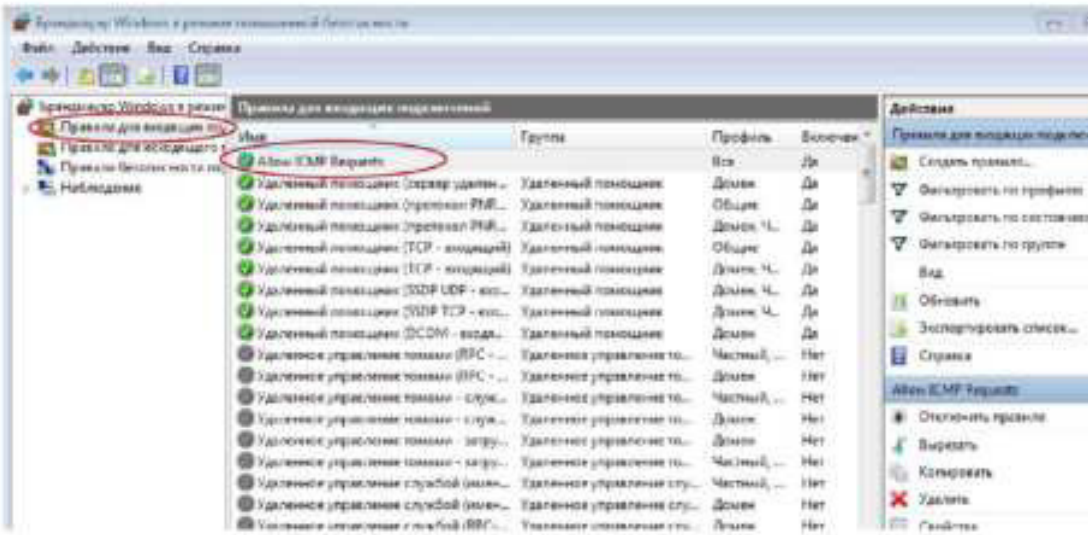


Созданное правило позволит другим учащимся получать эхо-отклики с вашего ПК.

Шаг 2: Отключите и удалите новое правило ICMP.

По завершении лабораторной работы необходимо отключить или удалить новое правило, созданное в шаге 1. Вариант Отключить правило позволит снова включить его при необходимости. Полное удаление правила навсегда удалит его из списка правил для входящих подключений.

a. В левой части окна «Дополнительные настройки безопасности» выберите Правила для входящих подключений и найдите правило, созданное в шаге 1.



b. Чтобы отключить правило, выберите вариант Отключить правило. После этого она изменится на вариант Включить правило. Правило можно включать и отключать. Состояние правила отображается в столбце «Включено» списка правил для входящих подключений.

с. Чтобы удалить правило ICMP навсегда, выберите вариант Удалить. После этого для разрешения запросов ICMP это правило нужно будет создать заново.

ИС I.	1Й.ШЫИ,..	nei
ие,,	Домен	Нет
ие..	Частный, ..	Нет
ие..	Домен	Нет
ие..	Домен	Нет
ие..	Частный, ..	Нет
ие м	Частный, ,.	Нет
ие..	Домен	Нет
И Р	Лпмрн	НРТ

Практическая работа 6 : определение сетевых устройств и кабелей

Задачи

Часть 1. Определение сетевых устройств

- Опишите функции и физические характеристики сетевого устройства. Часть 2. Определение сетевой среды
- Опишите функции и физические характеристики сетевой среды.

Исходные данные/сценарий

Как сотрудник отдела технической поддержки, вы должны уметь определять различное сетевое оборудование и его функцию в соответствующей части сети. В данной лабораторной работе вы получите доступ к сетевым устройствам и среде, определите их типы и характеристики.

Часть 1: Определение сетевых устройств

Преподаватель предложит вам определить различные сетевые устройства. Каждому из них будет присвоен идентификационный номер.

Заполните приведённую ниже таблицу, указав идентификационный номер устройства, название производителя и модель устройства, тип (концентратор, коммутатор или маршрутизатор), функцию (беспроводное устройство, маршрутизатор, коммутатор или комбинация функций) и другие физические характеристики, например количество типов интерфейсов. Первая строка уже заполнена в качестве образца.

Идентификатор	Производитель	Модель	Тип	Функции	Физические характеристики
					2 порта Gigabit Ethernet 2 слота EHWIC
1	Cisco	1941	Маршрутизатор	Маршрутизатор	2 слота CompactFlash 1 ISM-слот 2 порта консоли: USB, RJ-45
2					
3					
4					
5					
6					

Часть 2: Определение сетевой среды

Преподаватель предложит вам определить различные сетевые среды. Вам необходимо назвать сетевую среду, определить её тип (медные, оптоволоконные или беспроводные сети), дать краткое описание и указать типы подключаемых с её помощью устройств. Запишите эти данные в приведённую ниже таблицу. Первая строка уже заполнена в качестве образца

Идентификатор	Сетевая среда	Тип	Описание, к чему подключается
1	UTP	Медный кабель	Подключает сетевой адаптер и порты Ethernet проводной сети на сетевых устройствах. Прямой кабель категории 5. Подключает персональные компьютеры и маршрутизаторы к коммутаторам и коммутационным панелям.
2			
3			
4			
5			
6			

Вопросы на закрепление

Где можно найти дополнительную информацию об идентифицированном вами сетевом оборудовании?

Практическая работа 7: просмотр данных о беспроводных и проводных сетевых адаптерах

Задачи

Часть 1. Определение сетевых адаптеров ПК и работа с ними

Часть 2. Определение сетевых значков области уведомлений и их использование

Исходные данные/сценарий

В данной лабораторной работе вы должны определить доступность и состояние сетевых адаптеров на используемом ПК. ОС Windows предлагает множество способов просмотра и применения сетевых адаптеров.

Также в этой лабораторной работе вам нужно получить доступ к данным о сетевом адаптере вашего ПК и изменить его состояние.

Необходимые ресурсы

• Один ПК (ОС Windows 7, Vista или XP с двумя сетевыми адаптерами, проводным и беспроводным, а также с беспроводным подключением).

Примечание. В начале этой лабораторной работы проводной сетевой адаптер компьютера подключили к одному из встроенных портов коммутатора на беспроводном маршрутизаторе и активировали проводное подключение по локальной сети. Изначально беспроводной сетевой адаптер был отключён. Если проводной и беспроводной сетевые адаптеры включены, компьютеру будут присвоены два разных IP-адреса, причём беспроводной сетевой адаптер получит приоритет.

Часть 1: Определение сетевых адаптеров ПК и работа с ними

В части 1 вы определите различные типы сетевых адаптеров в используемом ПК и изучите разные способы получения данных о сетевых адаптерах, их включения и отключения.

Примечание. Данная Практическая работа была выполнена на ПК с ОС Windows 7. Её можно выполнить и в любой другой из указанных версий операционной системы Windows, однако параметры меню и окна в этом случае могут отличаться.

Шаг 1: Используйте «Центр управления сетями и общим доступом».

a. Откройте Центр управления сетями и общим доступом, нажав кнопку Пуск > Панель управления > Просмотр состояния сети и задач под заголовком «Сеть и Интернет»

в представлении по категориям.

b. В левой части экрана нажмите на ссылку Изменение параметров адаптера.

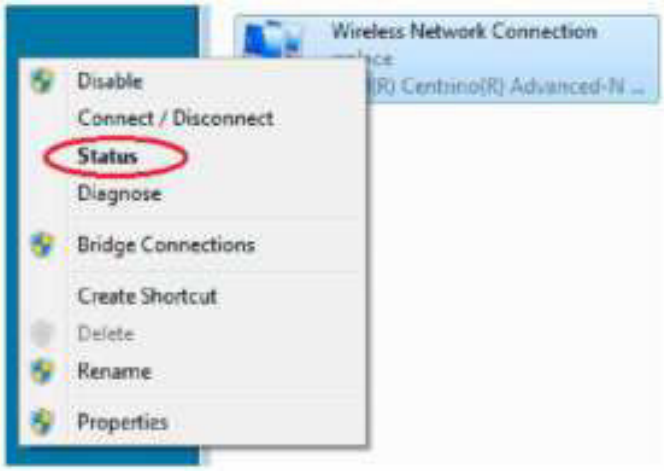
c. Откроется окно «Сетевые подключения» со списком доступных сетевых адаптеров. В данном окне найдите адаптеры локальной и беспроводной сети.

Примечание. В этом окне могут отображаться также адаптеры виртуальной частной сети (VPN) и другие типы сетевых подключений.

Шаг 2: Поработайте с беспроводным сетевым адаптером.

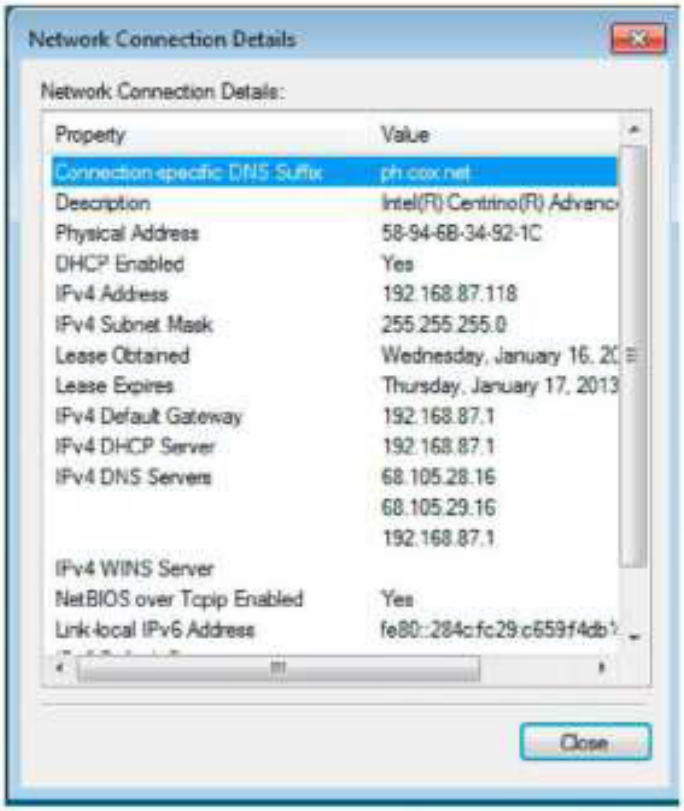
a. Выберите вариант Подключение по беспроводной сети и нажмите на неё правой кнопкой мыши, чтобы открыть раскрывающееся меню. Если беспроводной сетевой адаптер отключён, выберите вариант Включить. Если сетевой адаптер уже включён, в верхней строке раскрывающегося меню будет указан вариант Отключить. Если Подключение по беспроводной сети на данный момент отключено, выберите вариант Включить.

b. Нажмите правой кнопкой мыши на Подключение по беспроводной сети и выберите вариант Состояние.



c. Откроется окно «Состояние подключения по беспроводной сети» с информацией о беспроводном соединении.

Какой идентификатор SSID соответствует беспроводному маршрутизатору вашего подключения? Какова скорость вашего беспроводного подключения? d. Нажмите кнопку Подробнее, чтобы открыть сведения о сетевом подключении.



Какой MAC-адрес присвоен вашему беспроводному сетевому адаптеру? Указаны ли у вас несколько DNS-серверов IPv4? Зачем указано несколько DNS-серверов?

e. Изучив сведения о сетевом подключении, нажмите кнопку Закрыть.

f. Откройте окно ввода команды и введите ipconfig /all.

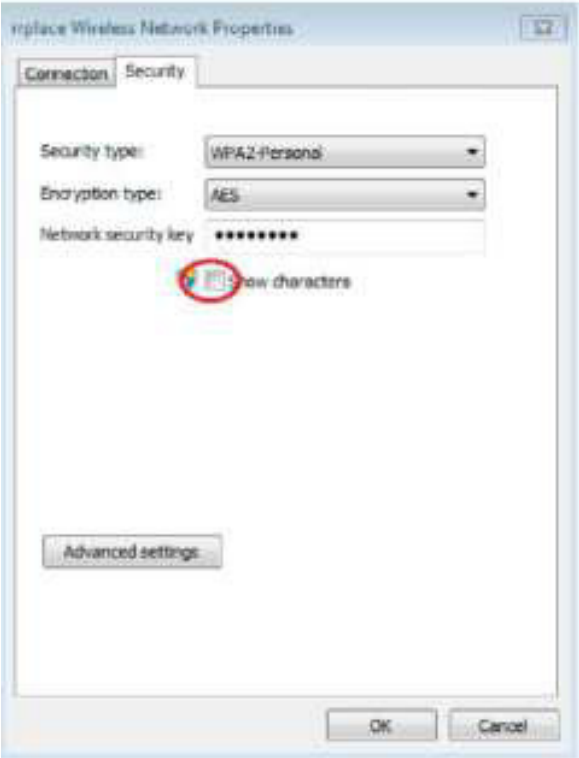
```
Wireless LAN adapter Wireless Network Connection:

   Connection-specific DNS Suffix  . : ph.cox.net
   Description . . . . . . . . . . . : Intel(R) Centrino(R) Advanced-N 6200 AGN
   Physical Address. . . . . . . . . : 58-94-6B-34-92-1C
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::284c:fc29:c659:f4db%11(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.87.118(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Thursday, January 17, 2013 8:30:40 AM
   Lease Expires . . . . . . . . . . : Friday, January 18, 2013 8:30:41 AM
   Default Gateway . . . . . . . . . : 192.168.87.1
   DHCP Server . . . . . . . . . . . : 192.168.87.1
   DHCPv6 IAID . . . . . . . . . . . : 307795051
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-14-AC-22-0A-5C-26-0A-24-2A-60
   DNS Servers . . . . . . . . . . . : 68.105.28.16
                                       68.105.29.16
                                       192.168.87.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Обратите внимание на то, что здесь отображается та же информация, что и в окне сведений о сетевом подключении из шага d.

g. Закройте окно ввода командной строки и окно сведений о сетевом подключении. После этого вы вернётесь в окно состояния беспроводного сетевого подключения. Нажмите на Свойства беспроводного соединения.

h. В окне Свойства беспроводного соединения откройте вкладку Безопасность.

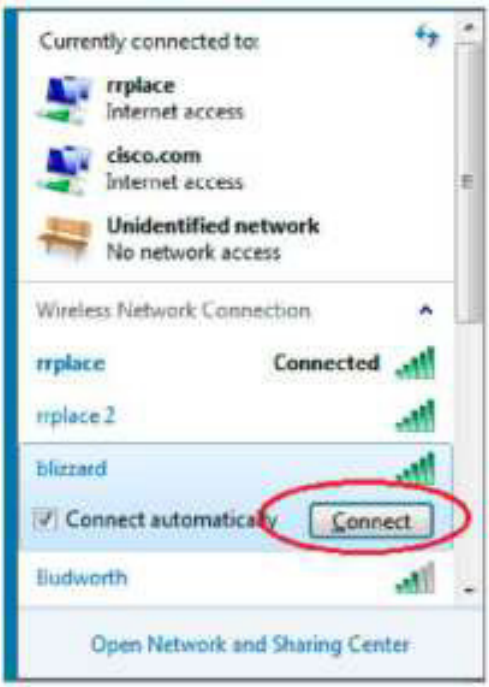
i. Откроется информация о типе мер безопасности, действующих на подключённом беспроводном маршрутизаторе. Установите флажок напротив варианта Показать символы, чтобы вместо скрытых символов увидеть действующий ключ безопасности сети. После этого нажмите кнопку OK



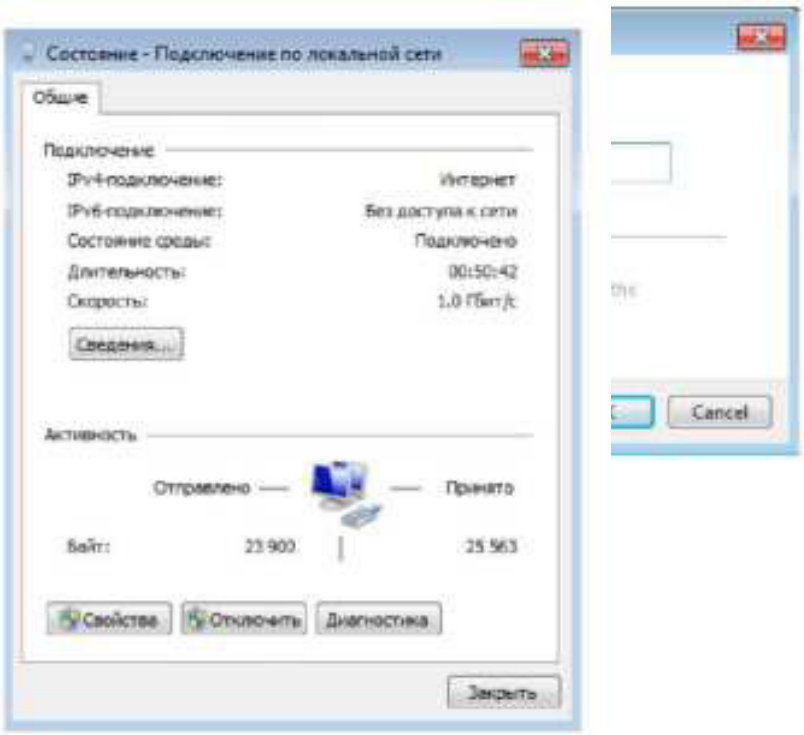
j. Закройте окна свойств беспроводной сети и состояния сетевого подключения. Нажмите правой кнопкой мыши на вариант Подключение по беспроводной сети > Подключить/Отключить.

После этого в правом нижнем углу экрана появится всплывающее окно со списком текущих подключений, а также список идентификаторов SSID, которые находятся в диапазоне беспроводного сетевого адаптера вашего ПК. Если в правой части этого окна есть полоса прокрутки, её можно использовать для просмотра дополнительных идентификаторов SSID

k. Для подключения к одному из других указанных идентификаторов SSID беспроводной сети выберите интересующий вас идентификатор и нажмите кнопку Подключить.

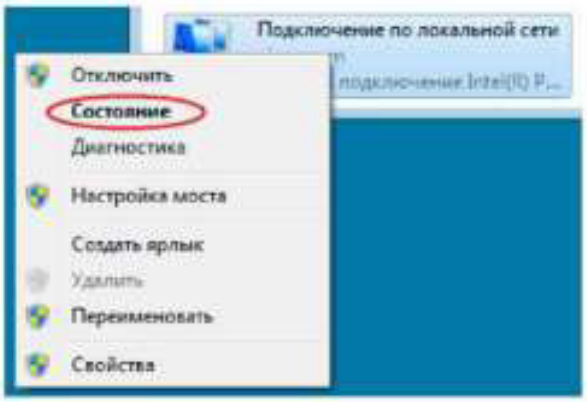


l. Если вы выбрали безопасный идентификатор SSID, нужно будет ввести Ключ безопасности для SSID. Введите ключ безопасности для этого идентификатора SSID и нажмите кнопку OK. Чтобы никто не смог прочитать вводимые символы в поле Ключ безопасности, установите флажок напротив варианта Скрыть символы.



Чтобы увидеть данные адреса локального подключения, нажмите кнопку Подробнее.

Шаг 3: Поработайте с проводным сетевым адаптером.



a. В окне «Сетевые подключения» нажмите правой кнопкой мыши на Подключение по локальной сети, чтобы открыть раскрывающийся список. Если сетевой адаптер отключён, включите его и выберите вариант Состояние.

Примечание. Для просмотра состояния сетевого адаптера ПК должен быть подключён к коммутатору или аналогичному устройству с помощью кабеля Ethernet. У многих беспроводных маршрутизаторов есть небольшой встроенный коммутатор с четырьмя Ethernet-портами. Вы можете подключиться к одному из этих портов с помощью прямого кабеля Ethernet.

b. Откроется окно «Состояние подключения по локальной сети». В нём отображается информация о проводном подключении к локальной сети.

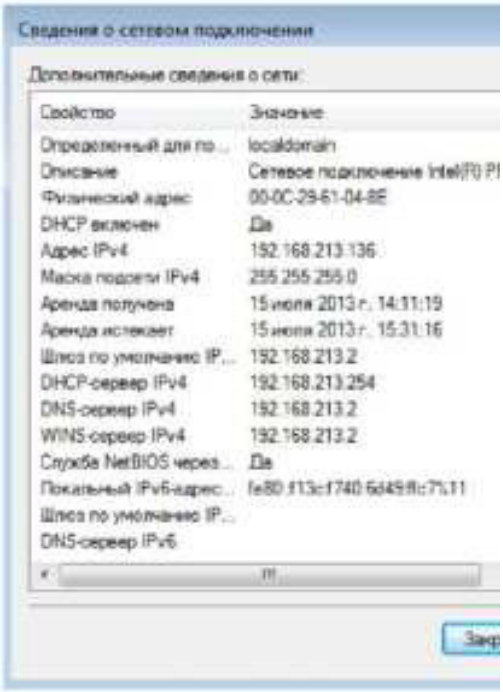
c. Откройте окно ввода команды и введите ipconfig /all. Найдите информацию о подключении по локальной сети и сравните её с информацией, указанной в окне «Сведения о сетевом подключении»

```
Ethernet adapter Подключение по локальной сети:

   DNS-суффикс подключения . . . . . : localdomain
   Описание. . . . . . . . . . . . . : Сетевое подключение Intel(R) PRO/1000 MT
   Физический адрес. . . . . . . . . : 00-0C-29-61-04-8E
   DHCP включен. . . . . . . . . . . : Да
   Автонастройка включена. . . . . . : Да
   Локальный IPv6-адрес канала . . . : fe80::f13c:f740:6d49:ffc7%11(Основной)
   IPv4-адрес. . . . . . . . . . . . : 192.168.213.136(Основной)
   Маска подсети . . . . . . . . . . : 255.255.255.0
   Аренда получена. . . . . . . . . . : 15 июля 2013 г. 15:20:08
   Срок аренды истекает. . . . . . . . . . : 15 июля 2013 г. 15:50:08
   Основной шлюз. . . . . . . . . : 192.168.213.2
   DHCP-сервер. . . . . . . . . . . : 192.168.213.254
   IAID DHCPv6 . . . . . . . . . . . : 234884137
   DUID клиента DHCPv6 . . . . . . . : 00-01-00-01-19-71-01-41-00-0C-29-61-04-8E

   DNS-серверы. . . . . . . . . . . : 192.168.213.2
   Основной WINS-сервер. . . . . . . : 192.168.213.2
   NetBios через TCP/IP. . . . . . . : Включен
```

d. Закройте все окна на рабочем столе.

Часть 2: Определение сетевых значков области уведомлений и их использование

В части 2 вы будете использовать сетевые значки в области



уведомлений для определения и контроля сетевого адаптера на вашем ПК.

Шаг 1: Используйте значок беспроводной сети.

a. Чтобы открыть всплывающее окно со списком идентификаторов SSID в диапазоне сетевого адаптера, нажмите на значок Беспроводная сеть в области уведомлений. Если в области уведомлений отображается значок

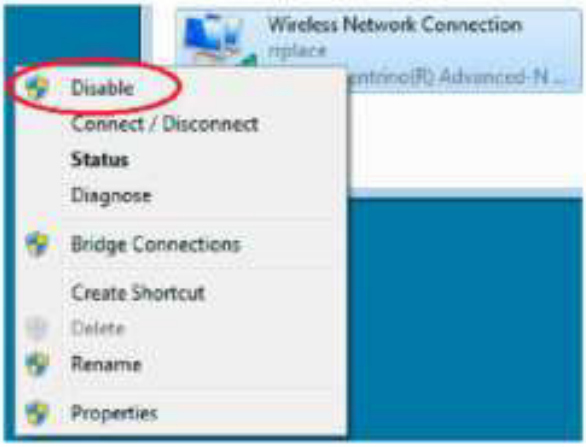
b. Нажмите пункт Открыть центр управления сетями и общим доступом. Примечание. Это

быстрый способ открыть это окно.

беспроводной сети, это означает, что беспроводной сетевой адаптер работает.

c. В левой части экрана нажмите на ссылку Изменение параметров адаптера, чтобы открыть окно «Сетевые подключения».

d. Нажмите правой кнопкой мыши на Подключение по беспроводной сети и выберите вариант Отключить, чтобы отключить беспроводной сетевой адаптер.



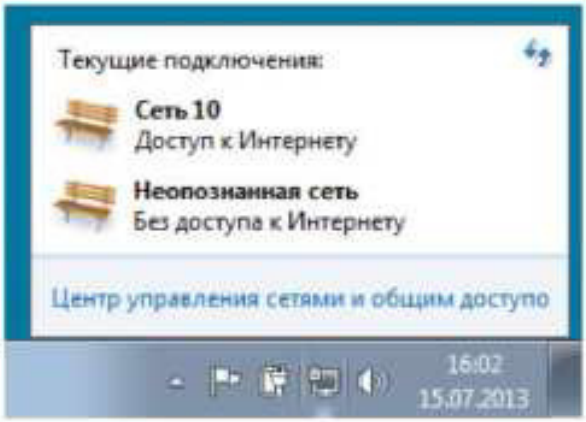
e. Посмотрите на область уведомлений. Значок Подключение по беспроводной сети должен смениться на значок Проводная сеть, который показывает, что для сетевого соединения используется проводной сетевой адаптер.

Примечание. Если работают оба сетевых адаптера, то в области уведомлений отображается значок Беспроводная сеть.

Шаг 2: Воспользуйтесь значком проводной сети.

a. Нажмите на значок Проводная сеть. Обратите внимание на то, что беспроводные

идентификаторы SSID больше не отображаются в этом всплывающем окне, но возможность открыть окно «Центр управления сетями и общим доступом» сохранилась.

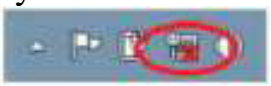


b. Нажмите Открыть центр управления сетями и общим доступом > Изменить параметры адаптера и выберите вариант Включить для параметра Подключение к беспроводной сети. Значок Беспроводная сеть должен заменить значок Проводная сеть в области уведомлений.

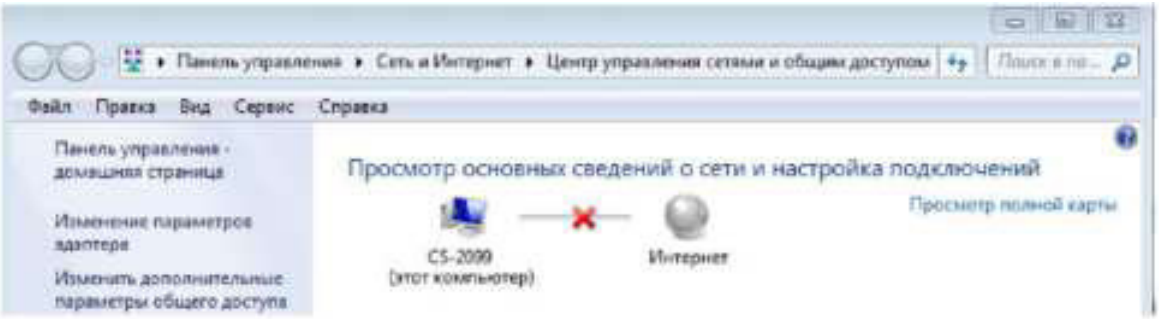
Шаг 3: Определите значок «Ошибка сети»

a. В окне «Сетевые подключения» отключите варианты Подключение по беспроводной сети и Подключение по локальной сети .

b. Теперь в области уведомлений отображается значок Сеть отключена, что указывает на отсутствие сетевого подключения.



c. Нажмите на этот значок, чтобы вернуться в раздел «Центр управления сетями и общим доступом» (изучите схему сети сверху).



Нажмите на красный X, чтобы ПК нашёл и устранил проблему с сетевым подключением. Средство диагностики попытается устранить неполадки с сетью.

d. Если это не помогло и сетевой адаптер не работает, рекомендуется найти и устранить неполадки подключения вручную.

Примечание. Если сетевой адаптер включён, но не может установить сетевое подключение, то в области уведомлений появляется значок Ошибка сети.

Если появился такой значок, можно попытаться решить эту проблему точно так же, как указано в шаге 3с.

Вопросы на закрепление

Зачем активировать на ПК больше одного сетевого адаптера?

Практическая работа 8. Просмотр MAC-адресов сетевых устройств

Топология

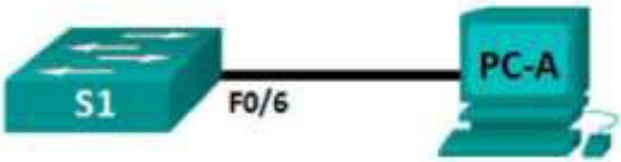


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
S1	VLAN 1	192.168.1.1	255.255.255.0	—
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Задачи

Часть 1. Настройка устройств и проверка подключения Часть 2. Отображение, описание и анализ MAC-адресов Ethernet

Общие сведения/сценарий

Каждое устройство в локальной сети Ethernet определяется MAC-адресом уровня 2. Этот адрес назначается производителем и хранится в микропрограммном обеспечении сетевой платы. В ходе лабораторной работы вам предстоит изучить и проанализировать компоненты MAC-адреса, а также процедуры поиска такой информации на коммутаторе и ПК.

Вы подключите оборудование, как показано в топологии. Затем вы настроите коммутатор и ПК в соответствии с таблицей адресации и протестируете настроенные конфигурации, проверив подключение к сети.

После завершения настройки и проверки подключения к сети вы должны будете ответить на вопросы о сетевом оборудовании, используя различные команды для получения данных от устройств.

Примечание. Используются коммутаторы Cisco Catalyst 2960s с Cisco IOS версии 15.0(2) (образ lanbasek9). Допускается использование других

моделей коммутаторов и других версий Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и результаты их выполнения могут отличаться от тех, которые показаны в лабораторных работах.

Примечание. Убедитесь, что все настройки коммутатора удалены и загрузочная конфигурация отсутствует. Если вы не уверены, обратитесь к инструктору.

Необходимые ресурсы

- 1 коммутатор (Cisco 2960 с ПО Cisco IOS версии 15.0(2) с образом lanbasek9 или аналогичная модель)
- 1 ПК (под управлением Windows 7 или 8 с программой эмуляции терминала, например, Tera Term)
- Консольный кабель для настройки коммутатора Cisco через консольные порты
- Кабели Ethernet, расположенные в соответствии с топологией

Часть 1: Настройка устройств и проверка подключения

В этой части вам необходимо настроить топологию сети и базовые параметры, такие как IP-адреса интерфейсов и имя устройства. Данные об имени и адресах устройств см. в таблицах топологии и адресации.

Шаг 1: Создайте сеть согласно топологии.

a. Подключите устройства, показанные в топологии, и кабели соответствующим образом.

b. Включите все устройства в топологии.

Шаг 2: Настройте ^4-адрес на ПК.

a. Настройте ^4-адрес, маску подсети и адрес шлюза по умолчанию для компьютера PC-A.

b. Из командной строки компьютера PC-A отправьте эхо-запрос на адрес коммутатора. Успешно ли выполнена проверка связи? Дайте пояснение.

Pinghasfailedbecause wedidn'tsetup Vlanl interfaceonSI yet.

Шаг 3: Настройте базовые параметры коммутатора.

В этом шаге вам необходимо настроить имя устройства и IP-адрес, а также отключить на коммутаторе поиск DNS.

```
Switch> enable
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/
Switch(config)#
```

b. Назначьте коммутатору имя узла в соответствии с таблицей адресации.

```
Switch(config)# hostna
```

c. Отключите поиск DNS.

```
S1(config)# no ip domain-l
```

d. Настройте и включите интерфейс SVI для сети VLAN 1.

```
S1(config)# interface vlan 1
S1(config if)# ip address 192.168.1.1 255.255.255.0
S1(config if)# no shutdown
S1(config if)# end
*Mar 1 00:07:59.048: %SYS-5-CONFIG 1: Configured from console by cons
```

а. Подключитесь к коммутатору с помощью консоли и перейдите в режим глобальной настройки.

Шаг 4: Проверьте подключение к сети.

Отправьте эхо-запрос с компьютера PC-A. Успешно ли выполнена проверка связи? nnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnn

Часть 2: Отображение, описание и анализ MAC-адресов Ethernet

У каждого устройства в локальной сети Ethernet есть MAC-адрес, который назначается производителем и хранится в микропрограммном обеспечении сетевой платы. MAC-адреса Ethernet имеют длину 48 битов и отображаются в виде шести наборов шестнадцатеричных цифр, которые обычно отделяются друг от друга с помощью тире, двоеточия или точки. В следующем примере один и тот же MAC-адрес представлен тремя различными способами.

00-05-9A-3C-78-00 00:05:9A:3C:78:00 0005.9A3C.7800

Примечание. MAC-адреса называют также физическими адресами, аппаратными адресами или адресами Ethernet.

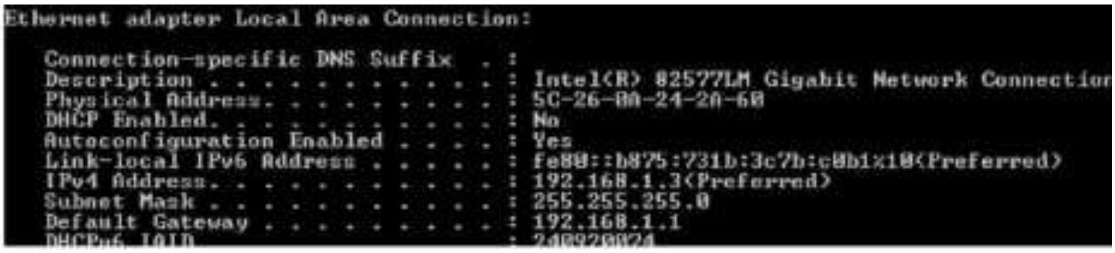
Вам необходимо выполнить команды для отображения MAC-адресов на ПК и коммутаторе, а затем проанализировать свойства каждого адреса.

Шаг 1: Проанализируйте MAC-адрес сетевой платы компьютера PC-A.

Прежде чем анализировать MAC-адрес компьютера PC-A, посмотрите пример сетевой платы другого ПК. Для просмотра MAC-адресов сетевых плат введите команду ipconfig /all . Пример результата выполнения данной команды показан ниже. При использовании команды ipconfig /all помните, что MAC-адреса называются физическими адресами. При чтении MAC-адреса слева направо первые шесть шестнадцатеричных цифр обозначают поставщика (производителя) данного устройства. Первые шесть шестнадцатеричных цифр (3 байта) называют также уникальным идентификатором организации (OUI). Этот трехбайтный код назначается поставщику организацией IEEE. Чтобы определить производителя, можно воспользоваться инструментом www.macvendorlookup.com или просмотреть зарегистрированные идентификаторы производителей оборудования на веб-сайте IEEE. Информация по OUI расположена на сайте IEEE по следующему адресу:

http://standards.ieee.org/develop/regauth/oui/public.html. Последние шесть цифр — это серийный номер сетевой платы, присвоенный производителем.

а. Используя результаты выполнения команды ipconfig /all, ответьте на следующие вопросы.



```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82577LM Gigabit Network Connectio
   Physical Address. . . . . . . . . : 5C-26-0A-24-2A-60
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::b875:731b:3c7b:c0b1%10(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.3(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 240920024
```

Какая часть MAC-адреса этого устройства соответствует OUI? 5C-26-0A

Какая часть MAC-адреса этого устройства соответствует серийному номеру? 555555555555555555555555555555555555555555555555555555555555 555555555555555 В приведенном выше примере определите производителя сетевой платы.

55555555555555555555555555555555555555555555555555555555 55555555555555555555

b. Введите команду ipconfig /all в командной строке на компьютере PC-A и определите OUI в MAC- адресе сетевой платы компьютера PC-A.

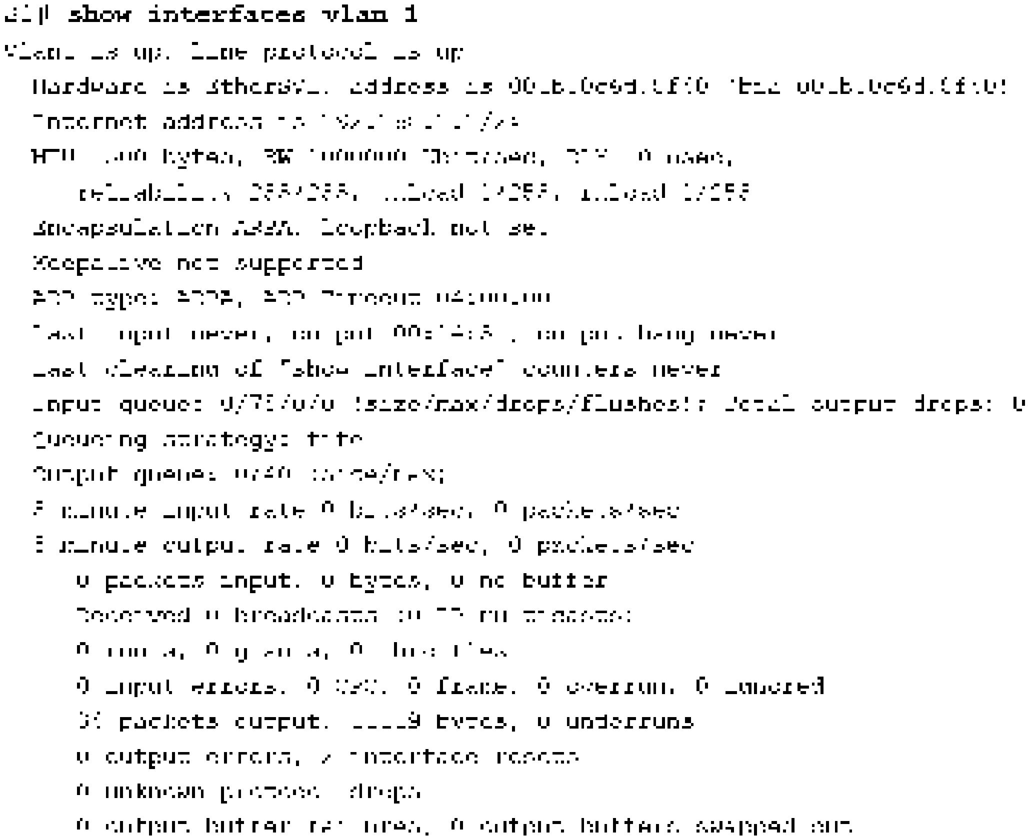
55555555555555555555555555555555555555555555555555555555 55555555555555555555 Определите серийный номер в MAC-адресе сетевой платы компьютера PC-A. 555555555555555555555555555555555555555555555555555555555555 555555555555555

Определите производителя сетевой платы компьютера PC-A. CISCOSYSTEMS, INC.

Шаг 2: Проанализируйте MAC-адрес интерфейса F0/6 коммутатора S1.

Для отображения MAC-адреса на коммутаторе можно использовать различные команды.

a. С помощью консоли подключитесь к коммутатору S1 и выполните команду show interfaces vlan 1, чтобы найти информацию о MAC-адресе. Пример показан ниже. Чтобы ответить на вопросы, используйте выходные данные, сгенерированные коммутатором.



```
S1# show interfaces vlan 1
Vlan1 is up, line protocol is up
  Hardware is EtherSVI, address is 001b.0c6d.8f40 (bia 001b.0c6d.8f40)
  Internet address is 192.168.1.11/24
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:14:51, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     34 packets output, 11119 bytes, 0 underruns
     0 output errors, 2 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
```

Какой MAC-адрес имеет интерфейс VLAN 1 на коммутаторе S1?

CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC Какой серийный номер указан в MAC-адресе интерфейса VLAN 1?

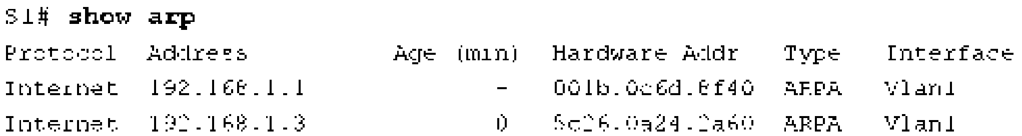
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC Какой OUI имеет интерфейс VLAN 1?

CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC Назовите производителя оборудования согласно OUI.

CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC Что означает bia?

CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC Почему в результатах выполнения команды дважды указан один и тот же MAC-адрес? CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC CCCCCCCCCCCCCCCCCCCCCCCCCCCC

b. Другой способ отображения MAC-адреса на коммутаторе — это команда show arp. Отобразите MAC-адрес с помощью команды show arp. Она сопоставляет адрес уровня 2 с соответствующим адресом уровня 3. Пример показан ниже. Чтобы ответить на вопросы, используйте выходные данные, сгенерированные коммутатором.



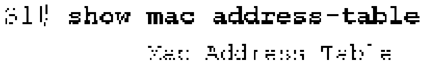
```
S1# show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.1.1              -   001b.0c6d.8f40  ARPA   Vlan1
Internet  192.168.1.3              0   5c26.0a24.2a60  ARPA   Vlan1
```

Какие адреса уровня 2 отображены на коммутаторе S1? nnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnn Какие адреса уровня 3 отображены на коммутаторе S1?

nnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnn

Шаг 3: Посмотрите на MAC-адреса коммутатора.

Выполните команду show mac address-table на коммутаторе S1. Пример показан ниже. Чтобы ответить на вопросы, используйте выходные данные, сгенерированные коммутатором.



```
S1# show mac address-table
          Mac Address Table
```

Vlan	Mac Address	Type	Ports
All	0100.0ccc.cccc	STATIC	CPU
All	0100.0ccc.cccd	STATIC	CPU
All	0180.c200.0000	STATIC	CPU
All	0180.c200.0001	STATIC	CPU
All	0180.c200.0002	STATIC	CPU
All	0180.c200.0003	STATIC	CPU
All	0180.c200.0004	STATIC	CPU
All	0180.c200.0005	STATIC	CPU
All	0180.c200.0006	STATIC	CPU
All	0180.c200.0007	STATIC	CPU
All	0180.c200.0008	STATIC	CPU
All	0180.c200.0009	STATIC	CPU
All	0180.c200.000a	STATIC	CPU
All	0180.c200.000b	STATIC	CPU
All	0180.c200.000c	STATIC	CPU
All	0180.c200.000d	STATIC	CPU
All	0180.c200.000e	STATIC	CPU
All	0180.c200.000f	STATIC	CPU
All	0180.c200.0010	STATIC	CPU
All	ffff.ffff.ffff	STATIC	CPU
12	5c26.0a24.6060	DYNAMIC	Fa0/6

Total Mac Addresses for this criterion: 21

Отобразил ли коммутатор MAC-адрес компьютера PC-A? Если вы ответили «да», на каком порте он находился?

CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC Вопросы для повторения

1. Можете ли вы использовать широковещательную рассылку на уровне 2? Если да, то каким будет ее MAC-адрес?

CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC

2. Зачем нужно знать MAC-адрес устройства? CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC

Практическая работа 9: изучение кадров Ethernet с помощью программы Wireshark

Топология

Задачи

Часть 1. Изучение полей заголовков в кадре Ethernet II

Часть 2. Захват и анализ кадров Ethernet с помощью программы Wireshark

Исходные данные/сценарий

При взаимодействии протоколов верхнего уровня данные проходят уровни взаимодействия открытых систем (OSI) и инкапсулируются в кадры уровня 2. Структура кадра зависит от типа доступа к среде передачи данных. Например, если в качестве протоколов верхнего уровня используются TCP и IP, а тип доступа к среде передачи — Ethernet, то инкапсуляция кадров уровня 2 происходит через Ethernet II. Это типично для локальной среды.

При изучении концепций уровня 2 полезно анализировать данные заголовков кадров. В первой части этой лабораторной работы вы сможете посмотреть поля в кадре Ethernet II. Во второй части вам предстоит захватить и проанализировать поля заголовков кадра Ethernet II для локального и удалённого трафика с помощью программы Wireshark.

Необходимые ресурсы

• Один ПК (Windows 7, Vista или XP с выходом в Интернет и установленной программой Wireshark)

Часть 1: Изучение полей заголовков в кадре Ethernet II

В части 1 вы изучите поля и содержание заголовков в кадре Ethernet II. Для этого будет использоваться захват данных программой Wireshark.

Шаг 1: Просмотрите длины и описания полей заголовков Ethernet II.

Преамбула	Адрес назначения	Адрес источника	Тип кадра	Данные	Контрольная последовательность кадра (Frame Check Sequence-FCS)
8 байт	6 байт	6 байт	2 байта	от 46 до 1500 байт	4 байта

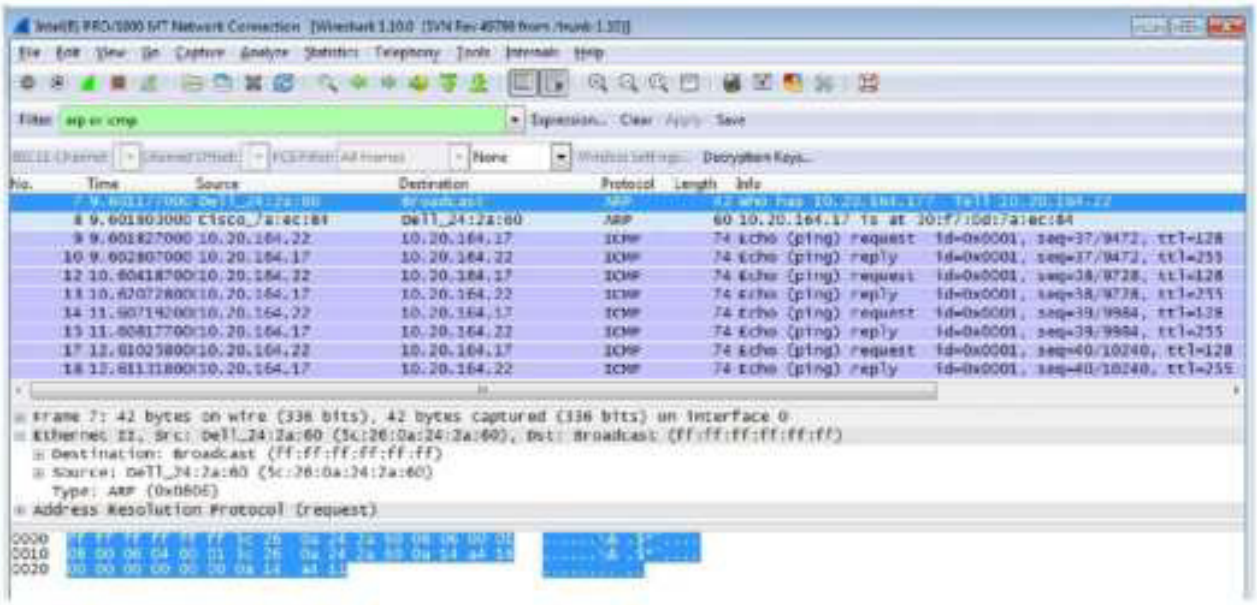
Шаг 2: Изучите конфигурацию сети ПК.

IP-адрес узла ПК — 10.20.164.22, IP-адрес шлюза по умолчанию — 10.20.164.17.

```
Ethernet adapter Подключение по локальной сети:

   DNS-суффикс подключения . . . . . : cisco.com
   Локальный IPv6-адрес канала . . . : fe80::b875:731b:3c7b:c0b1%10
   IPv4-адрес. . . . . . . . . . . . : 10.20.164.22
   Маска подсети . . . . . . . . . . : 255.255.255.240
   Основной шлюз. . . . . . . . . . : 10.20.164.17
```

Шаг 3: Изучите кадры Ethernet в данных, захваченных программой Wireshark.

Показанный ниже результат захвата данных в программе Wireshark отображает пакеты, которые были сгенерированы эхо-запросом узлового ПК, отправленным на шлюз по умолчанию. В программе Wireshark включён фильтр для просмотра только ARP- и ICMP-протоколов. Сеанс начинается с ARP- запроса MAC-адреса маршрутизатора шлюза, за которым следуют четыре эхо-запроса с помощью команды ping и отклика.



Шаг 4: Изучите содержание заголовков Ethernet II в ARP-запросе.

В приведённой ниже таблице выбран первый кадр из данных, захваченных программой Wireshark, и отображаются данные в полях заголовков Ethernet

Поле	Значение	Описание
Преамбула	Не показано в захвате данных	В этом поле содержатся синхронизированные биты, обработанные аппаратным обеспечением сетевого адаптера.
Адрес назначения	Широковещательная рассылка (ff:ff:ff:ff:ff:fl)	Адреса уровня 2 для кадра. Длина каждого адреса составляет 48 бит или 6 октетов, выраженных 12 шестнадцатеричными цифрами, 0-9,A-F. Общий формат — 12:34:56:78:9A:BC.
Адрес источника	Dell 24:2a:60 (5c:26:0a:24:2a:60)	Первые шесть шестнадцатеричных номеров обозначают производителя сетевого адаптера, а последние — серийный номер устройства. Адрес назначения может быть широковещательным (состоящим только из единиц), либо индивидуальным. Адрес источника всегда индивидуальный.
Тип кадра	0x0806	В кадрах Ethernet II это поле содержит шестнадцатеричное значение, которое используется для указания типа протокола верхнего уровня в поле данных. Ethernet II поддерживает множество протоколов верхнего уровня. Наиболее распространены следующие два типа кадров: Значение Описание 0x0800 Протокол IPv4 0x08 06 Протокол разрешения адресов (ARP)
Данные	ARP	Содержит инкапсулированный протокол верхнего уровня. Поле данных в диапазоне от 46 до 1500 байт.
Контрольная последовательность кадра (Frame Check Sequence-FCS)	Не показано в захвате данных	Контрольная последовательность кадра, используемая сетевым адаптером для выявления ошибок при передаче данных. Значение вычисляется компьютером отправителя, включает адреса, тип и поле данных кадра и проверяется получателем.

Какова особенность содержания поля адреса назначения?

Почему перед первым эхо-запросом с помощью команды ping ПК отправляет широковещательную рассылку ARP?

Назовите MAC-адрес источника в первом кадре.

Назовите идентификатор производителя (OUI) сетевого адаптера источника. Какая часть MAC-адреса соответствует OUI?

Назовите серийный номер сетевого адаптера источника.

Часть 2: Захват и анализ кадров Ethernet с помощью программы Wireshark

В части 2 вы воспользуетесь программой Wireshark для захвата локальных и удалённых кадров Ethernet. Затем вы изучите сведения, содержащиеся в полях заголовков кадров.

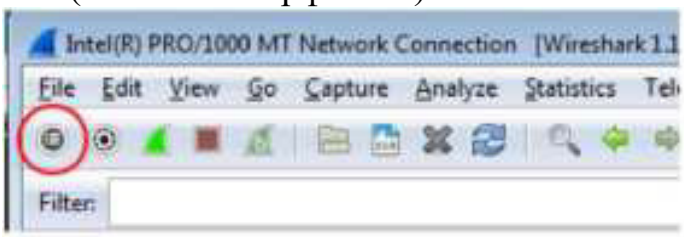
Шаг 1: Определите IP-адрес шлюза по умолчанию на своём ПК.

Откройте окно командной строки и введитеipconfig. Назовите IP-адрес шлюза ПК по умолчанию. ,

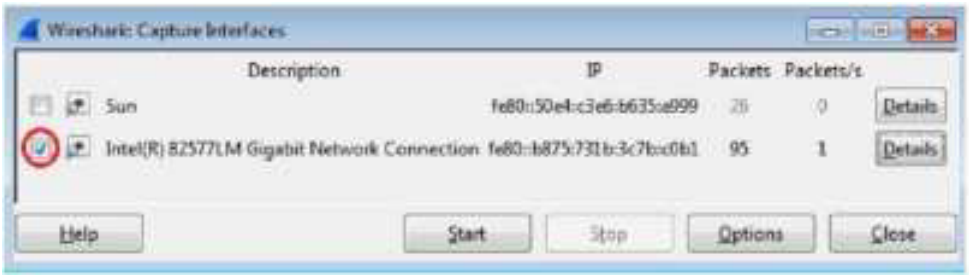
Шаг 2: Начните захват трафика на сетевом адаптере своего ПК.

a. Откройте Wireshark.

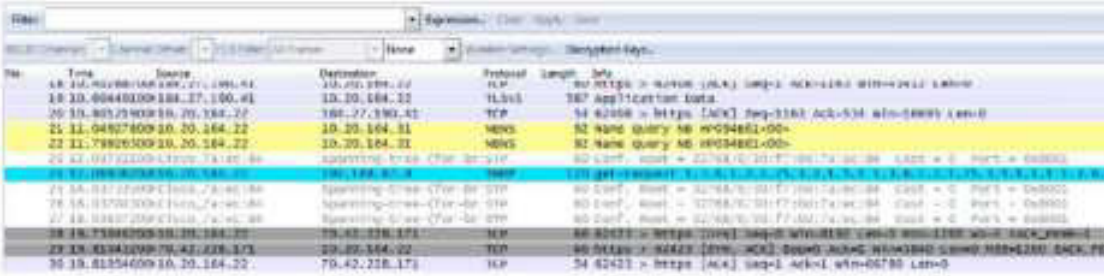
b. На панели инструментов анализатора сети Wireshark нажмите на значок Interface List (Список интерфейсов).



c. В окне Wireshark: Capture Interfaces (Захват интерфейсов) выберите интерфейс, в котором нужно начать захват трафика, установив соответствующий флажок, и нажмите кнопку Start (Пуск). Если вы не знаете, какой интерфейс выбрать, нажмите кнопку Details (Сведения), чтобы открыть подробную информацию о каждом из указанных интерфейсов.



d. Понаблюдайте за трафиком в окне списка пакетов (Packet List).



Шаг 3: С помощью фильтров программы Wireshark отобразите на экране только трафик ICMP.

Чтобы скрыть ненужный трафик, установите соответствующий фильтр Wireshark. Фильтр не блокирует захват ненужных данных, а лишь отбирает то, что нужно показывать на экране. На данный момент разрешено отображение только ICMP-трафика.

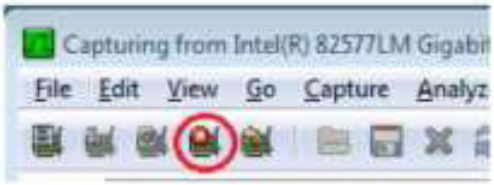
В поле Filter (Фильтр) программы Wireshark введите icmp. При правильной настройке фильтра поле должно стать зелёным. Если поле стало зелёным, нажмите кнопку Apply (Применить), чтобы применить фильтр.

Шаг 4: Из окна командной строки отправьте эхо-запрос с помощью команды ping на шлюз ПК по умолчанию.

Из окна командной строки отправьте эхо-запрос с помощью команды ping на шлюз по умолчанию, используя IP-адрес, записанный в шаге 1.

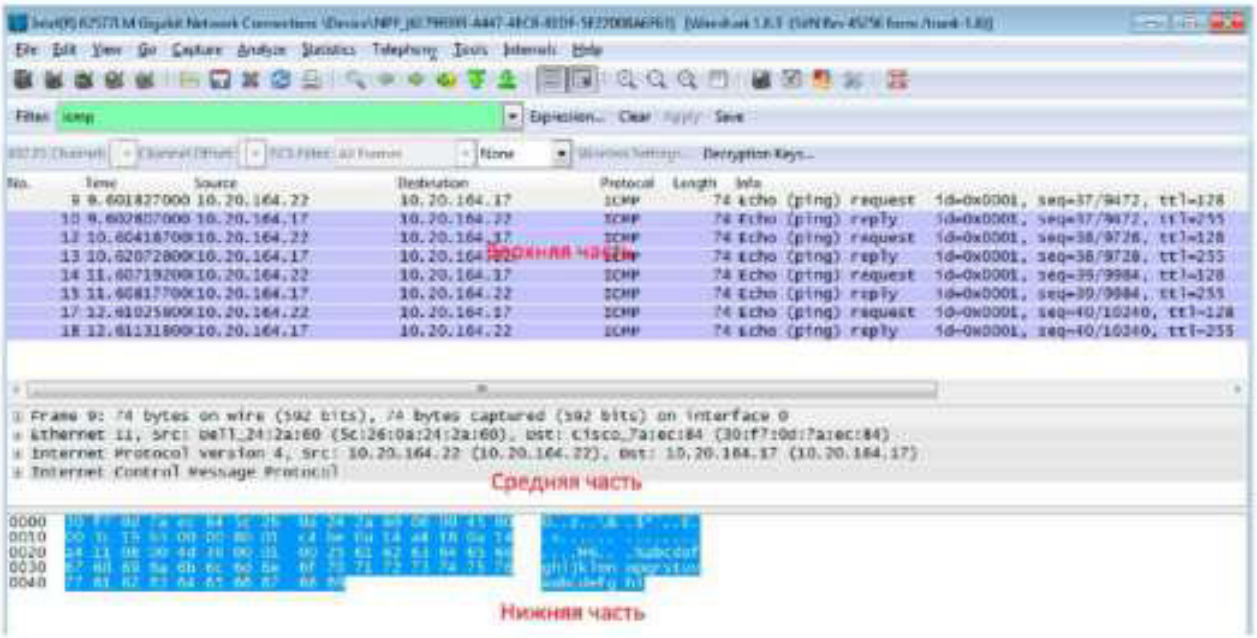
Шаг 5: Остановите захват трафика на сетевом адаптере.

Чтобы остановить захват трафика, нажмите на значок Stop Capture (Остановить захват).



Шаг 6: Изучите первый эхо-запрос с помощью команды ping в программе Wireshark.

Главное окно программы Wireshark состоит из трёх разделов: панель списка пакетов (вверху), панель сведений о пакете (посередине) и панель отображения пакета в виде последовательности байтов (внизу). Если вы правильно выбрали интерфейс для захвата пакетов в шаге 3, программа Wireshark отобразит данные протокола ICMP на панели списка пакетов, как показано в приведённом ниже примере.



a. На панели списка пакетов (верхний раздел) выберите первый указанный кадр. В столбце Info (Информация) появится значение Echo (ping) request (эхо-запрос с помощью команды ping). Строка станет синей.

b. Изучите первую строку в панели сведений о пакете в средней части экрана. В этой строке указывается длина кадра (в данном примере — 74 байта).

c. Вторая строка в панели Packet Details (Сведения о пакете) показывает, что это кадр Ethernet II. Также отображаются MAC-адреса источника и назначения.

Назовите MAC-адрес сетевого адаптера этого ПК.

Назовите MAC-адрес шлюза по умолчанию.

d. Чтобы получить больше информации о кадре Ethernet II, нажмите на значок плюса («+») в начале второй строки. Обратите внимание на то, что значок плюса при этом изменится на значок минуса («-»).

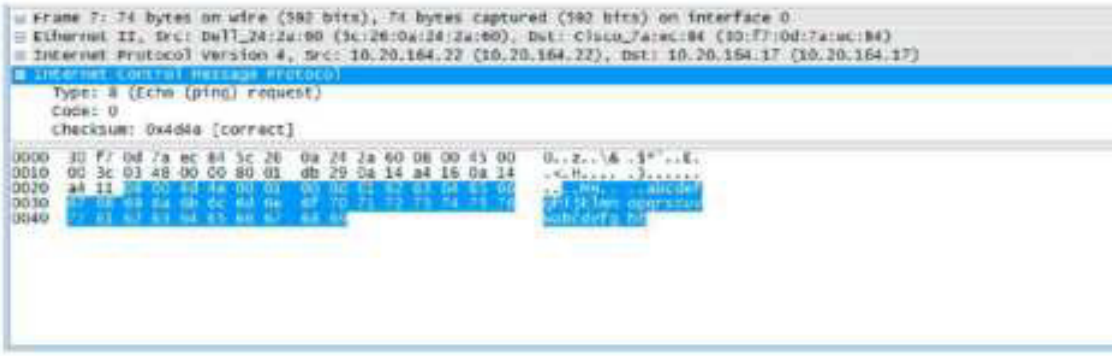
Назовите показанный тип кадра.

e. Последние две строки среднего раздела содержат информацию о поле данных кадра. Обратите внимание на то, что данные содержат ^4-адреса источника и назначения.

Назовите IP-адрес источника.

Назовите IP-адрес назначения.

f. Чтобы выделить эту часть кадра (в шестнадцатеричной системе и ASCII) в панели отображения пакета в виде последовательности байтов (нижний раздел) нажмите на любую строку в среднем разделе. Нажмите на строку Internet Control Message Protocol в среднем разделе и посмотрите, что будет выделено в панели отображения пакета в виде последовательности байтов.



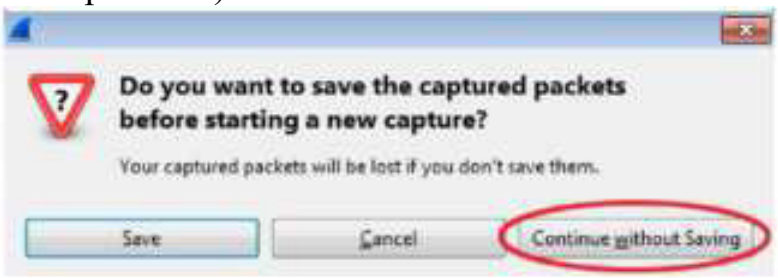
Какое слово образуют последние два выделенных октета?

g. Нажмите на следующий кадр в верхнем разделе и изучите кадр эхо-ответа. Обратите внимание на то, что MAC-адреса источника и назначения поменялись местами, поскольку маршрутизатор, который служит шлюзом по умолчанию, отправил этот кадр в ответ на первый эхо-запрос с помощью команды ping.

Какое устройство и MAC-адрес отображаются в качестве адреса назначения?

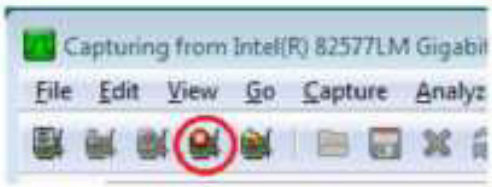
Шаг 7: Перезапустите захват пакетов в программе Wireshark.

Нажмите на значок Start Capture (Начать захват), чтобы начать новый захват данных в программе Wireshark. Откроется всплывающее окно с предложением сохранить предыдущие захваченные пакеты в файл перед началом нового захвата. Нажмите кнопку Continue without Saving (Продолжить без сохранения).



Шаг 8: Через окно командной строки отправьте эхо-запрос с помощью команды ping на веб-сайт www.cisco.com.

Шаг 9: Остановите захват пакетов.



Шаг 10: Изучите новые данные на панели списка пакетов в программе Wireshark.

Назовите MAC-адреса источника и назначения в первом кадре эхо-запроса с помощью команды ping.

Источник:

Назначение:

Назовите IP-адреса источника и назначения в поле данных кадра.

Источник:

Назначение:

Сравните эти адреса с адресами, полученными в шаге 7. Изменился только IP-адрес назначения. Почему IP-адрес назначения изменился, а MAC-адрес назначения остался прежним?

Вопросы на закрепление

Программа Wireshark не отображает поле преамбулы заголовка кадра. Что содержит преамбула?

Практическая работа 10: просмотр ARP с помощью интерфейса командной строки Windows, интерфейса командной строки IOS и Wireshark

Топология

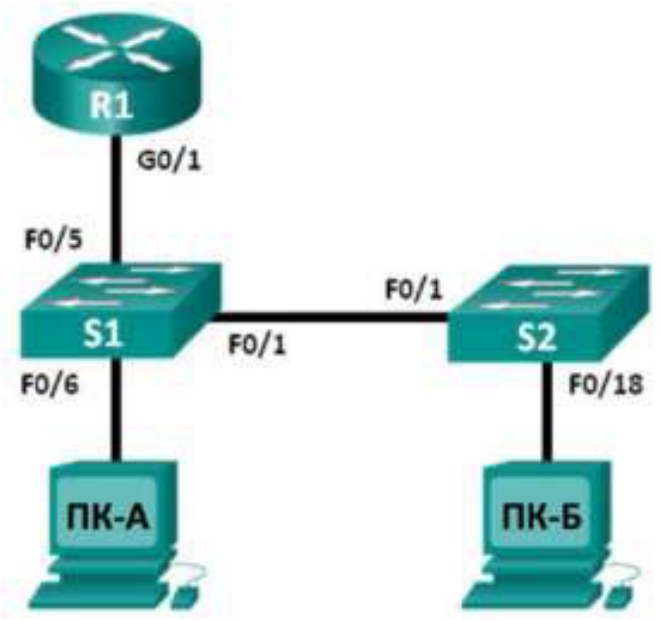


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1	192.168.1.1	255.255.255.0	Недоступно
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
S2	VLAN 1	192.168.1.12	255.255.255.0	192.168.1.1
ПК-А	Сетевой адаптер	192.168.1.3	255.255.255.0	192.168.1.1
ПК-Б	Сетевой адаптер	192.168.1.2	255.255.255.0	192.168.1.1

Задачи

Часть 1. Создание и настройка сети

Часть 2. Использование команды ARP в ОС Windows

Часть 3. Использование команды show arp в IOS

Часть 4. Анализ обмена сообщениями ARP с помощью программы Wireshark

Исходные данные/сценарий

Протокол разрешения адресов (ARP) используется протоколом TCP/IP для сопоставления IP-адреса уровня 3 с MAC-адресом уровня 2. Когда кадр помещается в сеть, он должен содержать MAC-адрес

назначения. Для динамического определения MAC-адреса устройства назначения по локальной сети отправляется широковещательный запрос ARP. Устройство, которое содержит IP-адрес назначения, отвечает, и MAC-адрес записывается в ARP-кэш. Каждое устройство в локальной сети имеет собственный ARP-кэш или небольшой участок в ОЗУ, где хранятся результаты ARP. Таймер ARP-кэша удаляет ARP-записи, которые не использовались в течение определённого периода времени.

ARP — яркий пример компромисса производительности. При отсутствии кэша протокол ARP должен непрерывно запрашивать трансляцию адресов каждый раз при помещении кадра в сеть. В этом случае для установления связи прибавляется время ожидания, что может вызвать перегрузку локальной сети. И наоборот, неограниченное время ожидания может привести к ошибкам устройств, которые покидают сеть или меняют адрес уровня 3.

Администратор сети должен знать о протоколе ARP, даже если не может с ним взаимодействовать на регулярной основе. ARP — это протокол, который позволяет сетевым устройствам обмениваться данными с протоколом TCP/IP. Без него невозможно эффективно построить датаграмму для адреса назначения уровня 2. Кроме того, ARP может создавать риски для безопасности. Хакеры используют ARP-спуфинг, или «отравление» ARP-кэша, для внедрения в сети неверных MAC-адресов. Злоумышленник генерирует ложный MAC-адрес устройства, в результате чего кадры передаются на неверный адрес назначения. Ручная конфигурация статических связей ARP — это один из способов предотвращения атак на основе протокола ARP. И, наконец, для предотвращения несанкционированного доступа к сети на устройствах Cisco можно настроить список авторизированных MAC-адресов.

В данной лабораторной работе вам предстоит открыть таблицу ARP с помощью команд ARP в маршрутизаторах Windows и Cisco. Кроме того, вы очистите ARP-кэш и добавите статические записи ARP.

Примечание. Маршрутизаторы, используемые на практических занятиях CCNA: маршрутизаторы с интеграцией сервисов серии Cisco 1941 (ISR) установленной версии Cisco IOS 15.2(4) M3 (образ universalk9). Используемые коммутаторы: семейство коммутаторов Cisco Catalyst 2960 версии CISCO IOS 15.0(2) (образ lanbasek9). Можно использовать другие маршрутизаторы, коммутаторы и версии CISCO IOS. В зависимости от модели и версии Cisco IOS выполняемые доступные команды и выводы могут отличаться от данных, полученных в ходе лабораторных работ. Точные идентификаторы интерфейса см. в таблице сводной информации об интерфейсах маршрутизаторов в конце данной лабораторной работы.

Примечание. Убедитесь, что информация, имеющаяся на маршрутизаторе и коммутаторе, удалена и они не содержат файлов загрузочной конфигурации. Если вы не уверены, что сможете это сделать, обратитесь к инструктору.

Необходимые ресурсы

- 1 маршрутизатор (Cisco 1941 с универсальным образом M3 версии CISCO IOS 15.2(4) или аналогичным)
- 2 коммутатора (Cisco 2960, ПО CISCO IOS версии 15.0(2), образ lanbasek9 или аналогичный)
- Два ПК (Windows 7, Vista или XP с установленным эмулятором терминала, например Tera Term, и программой Wireshark)
- Консольные кабели для настройки устройств CISCO IOS через консольные порты
- Кабели Ethernet в соответствии с топологией

Примечание. Интерфейсы Fast Ethernet на коммутаторах Cisco 2960 определяют тип подключения автоматически, поэтому между коммутаторами S1 и S2 можно использовать прямой кабель Ethernet. При использовании коммутатора Cisco другой модели может потребоваться кроссовый кабель Ethernet.

Часть 1: Создание и настройка сети

Шаг 1: Подключите сеть в соответствии с топологией.

Шаг 2: Настройте IP-адреса устройств в соответствии с таблицей адресации.

Шаг 3: Проверьте подключение к сети, отправив с ПК-Б эхо-запросы с помощью команды ping на все устройства.

Часть 2: Использование команды ARP в ОС Windows

Команда arp позволяет пользователю просматривать и изменять ARP-кэш в ОС Windows. Команда вводится в командную строку Windows.

Шаг 1: Отобразите ARP-кэш.

a. Откройте окно командной строки на ПК-А и введите arp.

```
C:\Documents and Settings\User1> arp

Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

ARP -a [inet_addr] [-N if_addr]
ARP -d inet_addr [if_addr]
ARP -s inet_addr eth_addr [if_addr]

  -a            Displays current ARP entries by interrogating the current
                protocol data.  If inet_addr is specified, the IP and Physical
                addresses for only the specified computer are displayed.  If
                more than one network interface uses ARP, entries for each ARP
                table are displayed.
  -g            Same as -a.
  -v            Displays current ARP entries in verbose mode.  All invalid
                entries and entries on the loop-back interface will be shown.
  inet_addr     Specifies an internet address.
  -N if_addr    Displays the ARP entries for the network interface specified
                by if_addr.
  -d            Deletes the host specified by inet_addr. inet_addr may be
                wildcarded with * to delete all hosts.
  -s            Adds the host and associates the Internet address inet_addr
                with the Physical address eth_addr.  The Physical address is
                given as 6 hexadecimal bytes separated by hyphens. The entry
                is permanent.
  eth_addr      Specifies a physical address.
  if_addr       If present, this specifies the Internet address of the
                interface whose address translation table should be modified.
                If not present, the first applicable interface will be used.
Example:
  > arp -s 157.55.85.212   00-aa-00-62-c6-09  .... Adds a static entry.
```

b. Изучите выходные данные.

Какая команда позволяет от

```
C:\Documents and Settings\User1> ping 192.168.1.2

Interface: 192.168.1.3 --- 0xb
  Internet Address      Physical Address      Type
  192.168.1.2           00-50-56-be-f6-db     dynamic
```

образить все записи в ARP-кэше?

Какая команда позволяет удалить все записи в ARP-кэше (очистить ARP-кэш)?

Какая команда позволяет удалить все записи в ARP-кэше для 192.168.1.11?

Шаг 2: Настройте записи в ARP-кэш вручную.

Чтобы удалить записи из ARP-кэша, выполните команду arp -d {inet-addr | *}. Можно удалить адреса по отдельности, указав соответствующие IP-адреса, либо стереть сразу все записи с помощью подстановочного символа *.

Убедитесь в том, что ARP-кэш содержит следующие записи: шлюз по умолчанию R1 G0/1 (192.168.1.1), ПК-Б (192.168.1.2) и оба коммутатора (192.168.1.11 и 192.168.1.12).

a. С ПК-А отправьте эхо-запросы с помощью команды ping на все адреса в таблице адресов.

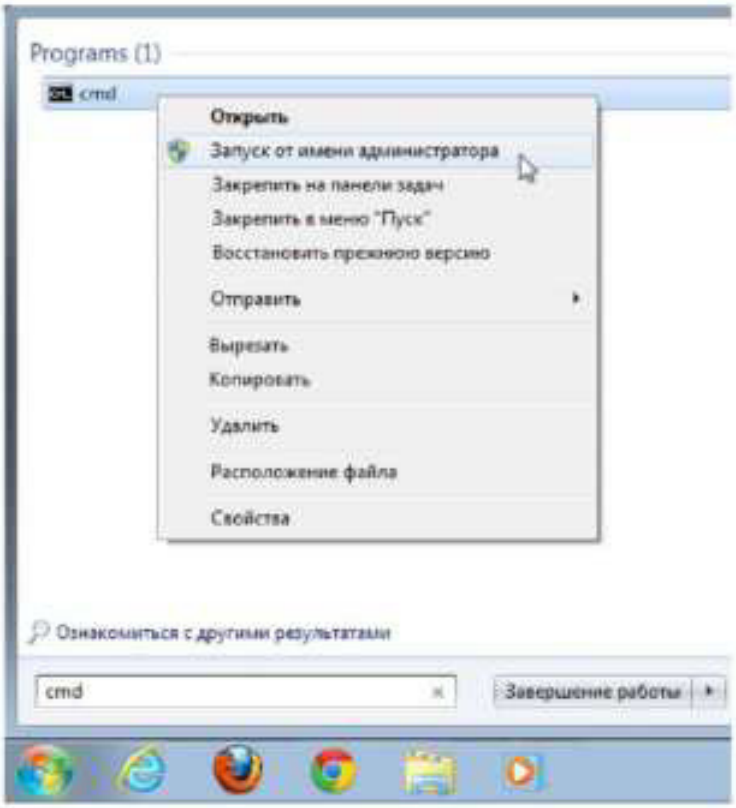
b. Убедитесь в том, что все адреса добавлены в ARP-кэш. Если адрес в ARP-кэше отсутствует, отправьте эхо-запрос с помощью команды ping на адрес назначения и проверьте, добавлен ли адрес в ARP-кэш.

```
C:\Users\User1> arp -a

Interface: 192.168.1.3 --- 0xb
  Internet Address      Physical Address      Type
  192.168.1.1           d4-8c-b5-ce-a0-c1     dynamic
```

```
                1.2                                  dy
92, 1 8         0-    5  56 be f6 b    namic
  6 .                 0- -  -  -
                1.1                                  dy
92, 1 8 1       c-    d  96 8- 8a 0    namic
  6 .                 9- -     -
                1.1                                  dy
92. 1 8 2       c-    d  96 2- 40 0    namic
  6 .                 9- -     -
                1.2                                  sta
92. 1 8 55      f-    f  ff- f- f- f   tic
  6 .
                22                                   sta
24. 0 .         1-    0  5e 0- 0- 6    tic
  .                     -
                252                                  sta
24. 0 .         1-    0  5e 0- 0- c    tic
  .                     -
                255                                  sta
39. 25  .250    1-    0  5e 7f f- a    tic
  5.                    -  -
```

c. Откройте командную строку от имени администратора. Нажмите кнопку Пуск и в поле *Найти программы и файлы* введите команду cmd. Когда появится значок cmd, нажмите на него правой кнопкой мыши и выберите параметр Запуск от имени администратора. Нажмите кнопку Да, чтобы разрешить этой программе вносить изменения.

Примечание. Пользователям Windows XP для изменения записей в ARP-кэше права администратора не требуются.



d. В окне командной строки администратора введите arp -d *. Эта команда удалит все записи из ARP-кэша. Убедитесь в том, что все записи из ARP-кэша удалены. Для этого в командной строке введите arp -a.

C:\windows\system32> arp -d * C:\windows\system32> arp -a No ARP Entries Found.

e. Подождите несколько минут. Протокол обнаружения соседей снова начинает заполнять ARP-кэш.

C:\Users\User1> arp -a

Interface: 192.168.1.3 -- 0xb

```
Internet Address      Physical Address      Type
192.168.1.255         ff-ff-ff-ff-ff-ff     static
```

Примечание. В Windows XP протокол обнаружения соседей не работает.

f. С ПК-А отправьте эхо-запрос с помощью команды ping на ПК-Б (192.168.1.2) и коммутаторы (192.168.1.11 и 192.168.1.12), чтобы добавить записи ARP. Убедитесь в том, что все записи ARP добавлены в ARP-кэш.

C:\Users\User1> arp -a

```
Interface: 192.168.1.3 --- 0xb
  Internet Address      Physical Address      Type
  192.168.1.2           00-50-56-be-f6-db     dynamic
  192.168.1.11          0c-d9-96-e8-8a-40     dynamic
  192.168.1.12          0c-d9-96-d2-40-40     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
```

g. Запишите физический адрес коммутатора S2.

h. Чтобы удалить отдельную запись ADR, введите команду arp- d *inet-addr*. Чтобы удалить запись ARP для коммутатора S2, в командной строке введите arp -d 192.168.1.12.

C:\windows\system32> arp -d 192.168.1.12

i. Чтобы проверить, удалена ли запись ARP для коммутатора S2 из ARP-кэша, введите arp -a.

C:\Users\User1> arp -a

```
Interface: 192.168.1.3 --- 0xb
  Internet Address      Physical Address      Type
  192.168.1.2           00-50-56-be-f6-db     dynamic
  192.168.1.11          0c-d9-96-e8-8a-40     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
```

j. Для добавления отдельной записи ARP введите команду arp -s inet_addr mac_addr. В данном примере будут использоваться IP- и MAC-адреса для коммутатора S2. Используйте MAC-адрес, записанный в шаге g.

C:\windows\system32> arp -s 192.168.1.12 0c-d9-96-d2-40-40 k. Запись ARP для коммутатора S2 должна добавиться в кэш.

Часть 3: Использование команды show arp в IOS

В Cisco IOS ARP-кэш маршрутизаторов и коммутаторов можно также отображать с помощью команд show arp или show ip arp.

Шаг 1: Отобразите записи ARP на маршрутизаторе R1.

```
R1# show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.1.1            -    d48c.b5ce.a0c1  ARPA   GigabitEthernet0/1
Internet  192.168.1.2            0    0050.56be.f6db  ARPA   GigabitEthernet0/1
Internet  192.168.1.3            0    0050.56be.768c  ARPA   GigabitEthernet0/1
R1#
```

Обратите внимание на то, что первая запись интерфейса маршрутизатора G0/1 (шлюз по умолчанию для локальной сети) не имеет срока жизни. Срок жизни — это количество минут (мин), на протяжении которых запись содержалась в ARP-кэше. Для других записей это значение увеличивается. Протокол обнаружения соседей заполняет записи IP- и MAC-адресов на ПК-А и ПК-Б.

Шаг 2: Добавьте записи ARP на маршрутизатор R1.

Записи ARP можно добавлять в ARP-таблицу маршрутизатора, отправляя эхо-запросы с помощью команды ping на другие устройства.

a. Отправьте эхо-запрос с помощью команды ping с помощью команды ping на коммутатор S1.

b. Убедитесь в том, что запись ARP для коммутатора S2 добавлена в таблицу ARP коммутатора S1.

```
R1# ping 192.168.1.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.11, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/2/4 ms
```

b. Убедитесь в том, что запись ARP для коммутатора S1 добавлена в таблицу ARP маршрутизатора R1.

```
R1# show ip arp
Pr        A                Age        Hardwar                Interface
otocol    ddress           (min)      e Addr          ype
In        1                -          d48c.b5                GigabitEthe
ternet    92.168. 1                   ce.a0c1         RPA    rnet0/1
                  .
In        1                6          0050.56                GigabitEthe
ternet    92.168. .                   be.f6db         RPA    rnet0/1
In        1                6          0050.56                GigabitEthe
ternet    92.168. .  3                be.768c         RPA    rnet0/1
In        1                0          0cd9.96                GigabitEthe
ternet    92.168. .  1                e8.8a40         RPA    rnet0/1
R1#
```

Шаг 3: Отобразите записи ARP на коммутаторе S1.

```
S1# show ip arp
Protocol Addres          Age (min)  Hardware       Type  Interface
         s                           Addr
Internet 192.16  1 1     46         d48c.b5ce.a0c  ARP   Vlan1
         8.      .                   1              A
Internet 192.16  1 2     8          0050.56be.f6d  ARP   Vlan1
         8.      .                   b              A
Internet 192.16  1 3     8          0050.56be.768  ARP   Vlan1
         8.      .                   c              A
Internet 192.16  1 11    -          0cd9.96e8.8a4  ARP   Vlan1
         8.      .                   0              A
S1#
```

Шаг 4: Добавьте записи ARP на коммутаторе S1.

Записи ARP можно также добавлять в ARP-таблицу коммутатора, отправляя эхо-запросы с помощью команды ping на другие устройства.

a. С коммутатора S1 отправьте эхо-запрос с помощью команды ping на коммутатор S2.

```
Internet  192.168.1.2        11   0050.56be.f6db  ARPA   Vlan1
Internet  192.168.1.3        11   0050.56be.768c  ARPA   Vlan1
Internet  192.168.1.11        -   0cd9.96e8.8a40  ARPA   Vlan1
Internet  192.168.1.12        2   0cd9.96d2.4040  ARPA   Vlan1
S1#
```

Часть 4: Анализ обмена сообщениями ARP с помощью программы Wireshark

В части 4 вам предстоит изучить обмен сообщениями ARP, используя программу Wireshark для их захвата и оценки. Кроме того, вы проанализируете задержки сети, вызванные обменом сообщениями ARP между устройствами.

Шаг 1: Настройте программу Wireshark для захвата пакетов.

a. Запустите программу Wireshark.

b. Выберите сетевой интерфейс, который будете использовать для захвата сообщений ARP.

Шаг 2: Захватите и оцените сообщения ARP.

a. Начните захват пакетов в программе Wireshark. С помощью фильтра отобразите только пакеты ARP.

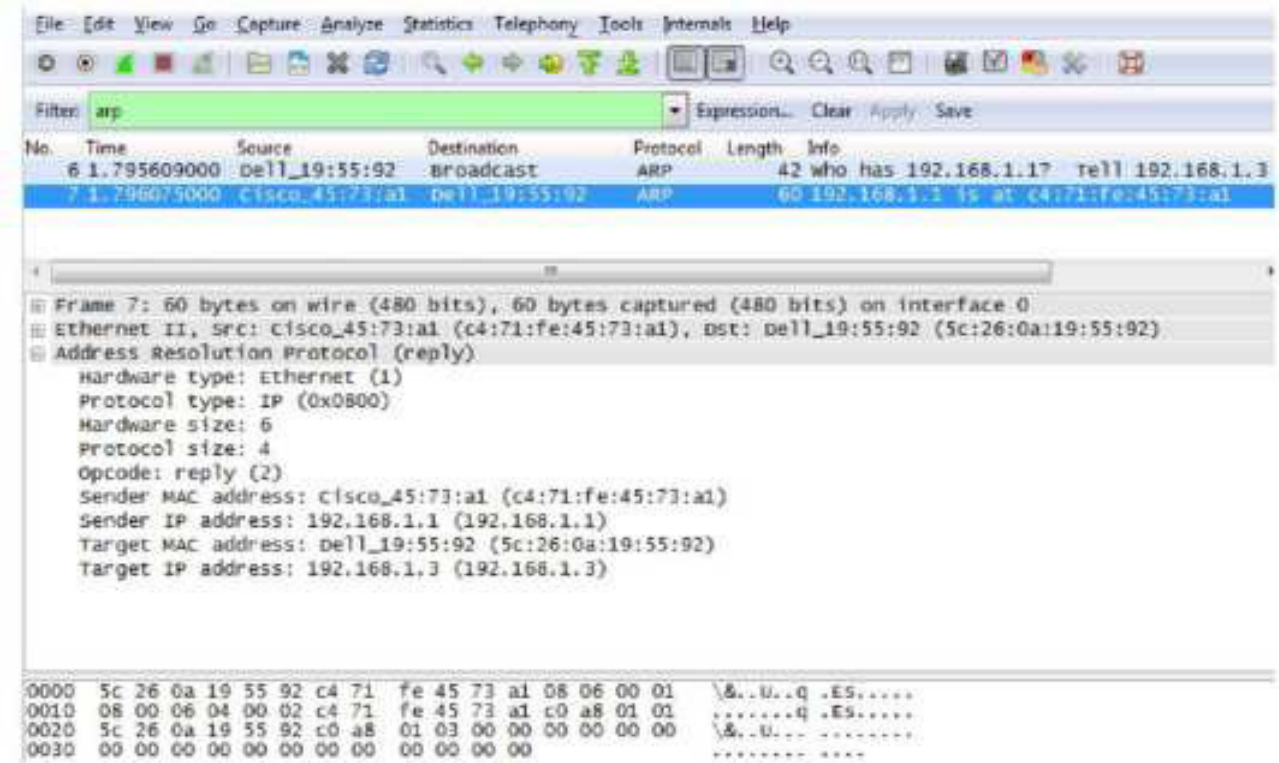
b. Очистите ARP-кэш, набрав в командной строке команду arp -d *.

c. Убедитесь в том, что ARP-кэш очищен.

d. Отправьте эхо-запрос с помощью команды ping на шлюз по умолчанию с помощью команды ping 192.168.1.1.

e. После отправки эхо-запроса на шлюз по умолчанию остановите захват данных программой Wireshark.

f. В захваченных данных найдите сообщения ARP в панели сведений о пакетах. Какой пакет ARP был первым?



Заполните приведённую ниже таблицу данными второго захваченного пакета ARP.

Поле	Значение
MAC-адрес отправителя	
IP-адрес отправителя	
MAC-адрес назначения	
IP-адрес назначения	

Шаг 3: Проанализируйте задержки сети, вызванные ARP.

a. Очистите записи ARP на ПК-А.

b. Начните захват данных программой Wireshark.

c. Отправьте эхо-запрос с помощью команды ping на коммутатор S2 (192.168.1.12). Эхо-запрос с помощью команды ping, отправленный после первого эхо-запроса, должен быть успешным.

Примечание. Если все эхо-запросы успешны, необходимо перезагрузить коммутатор S1, чтобы просмотреть задержки сети из-за ARP.

```
C:\Users\User1> ping 192.168.1.12
Request timed out.
Reply from 192.168.1.12: bytes=32 time=2ms TTL=255
Reply from 192.168.1.12: bytes=32 time=2ms TTL=255
Reply from 192.168.1.12: bytes=32 time=2ms TTL=255

Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),


Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 3ms, Average = 2ms
```

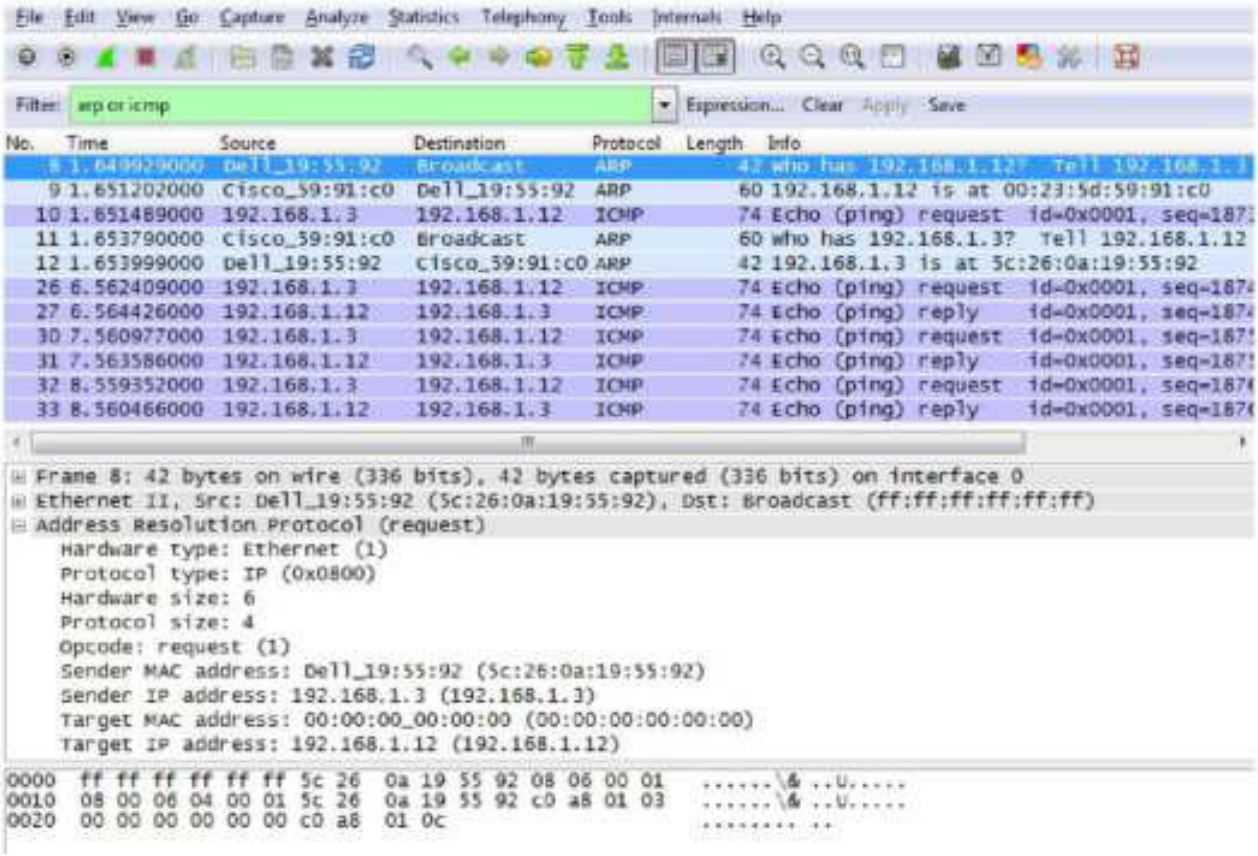
d. После отправления эхо-запросов с помощью команды ping остановите захват данных программой Wireshark. С помощью фильтра отобразите только данные ARP и ICMP. В поле Filter: (Фильтр) программы Wireshark введите arp или icmp.

e. Изучите захваченные данные. В данном примере кадр 10 — это первый ICMP-кадр, отправленный с ПК-Б на коммутатор S1. Поскольку для коммутатора S1 нет записи ARP, на IP-адрес управления коммутатора S1 был отправлен ARP-запрос на получение MAC-адреса. В процессе обмена данными ARP эхо-запрос с помощью команды ping не получил отклик за отведённое время (кадры 8-12).

После добавления записи ARP для коммутатора S1 в ARP-кэш последние три обмена данными ICMP были успешны, о чем свидетельствуют кадры 26, 27 и 30-33.

Как показано в захвате данных Wireshark, ARP — это яркий пример компромисса производительности. При отсутствии кэша протокол ARP

должен непрерывно запрашивать трансляцию адресов каждый раз при помещении кадра в сеть. В этом случае для установления связи прибавляется время ожидания, что может вызвать перегрузку локальной сети.



Вопросы на закрепление

1. Как и когда удаляются статические записи ARP?
2. Зачем добавить статические записи ARP в кэш?

3. Если ARP-запросы способны вызывать задержки сети, почему не рекомендуется снимать ограничения на время ожидания отклика для записей ARP?

Сводная таблица интерфейса маршрутизатора

Общие сведения об интерфейсах маршрутизаторов				
Модель маршрутизатора	Интерфейс Ethernet #1	Интерфейс Ethernet #2	Последовательный интерфейс #1	Последовательный интерфейс #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы для определения типа маршрутизатора и количества имеющихся на нём интерфейсов. Не существует эффективного способа перечислить все комбинации настроек для каждого класса маршрутизаторов. Эта таблица включает в себя идентификаторы возможных сочетаний Ethernet и последовательных интерфейсов в устройстве. В таблицу интерфейсов не включены иные типы интерфейсов, даже если они присутствуют на каком-либо определённом маршрутизаторе. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое может использоваться в командах IOS для представления интерфейса.				

Практическая работа 11. Просмотр таблицы MAC-адресов коммутатора

Топология

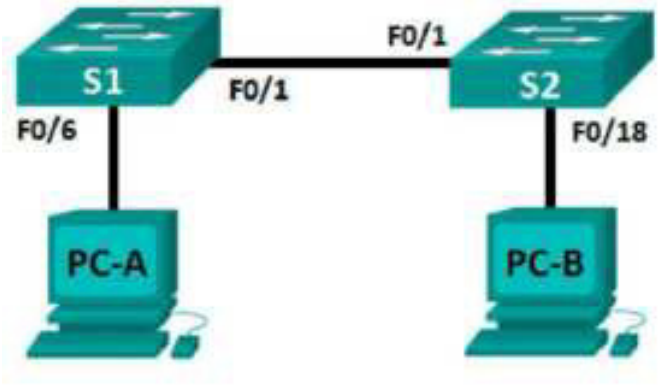


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
S 1	VLAN 1	192.168.1.11	255.255.255.0	—
S 2	VLAN 1	192.168.1.12	255.255.255.0	—
PC- A	NIC	192.168.1.3	255.255.255.0	—
PC- B	NIC	192.168.1.2	255.255.255.0	—

Задачи

Часть 1. Создание и настройка сети

Часть 2. Изучение таблицы MAC-адресов коммутатора

Общие сведения/сценарий

Коммутатор локальной сети на уровне 2 предназначен для доставки кадров Ethernet всем узловым устройствам в локальной сети (LAN). Он записывает MAC-адреса узлов, отображаемые в сети, и сопоставляет их с собственными портами коммутатора Ethernet. Этот процесс называется созданием таблицы MAC-адресов. Получив кадр от ПК, коммутатор изучает MAC-адреса источника и назначения кадра. MAC-адрес источника регистрируется и сопоставляется с портом коммутатора, от которого он был получен. Затем по таблице MAC-адресов определяется MAC-адрес назначения. Если MAC-адрес назначения известен, кадр пересылается через соответствующий порт коммутатора, связанный с этим MAC-адресом. Если MAC-адрес неизвестен, то кадр рассылается через все порты коммутатора, кроме того, через который он был получен. Важно видеть и понимать работу коммутатора и то, как он осуществляет передачу данных по сети. Понимание функционала коммутатора особенно важно для сетевых

администраторов, задача которых заключается в обеспечении безопасной и стабильной работы сети.

Коммутаторы используются для соединения компьютеров в локальных сетях (LAN) и передачи данных между ними. Коммутаторы отправляют кадры Ethernet на узловые устройства, которые идентифицируются по MAC-адресам сетевых плат.В части 1 вам нужно построить топологию, состоящую из двух коммутаторов, соединенных транком. В части 2 вам предстоит отправить эхо-запросы различным устройствам и посмотреть, как два коммутатора строят свои таблицы MAC-адресов.

Примечание. Используются коммутаторы Cisco Catalyst 2960s с Cisco IOS версии 15.0(2) (образ lanbasek9). Допускается использование других моделей коммутаторов и других версий Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и результаты их выполнения могут отличаться от тех, которые показаны в лабораторных работах.

Примечание. Убедитесь, что все настройки коммутатора удалены и загрузочная конфигурация отсутствует. Если вы не уверены в этом, обратитесь к инструктору.

Необходимые ресурсы

- 2 коммутатора (Cisco 2960 с операционной системой Cisco IOS 15.0(2) (образ lanbasek9) или аналогичная модель)
- 2 ПК (Windows 7 или 8 с программой эмуляции терминала, например, Tera Term)
- Консольные кабели для настройки устройств Cisco IOS через консольные порты
- Кабели Ethernet, расположенные в соответствии с топологией

Примечание. Интерфейсы Fast Ethernet на коммутаторах Cisco 2960 определяют тип подключения автоматически, поэтому между коммутаторами S1 и S2 можно использовать прямой кабель Ethernet. При использовании коммутатора Cisco другой модели может потребоваться перекрестный кабель Ethernet.

Часть 1: Создание и настройка сети

Шаг 1: Подключите сеть в соответствии с топологией. Шаг 2: Настройте узлы ПК.

Шаг 3: Выполните инициализацию и перезагрузите коммутаторы, если требуется.

Шаг 4: Настройте базовые параметры каждого коммутатора.

a. Настройте имена устройств в соответствии с топологией.
b. Настройте IP-адреса, как указано в таблице адресации.
c. Назначьте cisco в качестве паролей консоли и VTY.
d. Назначьте class в качестве пароля привилегированного режима EXEC.

Часть 2: Изучение таблицы MAC-адресов коммутатора

Как только между сетевыми устройствами начинается передача данных, коммутатор выясняет MAC- адреса и строит таблицу.

Шаг 1: Запишите MAC-адреса сетевых устройств.

a. Откройте командную строку на PC-A и PC-B и введите команду ipconfig /all. Назовите физические адреса адаптера Ethernet.

MAC-адрес компьютера PC-A:

00-01-97-C5-02-A6

MAC-адрес компьютера PC-B: 00-05-5E-58-AD-A1

b. Подключитесь к коммутаторам S1 и S2 через консоль и введите команду show interface F0/1 на каждом коммутаторе. Назовите адреса оборудования во второй строке выходных данных команды (или зашитый адрес — bia).

MAC-адрес коммутатора S1 Fast Ethernet 0/1: 00-02--0-80-27-0-

MAC-адрес коммутатора S2 Fast Ethernet 0/1: 0000000000000000000000000000000000000000000000000000

Шаг 2: Просмотрите таблицу MAC-адресов коммутатора.

Подключитесь к коммутатору S2 через консоль и просмотрите таблицу MAC-адресов до и после тестирования сетевой связи с помощью эхо-запросов.

a. Подключитесь к коммутатору S2 через консоль и войдите в привилегированный режим EXEC.

b. В привилегированном режиме EXEC введите команду show mac address-table и нажмите клавишу ввода.

S2# show mac address-table

Даже если сетевая коммуникация в сети не происходила (т. е. если команда ping не отправлялась), коммутатор может узнать MAC-адреса при подключении к ПК и другим коммутаторам.

Записаны ли в таблице MAC-адресов какие-либо MAC-адреса?

0000000000000000000000000000000000000000000000000000000000000000000000000000 Какие MAC-адреса записаны в таблице? С какими портами коммутатора они сопоставлены и каким устройствам принадлежат? Игнорируйте MAC-адреса, сопоставленные с центральным процессором.

0000000000000000000000000000000000000000000000000000000000000000000000000000

Если вы не записали MAC-адреса сетевых устройств в шаге 1, как можно определить, каким устройствам принадлежат MAC-адреса, используя только выходные данные команды show mac address-table? Работает ли это решение в любой ситуации?

0000000000000000000000000000000000000000000000000000000000000000000000000000

Шаг 3: Очистите таблицу MAC-адресов коммутатора S2 и снова отобразите таблицу MAC-адресов.

a. В привилегированном режиме EXEC введите команду clear mac address-table dynamic и нажмите клавишу Enter.

```
S2# clear mac address-table dynamic
```

b. Снова быстро введите команду show mac address-table. Указаны ли в таблице MAC-адресов адреса для VLAN 1? Указаны ли другие MAC-адреса?

Через 10 секунд введите команду show mac address-table и нажмите клавишу ввода. Появились ли в таблице MAC-адресов новые адреса? Th^is^olCMAT ^{a}ddressshowing^{a}g^{a}in.

Шаг 4: С компьютера PC-B отправьте эхо-запросы устройствам в сети и просмотрите таблицу MAC-адресов коммутатора.

a. На компьютере PC-B откройте командную строку и введите arp -a. Не считая адресов многоадресной и широковещательной рассылки, сколько пар IP- и MAC-адресов устройств было получено через протокол ARP?

3p^{a}irs:fore^{a}chdevice innetwork withoutPC-B

b. Из командной строки PC-B отправьте эхо-запросы на компьютер PC-A, а также коммутаторы S1 и

S2. От всех ли устройств получены ответы? Если нет, проверьте кабели и IP-конфигурации.
i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i
i i i i i i i i i i i i i i i i i i i i i i i

c. Подключившись через консоль к коммутатору S2, введите команду show mac address-table. Добавил ли коммутатор в таблицу MAC-адресов дополнительные MAC-адреса? Если да, то какие адреса и устройства?

i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i
i i i i i i i i i i i i i i i i i i i i i i i i i i i i

На компьютере PC-B откройте командную строку и еще раз введите команду arp -a. Появились ли в ARP-кэше компьютера PC-B дополнительные записи для всех сетевых устройств, которым были

отправлены эхо-запросы?
i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i
i i i i i i i i i i i i i i i i i i i i i i i

Вопросы для повторения

В сетях Ethernet данные передаются на устройства по соответствующим MAC-адресам. Для этого коммутаторы и компьютеры динамически создают ARP-кэш и таблицы MAC-адресов. Если компьютеров в сети немного, эта процедура выглядит достаточно простой. Какие сложности могут

возникнуть в крупных сетях?
i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i
i i i i i i i i i i i i i i i i i i i i i i i i i i

Практическая работа 12: просмотр таблиц маршрутизации узлов
Топология

Задачи

Часть 1. Доступ к таблице маршрутизации узла

Часть 2. Изучение записей в таблице маршрутизации узла IPv4

Часть 3. Изучение записей в таблице маршрутизации узла IPv6

Исходные данные/сценарий

Для доступа к ресурсам сети ваш узел должен определить маршрут до узла назначения по таблице маршрутизации. Таблица маршрутизации узла мало чем отличается от таблицы маршрутизатора, но характерна для локального узла и выглядит гораздо проще. Чтобы пакет достиг локального узла назначения, необходима таблица маршрутизации локального узла. Чтобы достигнуть удалённого узла назначения, нужны таблицы маршрутизации локального узла и маршрутизатора. Команды netstat -r и route print позволяют получить представление о том, как локальный узел маршрутизирует пакеты до места назначения.

В данной лабораторной работе вам предстоит отобразить и изучить информацию, которая содержится в таблице маршрутизации вашего ПК, с помощью команд netstat -r и router print. Вы увидите, как ваш ПК маршрутизирует пакеты в зависимости от адреса назначения.

Примечание. Эту лабораторную работу нельзя выполнять при помощи Netlab. Она предполагает наличие доступа к Интернету.

Необходимые ресурсы

• 1 ПК (Windows 7, Vista или XP с доступом в Интернет и командной строкой)

Часть 1: Доступ к таблице маршрутизации узла

Шаг 1: Запишите данные своего ПК.

На ПК откройте окно командной строки и введите команду ipconfig /all, чтобы отобразить и записать следующие данные:

^4-адрес	
MAC-адрес	
Шлюз по умолчанию	

Шаг 2: Отобразите таблицы маршрутизации.

В окне командной строки введите команду netstat -r (или route print), чтобы отобразить таблицу маршрутизации узла.

```
C:\Users\user1>netstat -r
===========================================================================
Interface List
 13...90 4c e5 be 15 63 ......Atheros AR9285 802.11b/g/n WiFi Adapter
  1...........................Software Loopback Interface 1
 25...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
 12...00 00 00 00 00 00 00 e0 Microsoft 6to4 Adapter
 26...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
 14...00 00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Met
          0.0.0.0          0.0.0.0      192.168.1.1     192.168.1.11
        127.0.0.0        255.0.0.0         On-link         127.0.0.1
        127.0.0.1  255.255.255.255         On-link         127.0.0.1
  127.255.255.255  255.255.255.255         On-link         127.0.0.1
      192.168.1.0    255.255.255.0         On-link      192.168.1.11
     192.168.1.11  255.255.255.255         On-link      192.168.1.11
    192.168.1.255  255.255.255.255         On-link      192.168.1.11
        224.0.0.0        240.0.0.0         On-link         127.0.0.1
        224.0.0.0        240.0.0.0         On-link      192.168.1.11
  255.255.255.255  255.255.255.255         On-link         127.0.0.1
  255.255.255.255  255.255.255.255         On-link      192.168.1.11
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
 14     58 ::/0                     On-link
  1    306 ::1/128                  On-link
 14     58 2001::/32                On-link
 14    306 2001:0:9d38:6ab8:1863:3bca:3f57:fef4/128
                                    On-link
 14    306 fe80::/64                On-link
 14    306 fe80::1863:3bca:3f57:fef4/128
                                    On-link
  1    306 ff00::/8                 On-link
 14    306 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```

Какие три раздела отображаются в выходных данных команды?

Шаг 3: Изучите список интерфейсов.

В первом разделе, Interface List (Список интерфейсов), отображаются адреса управления доступом к среде передачи данных (MAC), а также номера, присвоенные каждому интерфейсу подключения к сети на этом узле.

```
===========================================================================
Interface List
 13...90 4c e5 be 15 63 ......Atheros AR9285 802.11b/g/n WiFi Adapter
  1...........................Software Loopback Interface 1
 25...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
 12...00 00 00 00 00 00 00 e0 Microsoft 6to4 Adapter
 26...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
 14...00 00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
===========================================================================
```

В первом столбце приводится номер интерфейса, а во втором — список MAC-адресов, связанных с интерфейсами подключения к сети на узлах. Эти интерфейсы могут включать в себя адаптеры Ethernet, Wi-Fi и Bluetooth. В третьем столбце указываются производитель и описание интерфейса.

В данном примере в первой строке отображается беспроводной интерфейс, подключённый к локальной сети.

Примечание. Если на вашем ПК активированы интерфейс Ethernet и беспроводной адаптер, то в списке интерфейсов будут указаны оба интерфейса.

Назовите MAC-адрес интерфейса, подключённого к вашей локальной сети. Отличается ли этот MAC- адрес от того, который вы записали в шаге 1?

Во второй строке указан loopback (интерфейс «обратной петли»). Если на узле работает протокол TCP/IP, интерфейсу loopback автоматически назначается IP-адрес 127.0.0.1.

Последние четыре строки отражают технологию передачи данных, которая обеспечивает связь в смешанной среде и включает протоколы IPv4 и IPv6.

Часть 2: Изучение записей в таблице маршрутизации узла IPv4

В части 2 вам необходимо изучить таблицу маршрутизации узла IPv4. Она составляет второй раздел выходных данных команды netstat -r. В таблице указываются все известные маршруты IPv4, включая прямые подключения, локальную сеть и локальные маршруты по умолчанию.

```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.1.1     192.168.1.11     25
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
      192.168.1.0    255.255.255.0         On-link     192.168.1.11     281
     192.168.1.11  255.255.255.255         On-link     192.168.1.11     281
    192.168.1.255  255.255.255.255         On-link     192.168.1.11     281
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link     192.168.1.11     281
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link     192.168.1.11     281
===========================================================================
Persistent Routes:
  None
```

Выходные данные содержат пять столбцов: Сеть назначения (Network Destination), Маска подсети (Netmask), Шлюз (Gateway), Интерфейс (Interface) и Метрика (Metric).

• В столбце Network Destination (Сеть назначения) перечисляются доступные сети. Для сопоставления с IP-адресом назначения сеть назначения используется с маской подсети.

• В столбце Netmask (Маска подсети) указываются маски подсети, позволяющие определить сетевую и узловую части IP-адреса.

• В столбце Gateway (Шлюз) указывается, какой адрес используется узлом для отправления пакетов по адресу назначения удалённой сети. Если узел назначения подключён напрямую, то в выходных данных шлюз отображается как On-link.

- В столбце Interface (Интерфейс) указывается IP-адрес, настроенный на адаптере локальной сети. Он используется для передачи пакета по сети.
- В столбце Metric (Метрика) указывается стоимость использования маршрута. Эти данные позволяют рассчитать наилучший маршрут к месту назначения. Предпочтительный маршрут отличается более низким значением метрики по сравнению с другими вариантами.

В выходных данных отображаются пять различных типов активных маршрутов:

- Локальный маршрут по умолчанию 0.0.0.0 используется в тех случаях, когда пакет не соответствует другим адресам, указанным в таблице маршрутизации. Для дальнейшей обработки пакет направляется на шлюз с ПК. В данном примере пакет будет отправлен на адрес 192.168.1.1 с адреса 192.168.1.11.
- Адреса loopback с 127.0.0.0 до 127.255.255.255 относятся к прямому подключению и предоставляют сервисы локальному узлу.
- Все адреса для подсети с 192.168.1.0 до 192.168.1.255 относятся к узлу и локальной сети. Если конечный пункт назначения пакета находится в локальной сети, то пакет покинет интерфейс 192.168.1.11.
  - Адрес локального маршрута 192.168.1.0 представляет все устройства в сети 192.168.1.0/24.
  - Адрес локального узла — 192.168.1.11.
  - Широковещательный адрес сети 192.168.1.255 используется для отправки сообщений на все узлы в локальной сети.
- Особые групповые адреса класса D 224.0.0.0 зарезервированы для использования либо через интерфейс loopback (127.0.0.1), либо через узел (192.168.1.11).
- Локальный широковещательный адрес 255.255.255.255 можно использовать через интерфейс loopback (127.0.0.1) или узел (192.168.1.11).

Исходя из содержимого таблицы маршрутизации IPv4, что будет делать ПК, если пакет нужно отправить по адресу 192.168.1.15?

Что будет делать ПК, если пакет нужно отправить на удалённый узел по адресу 172.16.20.23?

Часть 3: Изучение записей в таблице маршрутизации узла IPv6

В части 3 вам необходимо изучить таблицу маршрутизации узла IPv6. Она составляет третий раздел выходных данных команды netstat -r. В таблице указываются все известные маршруты IPv6, включая прямые подключения, локальную сеть и локальные маршруты по умолчанию.

```
IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
 14     58 ::/0                     On-link
  1    306 ::1/128                  On-link
 14     58 2001::/32                On-link
 14    306 2001:0:9d38:6ab8:1863:3bca:3f57:fef4/128
                                    On-link
 14    306 fe80::/64                On-link
 14    306 fe80::1863:3bca:3f57:fef4/128
                                    On-link
  1    306 ff00::/8                 On-link
 14    306 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```

Выходные данные таблицы маршрутизации IPv6 отличаются по заголовкам столбцов и формату,

поскольку длина адресов IPv6 составляет не 32, а 128 бит. В разделе IPv6 Route Table (Таблица

маршрутизации IPv6) отображаются четыре столбца:

- В столбце If (Если) перечисляются номера сетевых интерфейсов под управлением протокола IPv6, взятые из раздела Interface List (Список интерфейсов) выходных данных команды netstat -r.
- В столбце Metric (Метрика) указывается стоимость каждого маршрута до места назначения. Чем ниже стоимость, тем более предпочтительным является маршрут, и метрика позволяет выбрать лучший из нескольких вариантов с одинаковым префиксом.
- В столбце Network Destination (Сеть назначения) указывается префикс адреса для маршрута.
- В столбце Gateway (Шлюз) указывается IPv6-адрес следующего перехода на пути к месту назначения. Если адрес следующего перехода подключён к узлу напрямую, приводится состояние On-link.

Раздел таблицы маршрутизации IPv6, сгенерированный командой netstat -r и приведённый

в данном примере, содержит следующие адреса назначения в сети:

- ::/0: эквивалент IPv6 в локальном маршруте по умолчанию. В столбце Gateway (Шлюз) указывается локальный адрес маршрутизатора по умолчанию.
- ::1/128: эквивалент ^4-адреса в интерфейсе loopback, обеспечивающий сервисы для локального узла.
- 2001 ::/32: глобальный индивидуальный префикс сети.
- 2001:0:9d38:6ab8:1863:3bca:3f57:fef4/128: глобальный индивидуальный ^6-адрес локального компьютера.
- fe80::/64: локальный адрес маршрута, который представляет все компьютеры в локальной сети IPv6.
- fe80::1863:3bca:3f57:fef4/128: локальный ^6-адрес канала локального компьютера.
- ff00::/8: специальные зарезервированные групповые адреса класса D, эквивалентные IPv4- адресам 224.x.x.x.

Таблица маршрутизации узла IPv6 содержит примерно ту же информацию, что и таблица маршрутизации IPv4. Назовите локальный маршрут по умолчанию для IPv4 и для IPv6.

Назовите адрес loopback и маску подсети для IPv4 и IP-адрес loopback для IPv6.

Сколько ^6-адресов присвоено данному компьютеру?

Сколько широковещательных адресов содержит таблица маршрутизации IPv6? Вопросы на закрепление

1. Как определяется количество битов для сети с протоколом IPv4? А с протоколом IPv6?
2. Почему в таблицах маршрутизации узлов отображаются данные обоих протоколов IPv4 и IPv6?

Практическая работа 13 Изучение физических характеристик маршрутизатора

Топология

Задачи

Часть 1. Изучение внешних характеристик маршрутизатора

Часть 2. Изучение внутренних характеристик маршрутизатора с помощью команд show

Общие сведения/сценарий

В ходе лабораторной работы вам предстоит изучить внешний вид маршрутизатора 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 порты USB.

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.

Примечание. В практических лабораторных работах CCNA используются маршрутизаторы с интегрированными сетевыми сервисами (ISR) Cisco 1941 с операционной системой Cisco IOS версии 15.2(4)M3 (образ universalk9). Допускается использование маршрутизаторов других моделей, а также других версий операционной системы Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и результаты их выполнения могут отличаться от тех, которые показаны в лабораторных работах.

Примечание. Убедитесь, что все настройки коммутатора удалены и загрузочная конфигурация отсутствует. Если вы не уверены, обратитесь к инструктору.

Необходимые ресурсы

- 1 маршрутизатор (Cisco 1941 с операционной системой Cisco IOS 15.2(4)M3 (универсальный образ) или аналогичная модель)
- 1 ПК (под управлением Windows 7 или 8 с программой эмуляции терминала, например, Tera Term)
- Консольные кабели для настройки устройств Cisco IOS через консольные порты

Часть 1: Изучение внешних характеристик маршрутизатора

Посмотрите на изображения ниже, осмотрите заднюю панель маршрутизатора Cisco и ответьте на следующие вопросы. Вы можете нарисовать на изображении стрелки или кружки, чтобы обозначить компоненты маршрутизатора.

Примечание. На приведенных ниже изображениях показан маршрутизатор Cisco 1941. В вашем учебном заведении могут использоваться другие модели. Информацию о маршрутизаторах Cisco серии 1941 и их спецификациях можно найти на веб-сайте cisco.com. Дополнительную информацию, включая ответы на многие заданные ниже вопросы, можно найти по следующей ссылке:

http://www.cisco.com/en/US/prod/collateral/routers/ps10538/data sheet c78 556319.html

Шаг 1: Обозначьте различные части маршрутизатора Cisco.

В этом шаге приводится изображение задней панели маршрутизатора Cisco 1941 ISR. Используйте его при ответах на заданные в этом шаге вопросы. Если же вы изучаете маршрутизатор другой модели, зарисуйте его заднюю панель в оставленном ниже пространстве и обозначьте компоненты и интерфейсы в соответствии со следующими вопросами.

a. Обведите и обозначьте выключатель питания маршрутизатора. Выключатель питания вашего маршрутизатора расположен в той же области, что и на приведенном изображении?

b. Обведите и обозначьте порты управления. Какие порты управления являются встроенными? Совпадают ли они с портами управления на вашем маршрутизаторе? Если нет, то чем они отличаются?

Все встроены. Совпадают.

c. Обведите и обозначьте LAN-интерфейсы маршрутизатора. Сколько LAN-интерфейсов имеет изображенный маршрутизатор? Какой тип интерфейса используется? Совпадают ли LAN- интерфейсы на вашем маршрутизаторе? Если нет, то чем они отличаются?

2 интерфейса Gigabit Ethernet. Совпадают.

d. Обведите и обозначьте WAN-интерфейсы маршрутизатора. Сколько WAN-интерфейсов имеет изображенный маршрутизатор? Какой тип интерфейса используется? Совпадают ли WAN- интерфейсы на вашем маршрутизаторе? Если нет, то чем они отличаются?

Один последовательный (Serial) интерфейс. Совпвдают.

e. Маршрутизатор Cisco 1941 ISR — это модульная платформа, оснащенная слотами расширения для различных модулей подключения к сети. Обведите и обозначьте слоты для модулей. Сколько здесь слотов для модулей? Сколько из них используется? Какого типа эти слоты? Совпадают они со слотами для модулей расширения на вашем маршрутизаторе? Если нет, то чем они отличаются?

Судя по надписям на корпусе, 2 слота. Используется 1. EHWIC. Совпадают.

f. Маршрутизатор Cisco 1941 оснащен слотами памяти Compact Flash для высокоскоростного хранения данных. Обведите и обозначьте слоты памяти Compact Flash. Сколько здесь слотов памяти? Сколько из них используется? Какой объем памяти они поддерживают? Совпадают они со слотами памяти на вашем маршрутизаторе? Если нет, то чем они отличаются?

Два слота. Используется первый (по умолчанию). До 4 ГБ. Совпадают.

g. Маршрутизатор Cisco 1941 оснащен портами USB 2.0. Встроенные порты USB поддерживают устройства eToken и карты флеш-памяти USB. USB-устройство eToken обеспечивает аутентификацию устройств и безопасную конфигурацию маршрутизаторов Cisco. Функция USB- накопителя позволяет использовать его как дополнительную внешнюю память и дополнительное загрузочное устройство. Обведите и обозначьте порты USB. Сколько здесь портов USB? На вашем маршрутизаторе есть порты USB?

2 порта. Да.

h. Маршрутизатор Cisco 1941 также оснащен консольным портом мини-USB типа B. Обведите и обозначьте консольный порт мини-USB типа B.

Шаг 2: Изучите индикаторы активности и состояния маршрутизатора.

На приведенных ниже изображениях показаны индикаторы активности и состояния на передней и задней панелях включенного и подключенного маршрутизатора Cisco 1941 ISR.

Примечание. Некоторые индикаторы на изображении задней панели маршрутизатора Cisco 1941 не горят.

a. Изучите индикаторы на представленном выше изображении передней панели маршрутизатора. Они обозначены метками SYS, ACT и POE. Что означают эти метки? О каком состоянии маршрутизатора говорят индикаторы на изображении? Когда индикатор горит, эти метки не читаются.

SYS — общее состояние

ACT — активность

POE — power over Ethernet

b. Изучите индикаторы маршрутизатора на представленном выше изображении задней панели. Видны три активных индикатора, по одному на каждый из подключенных интерфейсов и портов управления. Изучите индикаторы интерфейса своего маршрутизатора. Как помечены индикаторы? Что означают эти метки?

CONN — последовательным порт

EN — консольным порт

S — порт Ethernet

Эти метки означают, что порт активен.

c. За исключением портов управления и сетевых интерфейсов, какие еще индикаторы присутствуют на задней панели маршрутизатора? Для чего они могут быть предназначены?

Аналогичные индикаторы! есть у слотов Compact Flash и порта Mini-USB. Они выполняют ту же функцию: сообщают о том, что порт активен.

Часть 2: Изучение внутренних характеристик маршрутизатора с помощью команд show

Шаг 1: Подключитесь к маршрутизатору через консоль и воспользуйтесь командой show version.

a. С помощью программы Tera Term подключитесь к маршрутизатору через консоль и войдите в привилегированный режим EXEC с помощью команды enable:

Router> enable Router#

b. Отобразите информацию о маршрутизаторе с помощью команды show version. Для пролистывания выходных данных используйте клавишу ПРОБЕЛ.

Router# show version

Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.2(4)M3, RELEASE SOFTWARE (fc1)

Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2011 by Cisco Systems, Inc. Compiled Thu 2 6-Jul-12 19:34 by prod_rel_team

ROM: System Bootstrap, Version 15.0(1r)M15, RELEASE SOFTWARE (fc1)

Router uptime is 1 day, 14 hours, 46 minutes

System returned to ROM by power-on

System restarted at 07:26:55 UTC Mon Dec 3 2012

System image file is "flash0:c1900-universalk9-mz.SPA.152-4.M3.bin" Last reload type: Normal Reload Last reload reason: power-on

<output omitted>

If you require further assistance please contact us by sending email to export@cisco.com.

Cisco CISCO1941/K9 (revision 1.0) with 4 8742 4K/3 68 64K bytes of memory. Processor board ID FGL16082318 2 Gigabit Ethernet interfaces 2 Serial(sync/async) interfaces 1 terminal line

1 Virtual Private Network (VPN) Module

DRAM configuration is 64 bits wide with parity disabled. 255K bytes of non-volatile configuration memory. 250880K bytes of ATA System CompactFlash 0 (Read/Write) <output omitted>

Configuration register is 0x2102

c. Исходя из выходных данных команды show version, ответьте на следующие вопросы о

маршрутизаторе. Если вы изучаете маршрутизатор другой модели, укажите здесь его данные.

1) На какой версии операционной системы Cisco IOS работает маршрутизатор и как называется файл образа системы?

Версия 15. 1(4)M4. Образ flash0: c1900-universalk9-mz.SPA.151-1.M4.bin

2) Какая версия программы начального запуска установлена в ОЗУ BIOS?

Неотобразилось©

3) Как долго маршрутизатор работал без перезагрузки (время безотказной работы)?

4) Каким объемом оперативной динамической памяти DRAM обладает маршрутизатор? 512 МБ

5) Назовите идентификационный номер процессорной платы маршрутизатора. FTX152400KS

6) Какими сетевыми интерфейсами оснащен маршрутизатор?

Gigabit Ethernet и 2 последовательных интерфейса

7) Какой объем памяти Compact Flash предоставлен для хранения IOS? 249856 К Б

8) Какой объем энергонезависимой памяти (NVRAM) предоставлен для хранения файла конфигурации?

255 КБ

9) Какое значение используется для конфигурационного регистра? 0x2102

Шаг 2: Используйте команду show interface, чтобы изучить сетевые интерфейсы.

a. Используя команду show interface gigabitEthernet 0/0, узнайте состояние интерфейса Gigabit Ethernet 0/0.

Примечание. Набрав часть команды, например show interface g, можно завершить ввод оставшейся части команды gigabitEthernet нажатием клавиши Tab.

b. Используя приведенные выше выходные данные команды show interface gigabitEthernet 0/0 или выходные данные своего маршрутизатора, ответьте на следующие вопросы.

Какие используются тип оборудования и MAC-адрес интерфейса Gigabit Ethernet?

Оборудование Gigabit Ethernet. Адрес: 0002.1761. 7701.

Назовите тип интерфейсной среды. Интерфейс включен или выключен? Ethernet. Выключен.

c. С помощью команды show interfaces serial 0/0/0 определите состояние последовательного интерфейса Serial 0/0/0.

Практическая работа 14 Создание сети, состоящей из коммутатора и маршрутизатора

Топология

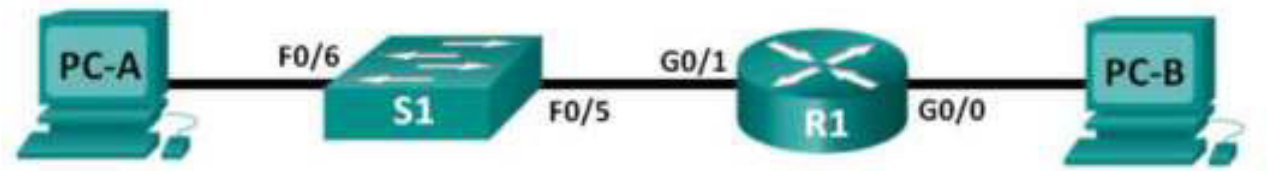


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/0	192.168.0.1	255.255.255.0	—
	G0/1	192.168.1.1	255.255.255.0	—
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.0.3	255.255.255.0	192.168.0.1

Задачи

Часть 1. Настройка топологии и инициализация устройств

Часть 2. Настройка устройств и проверка подключения

Часть 3. Отображение сведений об устройстве

Общие сведения/сценарий

Это комплексная Практическая работа , предназначенная для повторения рассмотренных ранее команд IOS. В этой лабораторной работе вы соедините оборудование кабелями в соответствии со схемой топологии. Затем вы настроите устройства согласно таблице адресации. После сохранения конфигурации вы проверите ее, выполнив тестирование сетевого подключения.

После настройки устройств и проверки сетевого подключения вы, воспользовавшись командами IOS, получите с этих устройств сведения, необходимые для подготовки ответов на вопросы о сетевом оборудовании. Эта Практическая работа содержит минимум инструкций по выполнению команд, необходимых для настройки маршрутизатора. Список требуемых команд приведен в Приложении А. Проверьте свои знания: настройте устройства, не пользуясь приложениями.

Примечание**.** В практических лабораторных работах CCNA используются маршрутизаторы с интегрированными сетевыми сервисами (ISR) Cisco 1941 с операционной системой Cisco IOS версии 15.2(4)M3 (образ universalk9). Также используются коммутаторы Cisco Catalyst 2960 с операционной системой Cisco IOS версии 15.0(2) (образ lanbasek9). Можно использовать другие маршрутизаторы, коммутаторы и версии Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и результаты их выполнения могут отличаться от тех, которые показаны в лабораторных

работах. Точные идентификаторы интерфейсов см. в сводной таблице по интерфейсам маршрутизаторов Сводная таблица по интерфейсам маршрутизаторов в конце лабораторной работ

Примечание**.** Убедитесь, что все настройки коммутатора и маршрутизатора удалены, и загрузочная конфигурация отсутствует. Процедуры инициализации и перезагрузки маршрутизатора и коммутатора описаны в Приложении Б.

Необходимые ресурсы

- 1 маршрутизатор (Cisco 1941 с операционной системой Cisco IOS 15.2(4)M3 (универсальный образ) или аналогичная модель)
- 1 коммутатор (Cisco 2960 с ПО Cisco IOS версии 15.0(2) с образом Ianbasek9 или аналогичная модель)
- 2 ПК (Windows 7 или 8 с программой эмуляции терминала, например, Tera Term)
- Консольные кабели для настройки устройств Cisco IOS через консольные порты
- Кабели Ethernet, расположенные в соответствии с топологией

Примечание. Интерфейсы Gigabit Ethernet на маршрутизаторах Cisco 1941 определяют скорость автоматически, поэтому для подключения маршрутизатора к PC-B можно использовать прямой кабель Ethernet. При использовании другой модели маршрутизатора Cisco может возникнуть необходимость использовать перекрестный кабель Ethernet.

Часть 1: Настройка топологии и инициализация устройств

Шаг 1: Создайте сеть согласно топологии.

a. Подключите устройства, показанные в топологии, и кабели соответствующим образом.
b. Включите все устройства в топологии.

Шаг 2: Выполните инициализацию и перезагрузку маршрутизатора и коммутатора.

Если на маршрутизаторе и коммутаторе имеются ранее сохраненные файлы конфигурации, выполните инициализацию и перезагрузите эти устройства, чтобы вернут их основные настройки. Инструкции по инициализации и перезагрузке этих устройств приводятся в Приложении Б.

Часть 2: Настройка устройств и проверка подключения

В части 2 вы настроите топологию сети и такие базовые параметры, как IP-адреса интерфейсов, доступ к устройствам и пароли. Имена устройств и адресные данные можно найти в разделах “Топология” и “Таблица адресации” в начале этой лабораторной работы.

Примечание. В Приложении А приведены сведения о конфигурации для выполнения шагов в части 2. Постарайтесь выполнить часть 2, не пользуясь этим приложением.

Шаг 1: Сделайте на интерфейсах ПК статические настройки IP-адресации.

a. Настройте на компьютере PC-A IP-адрес, маску подсети и параметры шлюза по умолчанию.

b. Настройте на компьютере PC-B IP-адрес, маску подсети и параметры шлюза по умолчанию.
c. Отправьте ping на PC-B из командной строки PC-A.
Почему проверка связи не удалась?
Маршрутизатор не настроен. Подключитесь к маршрутизатору с помощью консоли и активируйте привилегированный режим
exec.
a. Войдите в режим конфигурации.
b. Назначьте маршрутизатору имя устройства.
c. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.
d. Назначьте class в качестве зашифрованного пароля привилегированного режима EXEC.
e. Назначьте cisco в качестве пароля консоли и включите режим входа в систему по паролю. д. Назначьте cisco в качестве пароля виртуального терминала и включите вход по паролю.
h. Зашифруйте открытые пароли.
i. Создайте баннер с предупреждением о запрете несанкционированного доступа к устройству.
j. Настройте и активируйте на маршрутизаторе оба интерфейса.
k. Для каждого интерфейса введите описание, указав, какое устройство к нему подключено.
l. Сохраните файл текущей конфигурации в файл загрузочной конфигурации.
т. Настройте на маршрутизаторе время.
Примечание. Вопросительный знак (?) позволяет открыть справку с правильной последовательностью параметров, необходимых для выполнения этой команды.
п. Протестируйте компьютер PC-B, отправив компьютеру PC-A эхо-запрос из окна командной строки.
Успешно ли выполнена проверка связи? Почему?
Да, запрос выполнен успешно. Маршрутизатор направил ICMP пакет из одной под сети в другую и обратно .
Часть 3: Отображение сведений об устройстве
В части 3 вы воспользуетесь командами show для получения данных с маршрутизатора и коммутатора.
Шаг 1: Соберите с сетевых устройств данные об аппаратном и программном обеспечении.
а. С помощью команды show version ответьте на следующие вопросы о маршрутизаторе.
Как называется образ IOS, под управлением которой работает маршрутизатор? flasb h 0 : c 1 900- universaI k9 - mz . SPA. 151 - 1. M4 . bin
Каким объемом памяти DRAM обладает маршрутизатор?
3 2 М Б

Каким объемом памяти NVRAM обладает маршрутизатор?
2 5 5 К Б
Каким объемом флеш-памяти обладает маршрутизатор?
249856 КБ
Ь. С помощью команды show version ответьте на следующие вопросы о коммутаторе. Как называется образ IOS, под управлением которой работает коммутатор?
Не отображается.
Каким объемом динамического ОЗУ (DRAM) обладает коммутатор?
2 1 039 КБ
Каким объемом энергонезависимой памяти (NVRAM) обладает коммутатор?
6 3488 К Б
Назовите номер модели коммутатора.
WS- C2 960-24TT
Шаг 2: Отобразите таблицу маршрутизации на маршрутизаторе.
Выполните команду show ip route на маршрутизаторе, чтобы ответить на следующие вопросы. Какой код используется в таблице маршрутизации для обозначения сети с прямым подключением?
"C "
Сколько записей маршрутов обозначены буквой «С» в таблице маршрутизации? 2 Какие типы интерфейсов связаны с маршрутами, закодированными с символом «С»?
Fast Ethernet , Gigabit Ethernet, . . .
Шаг 3: Выведите на маршрутизатор сведения об интерфейсе.
С помощью команды show interface g0/1 ответьте на следующие вопросы.
Укажите текущее состояние интерфейса G0/1.
Gigabit Erhernet0/ 1isup , line protocol is up (connect.ed)
Назовите MAC-адрес интерфейса G0/1.
0 1.64a 0.2 80 2
Каким образом в этой команде отображается адрес в Интернете?
1 Р а д р е с и н те р ф е й с а с п р е ф и кс о м п о д с ети 1 92.1 68.1.1/24
Шаг 4: Выведите на маршрутизатор и коммутатор сводный список интерфейсов.
b. Введите команду **show ip interface brief** на коммутаторе.

```
Switch# show ip interface brief
Interface              IP Address      OK? Method Status                Protocol
Vlan1                  unassigned      YES manual up                    up
FastEthernet0/1        unassigned      YES unset  down                  down
FastEthernet0/2        unassigned      YES unset  down                  down
FastEthernet0/3        unassigned      YES unset  down                  down
FastEthernet0/4        unassigned      YES unset  down                  down
FastEthernet0/5        unassigned      YES unset  up                    up
FastEthernet0/6        unassigned      YES unset  up                    up
FastEthernet0/7        unassigned      YES unset  down                  down
FastEthernet0/8        unassigned      YES unset  down                  down
FastEthernet0/9        unassigned      YES unset  down                  down
FastEthernet0/10       unassigned      YES unset  down                  down
FastEthernet0/11       unassigned      YES unset  down                  down
FastEthernet0/12       unassigned      YES unset  down                  down
FastEthernet0/13       unassigned      YES unset  down                  down
FastEthernet0/14       unassigned      YES unset  down                  down
FastEthernet0/15       unassigned      YES unset  down                  down
FastEthernet0/16       unassigned      YES unset  down                  down
FastEthernet0/17       unassigned      YES unset  down                  down
FastEthernet0/18       unassigned      YES unset  down                  down
FastEthernet0/19       unassigned      YES unset  down                  down
FastEthernet0/20       unassigned      YES unset  down                  down
FastEthernet0/21       unassigned      YES unset  down                  down
FastEthernet0/22       unassigned      YES unset  down                  down
FastEthernet0/23       unassigned      YES unset  down                  down
FastEthernet0/24       unassigned      YES unset  down                  down
GigabitEthernet0/1     unassigned      YES unset  down                  down
GigabitEthernet0/2     unassigned      YES unset  down                  down
Switch#
```

Для проверки конфигурации интерфейса можно использовать несколько команд. Одна из наиболее удобных— команда show ip interface brief**.** Выходные данные команды содержат сводный список интерфейсов устройства с указанием статуса каждого интерфейса.

```
R1# show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Embedded Service Engine0/0 unassigned      YES unset  administratively down down
GigabitEthernet0/0         192.168.0.1     YES manual up                    up
GigabitEthernet0/1         192.168.1.1     YES manual up                    up
Serial0/0/0                unassigned      YES unset  administratively down down
Serial0/0/1                unassigned      YES unset  administratively down down
R1#
```

а. Введите команду **show ip interface brief** на маршрутизаторе.

Вопросы для повторения

1. Если интерфейс G0/1 выключен администратором, какая команда конфигурации интерфейса позволит его включить?

no shutdown

2. Что произойдет в случае неправильной конфигурации интерфейса G0/1 на маршрутизаторе с IP- адресом 192.168.1.2?

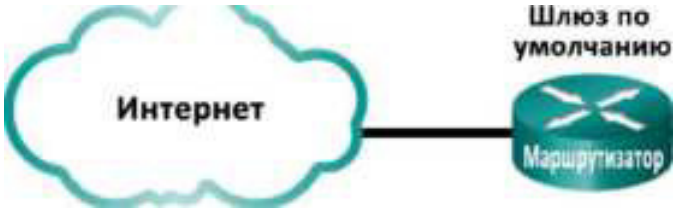
Пакеты с узла PC-A не смогут достигнуть других сетей , т.к . наиём в качестве основного шлюза на строен адрес 192.168.1.1.

Сводная таблица по интерфейсам маршрутизаторов

Сводная таблица по интерфейсам маршрутизаторов				
Модель маршрутизатора	Интерфейс Ethernet № 1	Интерфейс Ethernet № 2	Последовательный интерфейс № 1	Последовательный интерфейс № 2
1 800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Примечание. Чтобы узнать, как настроен маршрутизатор, посмотрите на интерфейсы и определите тип маршрутизатора и количество имеющихся у него интерфейсов. Перечислить все комбинации конфигураций для каждого класса маршрутизаторов невозможно. Эта таблица содержит идентификаторы для возможных комбинаций интерфейсов Ethernet и последовательных интерфейсов на устройстве. Другие типы интерфейсов в таблице не представлены, хотя они могут присутствовать в данном				

Практическая работа 15: наблюдение за процессом трёхстороннего рукопожатия TCP с помощью программы Wireshark

Топология



Задачи

Часть 1. Подготовка программы Wireshark к захвату пакетов

- Выберите подходящий интерфейс сетевого адаптера для захвата пакетов. Часть 2. Захват, поиск и изучение пакетов
- Захватите данные веб-сеанса на узле www.google.com.
- Найдите соответствующие пакеты для веб-сеанса.
- Изучите содержащиеся в пакетах данные, включая IP-адреса, номера портов TCP и флажки управления TCP.

Исходные данные/сценарий

В данной лабораторной работе вам предстоит воспользоваться программой Wireshark для захвата и изучения пакетов, сгенерированных между браузером ПК, где используется HTTP-протокол, и вебсервером, например www.google.com. При первом запуске приложения на узле, например HTTP или FTP, TCP устанавливает связь между двумя узлами с помощью трёхстороннего рукопожатия.

Например, при просмотре интернет-страниц через веб-браузер ПК трёхстороннее рукопожатие позволяет установить связь между узловым ПК и веб-сервером. Одновременно на ПК могут иметь место сразу несколько активных сеансов TCP с разными веб-сайтами.

Примечание. Эту лабораторную работу нельзя выполнять при помощи Netlab. Она предполагает наличие доступа к Интернету.

Необходимые ресурсы

1 ПК (Windows 7, Vista или XP с доступом к командной строке, доступу к Интернету и установленному анализатору пакетов Wireshark)

Часть 1: Подготовка программы Wireshark к захвату пакетов

В части 1 вам необходимо запустить программу Wireshark и выбрать подходящие интерфейсы для начала захвата пакетов.

Шаг 1: Узнайте адреса интерфейсов ПК.

Для выполнения лабораторной работы вам нужно узнать IP-адрес своего ПК и физический адрес сетевого адаптера, который также называется MAC-адресом.

а. Откройте окно командной строки, введите ipconfig /all и нажмите клавишу ВВОД.

```
Physical Address. . . . . . . . . : C8-0A-A9-FA-DE-0D
DHCP Enabled. . . . . . . . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv4 Address. . . . . . . . . . . : 192.168.1.130(Preferred)
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Lease Obtained. . . . . . . . . . : Saturday, December 01, 2012 1:43:35 PM
Lease Expires . . . . . . . . . . : Sunday, December 02, 2012 1:43:35 PM
Default Gateway . . . . . . . . . : 192.168.1.1
DHCP Server . . . . . . . . . . . : 192.168.1.1
DNS Servers . . . . . . . . . . . : 192.168.1.1
NetBIOS over Tcpip. . . . . . . . : Enabled
```

b. Запишите IP- и MAC-адреса, связанные с выбранным адаптером Ethernet, поскольку это и есть тот адрес источника, который нужно искать при анализе захваченных пакетов.

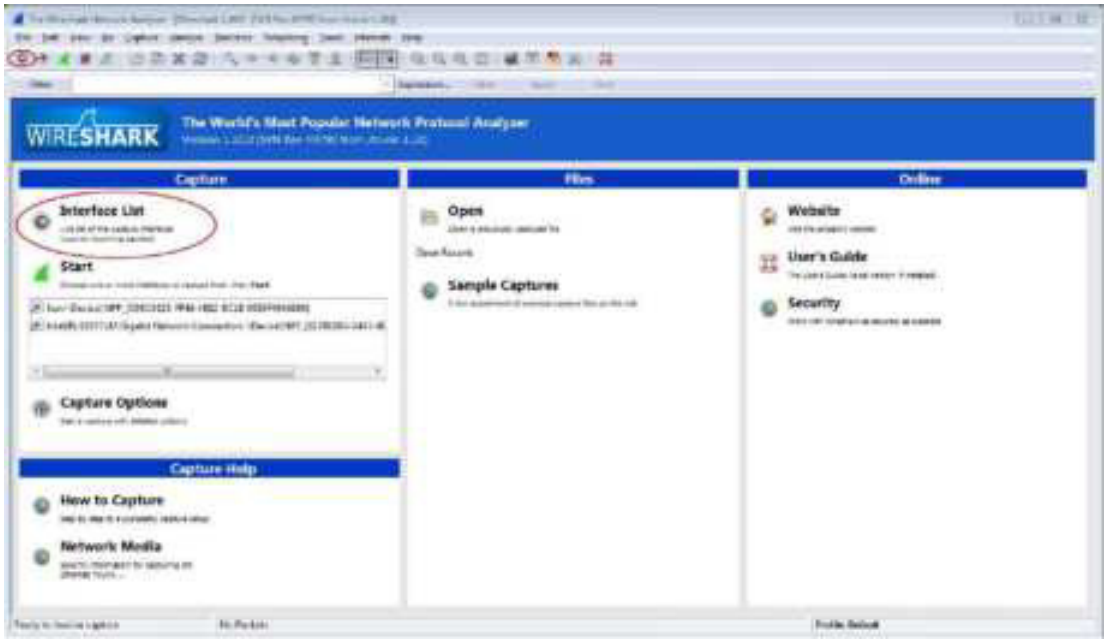
IP-адрес узла ПК:

MAC-адрес узла ПК:

Шаг 2: Запустите программу Wireshark и выберите подходящий интерфейс.

a. Нажмите кнопку Пуск и дважды нажмите на Wireshark.

b. Запустив программу Wireshark, нажмите на параметр Interface List (Список интерфейсов).



c. В окне Wireshark: Capture Interfaces (Захват интерфейсов) установите флажок напротив интерфейса подключения к вашей локальной сети.

Примечание. Если указано несколько интерфейсов и вы не уверены в выборе, нажмите кнопку Details (Сведения). Откройте вкладку 802.3 (Ethernet) и убедитесь в том, что MAC-адрес соответствует тому, что вы записали в шаге 1b. Проверив данные, закройте окно со сведениями об интерфейсе.

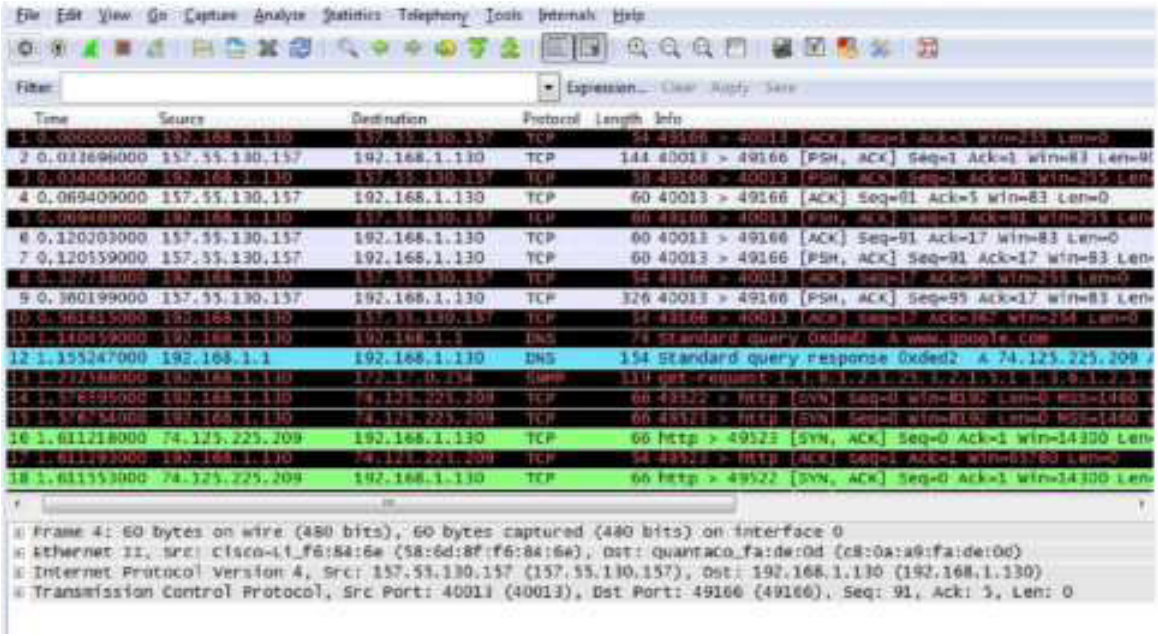
Часть 2: Захват, поиск и изучение пакетов

Шаг 1: Нажмите кнопку Start (Старт), чтобы начать захват данных.

a. Откройте веб-сайт www.google.com. Сверните окно Google и вернитесь в программу Wireshark. Остановите процесс захвата данных. Вы увидите захваченный трафик, как показано на шаге b.

Примечание. Инструктор может предложить вам другой веб-сайт. В этом случае введите название или адрес сайта в соответствующее поле:

b. Теперь окно перехвата данных активно. Найдите столбцы Source (Источник), Destination (Назначение) и Protocol (Протокол).



Шаг 2: Найдите соответствующие пакеты для веб-сеанса.

Если компьютер включён недавно и еще не использовался для доступа к Интернету, в захваченных данных вы сможете увидеть весь процесс, включая протокол разрешения адресов (ARP), службу доменных имен (DNS) и трёхстороннее рукопожатие TCP. На экране захвата в части 2, шаг 1 показаны

все пакеты, которые ПК должен отправить на адрес www.google.com. В данном случае ПК уже имел запись ARP для шлюза по умолчанию, поэтому первым делом он создал DNS-запрос для преобразования www.google.com.

b. В кадре 11 показан DNS-запрос от ПК к DNS-серверу, призванный преобразовать доменное имя www.google.com в IP-адрес веб-сервера. ПК должен знать IP-адрес до отправления первого пакета на веб-сервер.

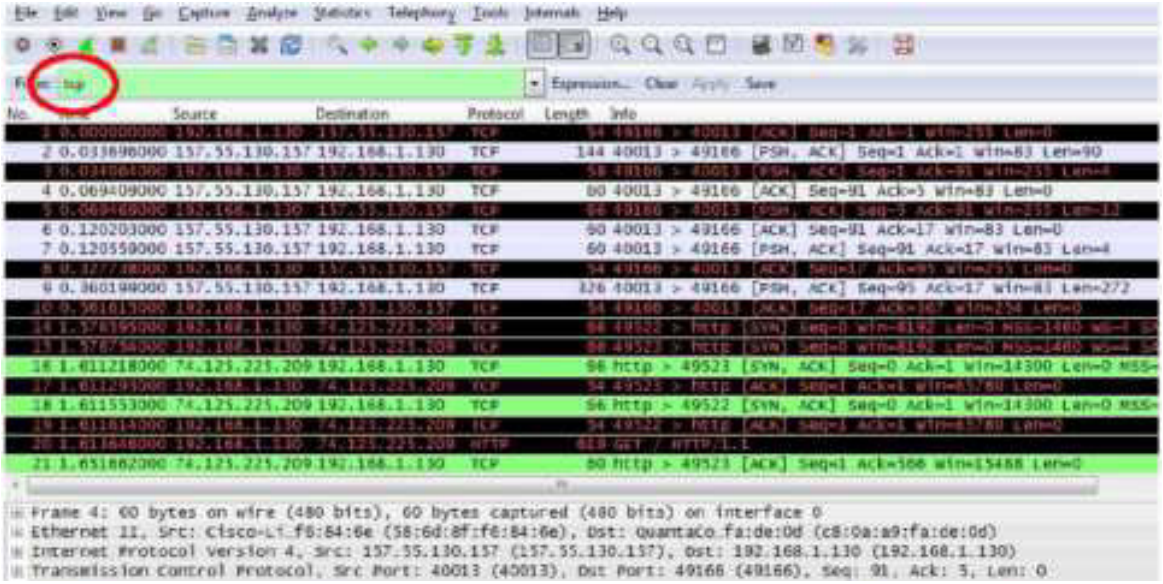
Назовите IP-адрес DNS-сервера, запрошенного компьютером.

c. Кадр 12 показывает ответ DNS-сервера, содержащий IP-адрес www.google.com.

d. Найдите соответствующий пакет, чтобы запустить процедуру трёхстороннего рукопожатия. В данном примере кадр 15 показывает начало трёхстороннего рукопожатия TCP.

Назовите IP-адрес веб-сервера Google.

e. Если вы получили много пакетов, связанных с TCP-соединением, воспользуйтесь фильтрами программы Wireshark. В поле фильтра программы Wireshark введите tcp и нажмите клавишу ВВОД.



Шаг 3: Изучите содержащиеся в пакетах данные, включая IP-адреса, номера портов TCP и флажки управления TCP.

e. В нашем примере кадр 15 показывает начало трёхстороннего рукопожатия между ПК и вебсервером Google. На панели списка пакетов (верхний раздел основного окна) выберите кадр. После этого будет выделена строка и отображена зашифрованная информация из пакета в двух нижних панелях. Проверьте данные TCP в панели сведений о пакетах (средний раздел основного окна).

e. На панели нажмите на значок + слева от строки Transmission Control Protocol (Протокол управления передачей данных), чтобы увидеть подробную информацию о TCP.

e. Слева от флажков нажмите на значок +. Обратите внимание на порты источника и назначения, а также на установленные флажки.

Примечание. Чтобы отобразить все необходимые данные, скорректируйте размеры окон программы Wireshark

Практическая работа **16**: изучение захваченных данных DNS UDP с помощью программы Wireshark

Топология

Задачи

Часть 1. Запись данных IP-конфигурации ПК

Часть 2. Захват запросов и ответов DNS с помощью программы Wireshark Часть 3. Анализ захваченных пакетов DNS или UDP

Исходные данные/сценарий

Если вы хоть раз выходили в Интернет, то пользовались службой доменных имён (DNS). DNS — это распределённая сеть серверов, которая преобразует понятные имена доменов, например www.google.com, в IP-адрес. При вводе в браузер URL-адреса какого-либо сайта ПК отправляет в DNS запрос об IP-адресе DNS-сервера. Запрос DNS-сервера вашего ПК и ответ DNS-сервера используют в качестве протокола транспортного уровня протокол пользовательских датаграмм (UDP). UDP не требует соединения и настройки сеанса, как TCP. Запросы и ответы DNS чрезвычайно малы и не требуют служебных сигналов TCP.

В ходе лабораторной работы вы будете обмениваться данными с DNS-сервером, отправляя в DNS запросы по транспортному протоколу UDP. Для анализа обмена данными с сервером доменных имен будет использоваться программа Wireshark.

Примечание. Эту лабораторную работу нельзя выполнять при помощи Netlab. Она предполагает наличие доступа к Интернету.

Необходимые ресурсы

1 ПК (Windows 7, Vista или XP с доступом к командной строке, доступу к Интернету и установленному анализатору пакетов Wireshark)

Часть 1: Запись данных IP-конфигурации ПК

В части 1 с помощью командыipconfig МПна локальном ПК вам нужно будет найти и записать MAC- и IP-адреса сетевого адаптера вашего ПК, IP-адрес указанного шлюза по умолчанию и IP-адрес DNS- сервера, указанного для ПК. Запишите эти данные в приведённую ниже таблицу. Они вам потребуются для анализа пакетов в следующих частях лабораторной работы.

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

Часть 2: Захват запросов и ответов DNS с помощью программы Wireshark

В части 2 вам нужно настроить программу Wireshark для захвата пакетов запросов и ответов DNS и продемонстрировать использование транспортного протокола UDP при обмене данными с DNS- сервером.

a. Нажмите кнопку **Пуск** и откройте программу Wireshark.

Примечание. Если программа Wireshark не установлена, её можно загрузить по адресу http://www.wireshark.org/download.html.

b. Выберите интерфейс Wireshark для захвата пакетов. Используйте **Interface List** (Список интерфейсов), чтобы выбрать интерфейс, который связан IP- и MAC-адресами ПК, записанными в части 1.

c. Выбрав нужный интерфейс, нажмите **Start** (Начать), чтобы начать захват пакетов.

d. Откройте веб-браузер и введите www.google.com**.** Нажмите клавишу ВВОД, чтобы продолжить.

e. Как только откроется главная страница Google, нажмите кнопку **Stop** (Остановить), чтобы остановить захват данных программой Wireshark.

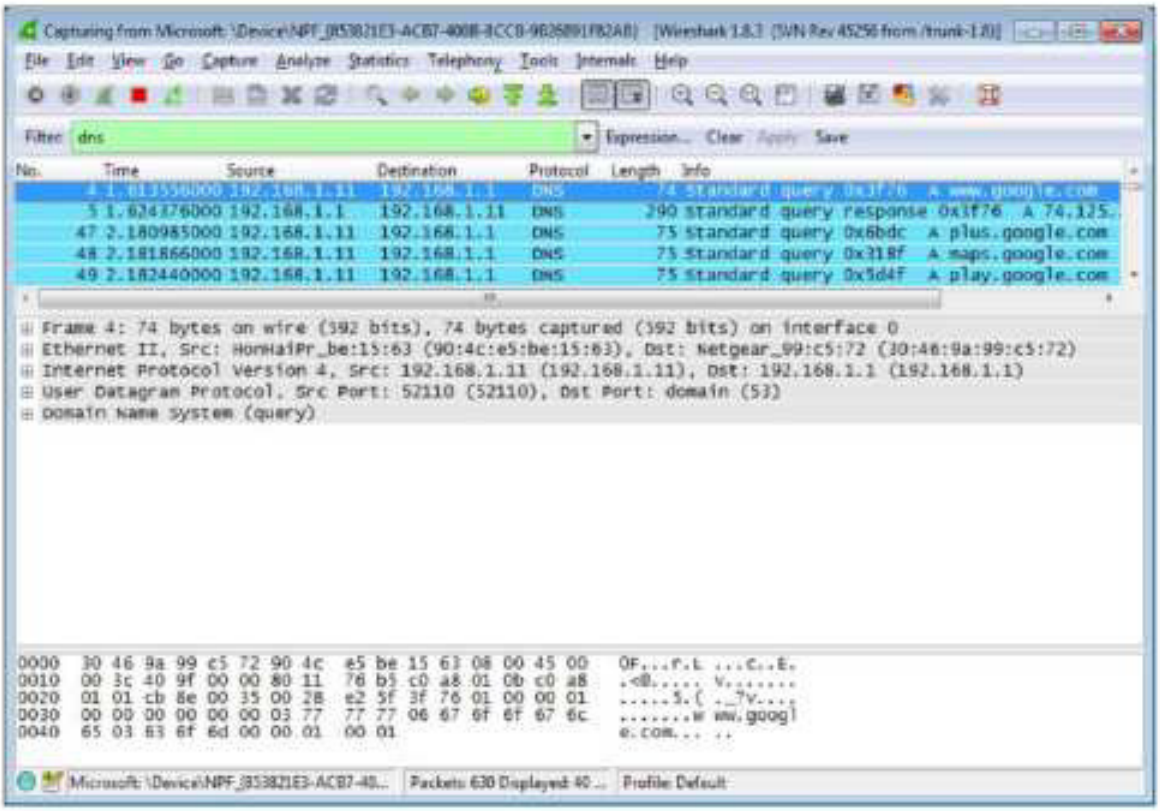
Часть 3: Анализ захваченных пакетов DNS или UDP

В части 3 вам необходимо изучить пакеты UDP, созданные при обмене данными с DNS-сервером для IP-адресов www.google.com.

Шаг 1: Отфильтруйте DNS-пакеты.

a. В главном окне программы Wireshark введите **dns в** строке **Filter** (Фильтр). Нажмите **Apply** (Применить) или клавишу ВВОД.

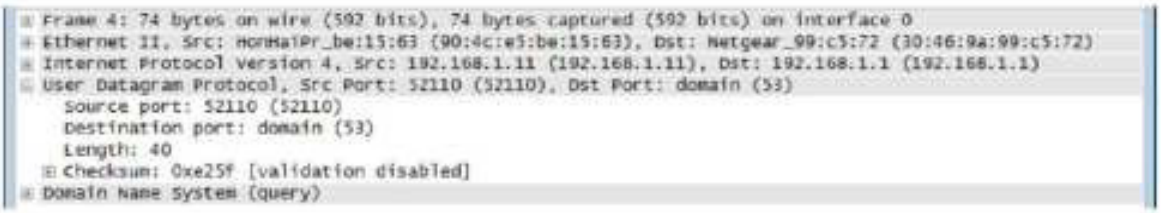
Примечание. Если после применения фильтра DNS никакие результаты не отображаются, закройте веб-браузер и введите в окне командной строки команду **ipconfig /flushdns,** чтобы удалить все предыдущие результаты DNS. Перезапустите захват данных программой Wireshark и повторите шаги 2b-2e. Если решить проблему не удалось, в окне командной строки введите команду **nslookup** www.google.com в качестве альтернативы браузеру.



b. На панели списка захваченных пакетов (верхний раздел) в главном окне программы найдите пакет со словами Standard query (стандартный запрос) и A www.google.com (запрос сайта google.com). См. пример в кадре 4.

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

Изучите UDP с помощью DNS-запроса о сайте www.google.com, захваченного программой Wireshark. В данном примере для анализа выбран захваченный кадр 4 на панели списка захваченных пакетов. Протоколы в этом запросе отображаются на панели сведений о пакетах (Details, средний раздел) в главном окне. Записи протокола выделены серым цветом.



a. На панели сведений о пакетах кадр 4 имеет 74 байта данных, как показано в первой строке. 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 назначения. MAC-адрес источника принадлежит вашему локальному ПК как источнику DNS-запроса. MAC-адрес назначения — это шлюз по умолчанию, поскольку это последняя остановка запроса перед выходом из локальной сети.

Совпадает ли MAC-адрес источника с адресом, записанным в части 1 для локального ПК?

c. В строке интернет-протокола версии 4 захваченные данные IP-пакета показывают, что IP-адрес источника данного DNS-запроса — 192.168.1.11, 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 сопоставить IP- и MAC-адреса для устройств источника и назначения?

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

IP-пакет и заголовок инкапсулируют сегмент UDP. Сегмент UDP содержит DNS-запрос в виде данных.

d. Заголовок UDP имеет только четыре поля: порт источника, порт адресата, длина и контрольная сумма. Как показано ниже, длина каждого поля в заголовке UDP составляет всего 16 бит.

СЕГМЕНТ UDP

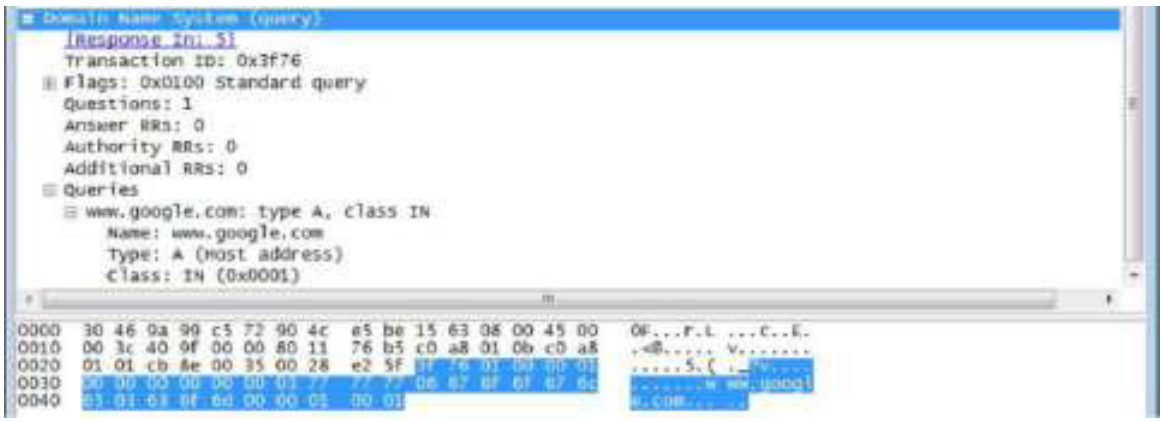
0 16 31

ПОРТ ИСТОЧНИКА unp	ПОРТ НАЭНАЧРНИЯ UDP
ДЛИНА СООБЩЕНИЯ JDP	КОН 1 РОЛЬНАЯ СУММА UDP
ДАННЫЕ	
ДАННЫЕ...	

Разверните протокол UDP на панели сведений о пакетах, нажав на значок плюса (+). Обратите внимание на то, что в открывшемся окне будут только четыре поля. Номер порта источника в данном примере — 52110. Порт источника был случайно сгенерирован локальным ПК с использованием зарезервированных номеров портов. Порт назначения — 53. Порт 53 — это общеизвестный порт, зарезервированный для использования с DNS. DNS-серверы получают DNS- запросы от клиентов через порт 53.

```
⊟ User Datagram Protocol, Src Port: 52110 (52110), Dst Port: domain (53)
    Source port: 52110 (52110)
    Destination port: domain (53)
    Length: 40
  ⊟ Checksum: 0xa25f [validation disabled]
      [Good Checksum: False]
      [Bad Checksum: False]
```

В данном примере длина этого сегмента UDP составляет 40 байт. Из 40 байтов восемь составляют заголовок. Остальные 32 байта используются данными DNS-запроса. На приведённом ниже снимке экрана выделены 32 байта данных DNS-запроса на панели отображения пакета в виде последовательности байтов (нижний раздел главного окне Wireshark).



Контрольная сумма используется для определения целостности пакета после передачи через Интернет.

Заголовок UDP отличается низкими потерями, поскольку протокол UDP не имеет полей, связанных с трёхсторонним рукопожатием в протоколе TCP. Любые проблемы с надёжностью передачи данных должны решаться на уровне приложений.

Запишите результаты захвата данных программой Wireshark в приведённую ниже таблицу.

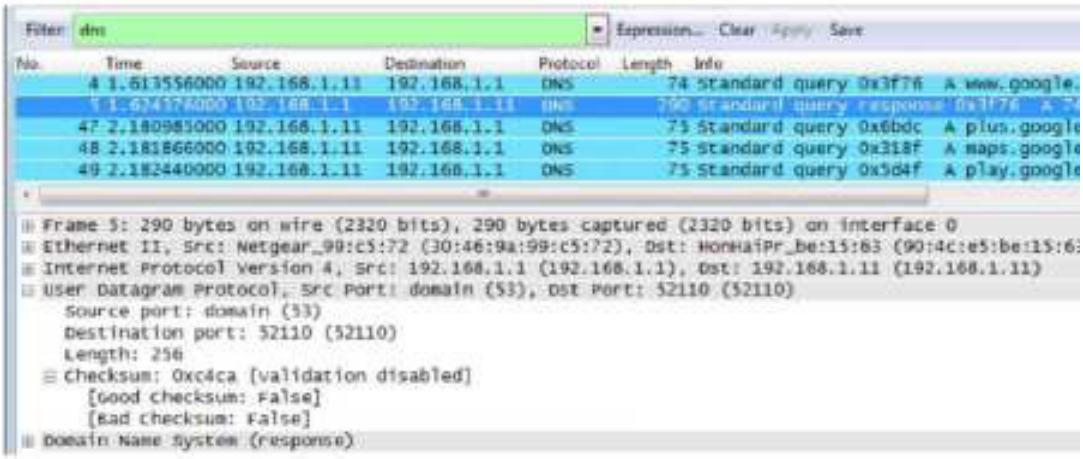
Размер кадра	
MAC-адрес источника	
MAC-адрес назначения	
IP-адрес источника	
IP-адрес назначения	
Порт источника	
Порт назначения	

Совпадает ли IP-адрес источника с IP-адресом локального ПК, записанным в части 1? Совпадает ли IP-адрес назначения со шлюзом по умолчанию, записанным в части 1?

Шаг 3: Изучите UDP с помощью DNS-ответа.

В этом шаге вам нужно изучить пакет DNS-ответа и убедиться в том, что он также использует протокол UDP.

a. В данном примере соответствующим пакетом DNS-ответа является кадр 5. Обратите внимание на то, что количество байт на линии составляет 290. Этот пакет превышает по объёму пакет DNS- запроса.



b. Судя по кадру Ethernet II для DNS-ответа, с какого устройства получен MAC-адрес источника и какое устройство является MAC-адресом назначения?

c. Обратите внимание на IP-адреса источника и назначения в IP-пакете. Назовите IP-адрес назначения. Назовите IP-адрес источника.

IP-адрес назначения: IP-адрес источника:

Что произошло с ролями источника и назначения локального узла и шлюза по умолчанию?

d. В сегменте UDP роли номеров портов также изменились на противоположные. Номер порта

назначения — 52110. Номер порта 52110 — это тот же порт, который был сгенерирован локальным ПК при отправке DNS-запроса на DNS-сервер. Ваш локальный ПК ожидает DNS-ответа от этого порта.

Номер порта назначения — 53. DNS-сервер ожидает DNS-запроса от порта 53, а затем отправляет DNS-ответ с номером порта источника 53 создателю DNS-запроса.

При расширении DNS-запроса обратите внимание на преобразованные IP-адреса сайта www.google.com в разделе Ответы.

```
⊟ User Datagram Protocol, Src Port: domain (53), Dst Port: 52110 (52110)
    Source port: domain (53)
    Destination port: 52110 (52110)
    Length: 256
  ⊞ Checksum: 0xc4ca [validation disabled]
      [Good Checksum: False]
      [Bad Checksum: False]
⊟ Domain Name System (response)
    [Request In: 4]
    [Time: 0.010820000 seconds]
    Transaction ID: 0x3f76
  ⊞ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 5
    Authority RRs: 4
    Additional RRs: 4
  ⊞ Queries
  ⊟ Answers
    ⊞ www.google.com: type A, class IN, addr 74.125.227.84
    ⊞ www.google.com: type A, class IN, addr 74.125.227.80
    ⊞ www.google.com: type A, class IN, addr 74.125.227.81
    ⊞ www.google.com: type A, class IN, addr 74.125.227.82
    ⊞ www.google.com: type A, class IN, addr 74.125.227.83
  ⊟ Authoritative nameservers
    ⊞ google.com: type NS, class IN, ns ns1.google.com
    ⊞ google.com: type NS, class IN, ns ns2.google.com
    ⊞ google.com: type NS, class IN, ns ns3.google.com
    ⊞ google.com: type NS, class IN, ns ns4.google.com
  ⊟ Additional records
    ⊞ ns1.google.com: type A, class IN, addr 216.239.32.10
    ⊞ ns2.google.com: type A, class IN, addr 216.239.34.10
    ⊞ ns3.google.com: type A, class IN, addr 216.239.36.10
    ⊞ ns4.google.com: type A, class IN, addr 216.239.38.10
```

Вопросы на закрепление

В чём состоят преимущества использования протокола UDP вместо протокола TCP в качестве транспортного протокола для DNS?

Практическая работа : 17 изучение захваченных пакетов FTP и TFTP с помощью программы Wireshark

Топология — часть 1 (FTP)

В части 1 описывается захват пакетов FTP по протоколу TCP. В эту топологию входит компьютер с доступом в Интернет.

Топология — часть 2 (TFTP)

В части 2 описывается захват пакетов TFTP по протоколу UDP. У компьютера должно быть установлено как Ethernet-подключение, так и консольное подключение к коммутатору S1.

Таблица адресации (часть 2)

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
S1	VLAN 1	192.168.1.1	255.255.255.0	Недоступно
ПК-А	Сетевой адаптер	192.168.1.3	255.255.255.0	192.168.1.1

Задачи

Часть 1. Определение полей и принципа работы заголовков TCP с помощью функции захвата сеанса FTP программы Wireshark

Часть 2. Определение полей и принципа работы заголовков UDP с помощью функции захвата сеанса TFTP программы Wireshark

Исходные данные/сценарий

На транспортном уровне TCP/IP используются два протокола — TCP, описанный в документе RFC 761, и UDP, описанный в документе RFC 768. Оба протокола поддерживают обмен данными по протоколу верхнего уровня. Например, TCP используется для поддержки транспортного уровня, в том числе и протоколов HTTP и FTP. Протокол UDP обеспечивает поддержку транспортного уровня DNS (службы доменных имён), TFTP и других протоколов.

Примечание. Сетевые инженеры обязаны знать компоненты заголовков и принцип работы протоколов TCP и UDP.

В части 1 лабораторной работы вам необходимо с помощью бесплатной программы Wireshark собрать и проанализировать поля заголовков протокола TCP для передачи файлов по протоколу FTP между главным компьютером и анонимным FTP-сервером. Подключение к анонимному FTP-серверу и загрузка файла выполняются с помощью утилиты командной строки Windows. В части 2 лабораторной работы вам необходимо с помощью бесплатной программы Wireshark собрать и проанализировать поля заголовков протокола UDP для передачи файлов по протоколу TFTP между главным компьютером и коммутатором S1.

Примечание. В задании используется коммутатор Cisco Catalyst 2960s с операционной системой Cisco IOS версии 15.0(2) (образ lanbasek9). Можно использовать другие коммутаторы и версии ПО Cisco IOS. В зависимости от модели и версии Cisco IOS доступные команды и результаты их выполнения могут отличаться от представленных в лабораторных работах.

Примечание. Коммутатор необходимо очистить от данных и загрузочной конфигурации. Если вы не уверены, что сможете это сделать, обратитесь к инструктору.

Примечание. Часть 1 предполагает наличие компьютера с доступом в Интернет; Netlab для её выполнения не подходит. Задания в части 2 могут выполняться с использованием Netlab.

Необходимые ресурсы — часть 1 (FTP)

Один ПК (Windows 7, Vista или XP с доступом к командной строке, выходом в Интернет и установленной программой Wireshark).

Необходимые ресурсы — часть 2 (TFTP)

- 1 коммутатор (серия Cisco 2960, с программным обеспечением Cisco IOS версии 15.0(2), образ lanbasek9 или аналогичный)
- Один ПК (Windows 7, Vista или XP с установленными программой Wireshark и TFTP-сервером, например Tftpd32)
- Кабель для настройки устройств с операционной системой Cisco IOS через консольный порт.
- Кабель Ethernet, как показано в схеме топологии.

Часть 1: Определение полей и принципа работы заголовков TCP с помощью функции захвата сеанса FTP программы Wireshark

В части 1 вам необходимо с помощью программы Wireshark получить данные о сеансе FTP и изучить поля заголовков TCP.

Шаг 1: Начните захват данных программой Wireshark.

a. Закройте все ненужные сетевые приложения, например браузер, чтобы ограничить количество трафика во время захвата данных программой Wireshark.

b. Начните захват данных программой Wireshark.

Шаг 2: Загрузите файл справки Readme.

a. В окне командной строки введите **ftp ftp.cdc.gov.**

b. Подключитесь к FTP-узлу Центра по контролю и профилактике заболеваний (CDC), указав в качестве имени пользователя **anonymous** (пароль вводить не нужно).

c. Найдите и загрузите файл справки Readme.

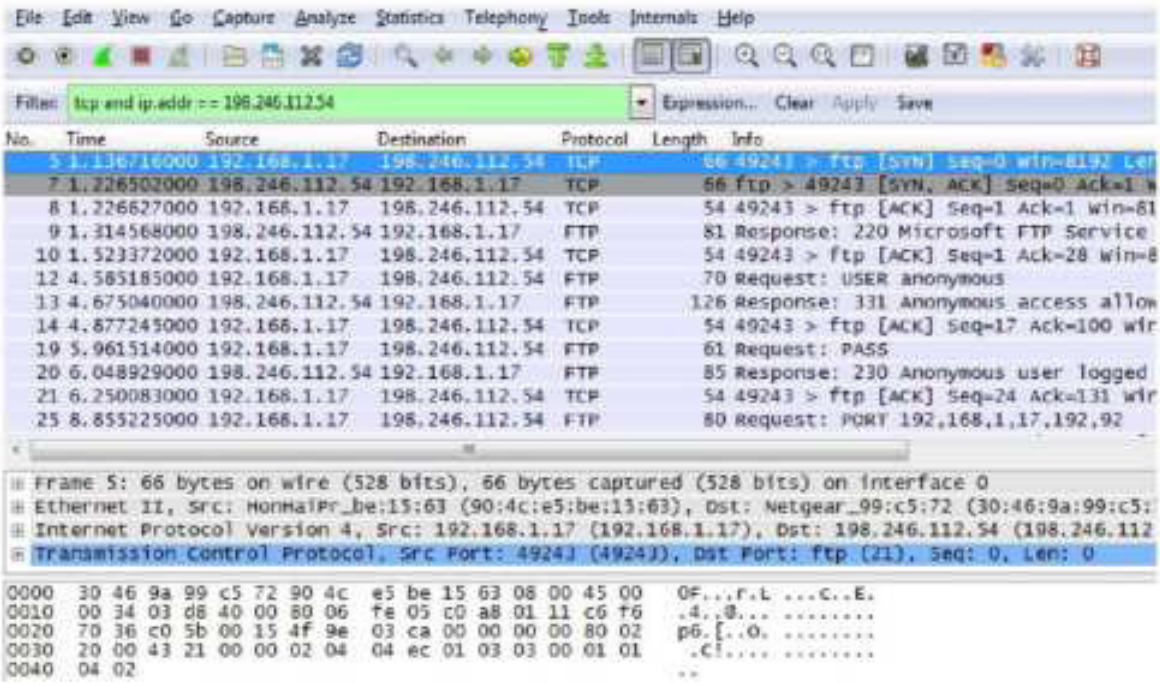
Практическая работа : изучение захваченных пакетов FTP и TFTP с помощью программы Wireshark

```
C:\Users\user1>ftp ftp.cdc.gov
Connected to ftp.cdc.gov.
220 Microsoft FTP Service
User (ftp.cdc.gov:(none)): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 Anonymous user logged in.
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection for file list.
aspnet_client
pub
Readme
Siteinfo
up.htm
w3c
web.config
welcome.msg
226 Transfer complete.
ftp: 76 bytes received in 0.00Seconds 19.00Kbytes/sec.
ftp> get Readme
200 PORT command successful.
150 Opening ASCII mode data connection for Readme(1428 bytes).
226 Transfer complete.
ftp: 1428 bytes received in 0.01Seconds 204.00Kbytes/sec.
ftp> quit
221
```

Шаг 3: Остановите сбор данных программой Wireshark.

Шаг 4: Откройте главное окно программы Wireshark.

Во время сеанса FTP-подключения к сайту ftp.cdc.gov программа Wireshark захватила большое число пакетов. Чтобы ограничить количество полученных данных для дальнейшего анализа, введите критерий **tcp and ip.addr == 198.246.112.54** в поле **Filter:** (Фильтр) и нажмите **Apply** (Применить) Введённый IP-адрес 198.246.112.54 — это адрес сайта ftp.cdc.gov.



Шаг 5: Проанализируйте поля TCP.

После применения фильтра TCP первые три кадра на панели списка пакетов (верхний раздел) отображают протокол транспортного уровня TCP, создающий надёжный сеанс связи. Последовательность [SYN], [SYN, ACK] и [ACK] иллюстрирует трёхстороннее рукопожатие.

5	1.138716000	192.168.1.17	198.246.112.54	TCP	66 49243 > ftp [SYN] Seq=0 Win=8192 L
7	1.226502000	198.246.112.54	192.168.1.17	TCP	66 ftp > 49243 [SYN, ACK] Seq=0 Ack=1
8	1.226627000	192.168.1.17	198.246.112.54	TCP	54 49243 > ftp [ACK] Seq=1 Ack=1 Win=

Протокол TCP регулярно используется во время сеанса связи для контроля доставки датаграмм, проверки их поступления и управления размером 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 главного компьютера и разверните строку TCP. Откроется показанная

```
⊞ Frame 5: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
⊞ Ethernet II, Src: HonHaiPr_be:15:63 (90:4c:e5:be:15:63), Dst: Netgear_99:c5:72 (30:46:9a:99:c5:72)
⊞ Internet Protocol Version 4, Src: 192.168.1.17 (192.168.1.17), Dst: 198.246.112.54 (198.246.112.54)
⊟ Transmission Control Protocol, Src Port: 49243 (49243), Dst Port: ftp (21), Seq: 0, Len: 0
    Source port: 49243 (49243)
    Destination port: ftp (21)
    [Stream index: 0]
    Sequence number: 0    (relative sequence number)
    Header length: 32 bytes
  ⊟ 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
    Window size value: 8192
    [Calculated window size: 8192]
  ⊞ Checksum: 0x4321 [validation disabled]
  ⊞ Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), Nc
```

ниже расширенная датаграмма TCP, подобная панели сведений о пакетах.

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

- Поле **Номер источника TCP** (TCP source port number) относится к узлу сеанса TCP, который установил подключение. Обычно используется произвольное значение больше 1023.
- Поле **TCP destination port number** (Номер порта назначения TCP) используется для идентификации протокола верхнего уровня или приложения на удалённом 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, такими как Telnet, FTP, HTTP и т. д.). Комбинация IP-адреса и порта источника и IP-адреса и порта назначения однозначно определяет сеанс как для отправителя, так и для получателя.

Примечание. В приведённых ниже данных, захваченных программой Wireshark, указан порт назначения 21, который используется для FTP. Через порт 21 FTP-серверы принимают пакеты, предназначенные для подключений FTP-клиента.

- В поле **Sequence number** (Порядковый номер) указывается номер последнего октета в сегменте.
- В поле **Acknowledgment number** (Номер подтверждения) указывается следующий октет, который ожидается получателем.
- Значение в поле **Code bits** (Кодовые биты) играет особую роль в управлении сеансами и обработке сегментов. Среди интересных значений можно привести следующие:

- ACK — подтверждение получения сегмента.
- SYN — синхронизация, устанавливается только в том случае, если новый сеанс TCP согласовывается в процессе трёхстороннего рукопожатия TCP.
- FIN — завершение, запрос о прекращении сеанса TCP.

- В поле **Window size** (Размер окна) отображается значение скользящего окна, которое определяет, сколько октетов могут быть отправлены до ожидания подтверждения.
- Поле **Urgent pointer** (Указатель важности) используется только с флагом срочности Urgent (URG), когда отправителю необходимо переслать важные данные на узел получателя.
- Для поля **Options** (Параметры) в настоящее время используется только один параметр, определяемый как максимальный размер TCP-сегмента (дополнительное значение).

Используя данные, захваченные программой Wireshark для запуска первого сеанса TCP (бит SYN установлен как 1), заполните информацию о заголовке TCP.

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

IP-адрес источника:	
IP-адрес назначения:	
Номер порта источника:	
Номер порта назначения:	
Порядковый номер:	
Номер подтверждения:	
Длина заголовка:	
Размер окна:	

Во втором окне отфильтрованных данных, захваченных программой Wireshark, FTP-сервер CDC подтверждает запрос, отправленный компьютером. Обратите внимание на значения битов для SYN и ACK.

```
⊞ Frame 7: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
⊞ Ethernet II, Src: Netgear_99:c5:72 (30:46:9a:99:c5:72), Dst: HonHaiPr_be:15:63 (90:4c:e5:be:15:63)
⊞ Internet Protocol Version 4, Src: 198.246.112.54 (198.246.112.54), Dst: 192.168.1.17 (192.168.1.17)
⊟ Transmission Control Protocol, Src Port: ftp (21), Dst Port: 49243 (49243), Seq: 0, Ack: 1, Len: 0
    Source port: ftp (21)
    Destination port: 49243 (49243)
    [Stream index: 0]
    Sequence number: 0    (relative sequence number)
    Acknowledgment number: 1    (relative ack number)
    Header length: 32 bytes
  ⊟ Flags: 0x012 (SYN, ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
    ⊞ .... .... ..1. = Syn: Set
      .... .... ...0 = Fin: Not set
    Window size value: 64240
    [Calculated window size: 64240]
  ⊞ Checksum: 0x05bb [validation disabled]
  ⊞ Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), N
  ⊞ [SEQ/ACK analysis]
```

Заполните приведённую ниже таблицу данными сообщения SYN-ACK.

IP-адрес источника:	
IP-адрес назначения:	
Номер порта источника:	
Номер порта назначения:	
Порядковый номер:	
Номер подтверждения:	
Длина заголовка:	
Размер окна:	

На последнем этапе согласования для установления связи компьютер отправляет серверу сообщение подтверждения. Обратите внимание на то, что только бит ACK имеет значение 1, в то время как значение Sequence number (Порядковый номер) увеличено до 1.

```
⊞ Frame 8: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
⊞ Ethernet II, Src: HonHaiPr_be:15:63 (90:4c:e5:be:15:63), Dst: Netgear_99:c5:72 (30:46:9a:99:c5:72)
⊞ Internet Protocol Version 4, Src: 192.168.1.17 (192.168.1.17), Dst: 198.246.112.54 (198.246.112.54)
⊟ Transmission Control Protocol, Src Port: 49243 (49243), Dst Port: ftp (21), Seq: 1, Ack: 1, Len: 0
    Source port: 49243 (49243)
    Destination port: ftp (21)
    [Stream index: 0]
    Sequence number: 1    (relative sequence number)
    Acknowledgment number: 1    (relative ack number)
    Header length: 20 bytes
  ⊟ Flags: 0x010 (ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
      .... .... ..0. = Syn: Not set
      .... .... ...0 = Fin: Not set
    Window size value: 8192
    [Calculated window size: 8192]
    [Window size scaling factor: 1]
  ⊞ Checksum: 0x2127 [validation disabled]
  ⊞ [SEQ/ACK analysis]
```

Заполните приведённую ниже таблицу данными сообщения ACK.

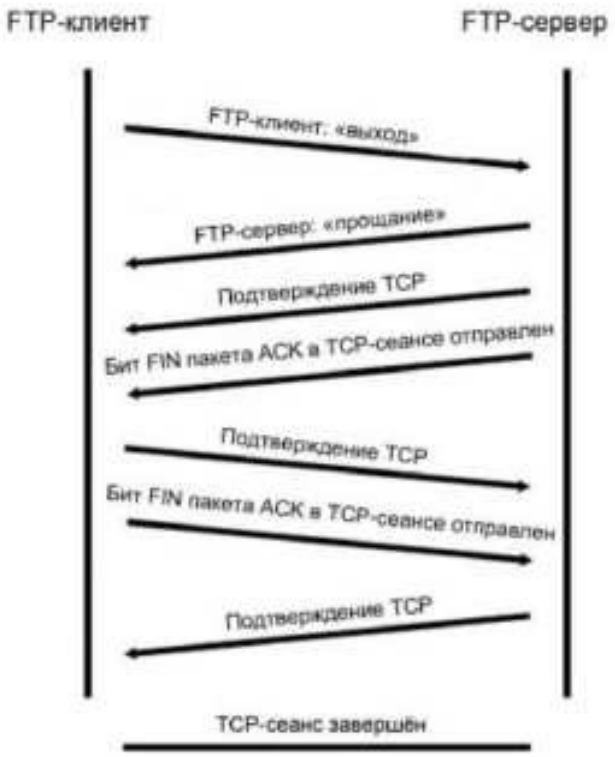
IP-адрес источника:	
IP-адрес назначения:	
Номер порта источника:	
Номер порта назначения:	
Порядковый номер:	
Номер подтверждения:	
Длина заголовка:	
Размер окна:	

Сколько других датаграмм TCP содержали бит SYN?

Как только сеанс TCP установлен, появляется возможность для передачи FTP-трафика между компьютером и FTP-сервером. FTP-клиент и сервер взаимодействуют друг с другом, не зная о том, что TCP контролирует сеанс и может им управлять. Когда FTP-сервер отправляет FTP-клиенту сообщение Response: 220, сеанс TCP на FTP-клиенте отправляет подтверждение сеансу TCP на сервере. Эту последовательность можно увидеть в приведенном ниже окне захвата данных программой Wireshark.

```
  9 1.314568000  198.246.112.54  192.168.1.17     FTP   81 Response: 220 Microsoft FTP Servic
 10 1.523372000  192.168.1.17    198.246.112.54   TCP   54 49243 > ftp [ACK] Seq=1 Ack=28 win
 12 4.585185000  192.168.1.17    198.246.112.54   FTP   70 Request: USER anonymous
 13 4.675040000  198.246.112.54  192.168.1.17     FTP  126 Response: 331 Anonymous access all

⊞ Frame 9: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface 0
⊞ Ethernet II, Src: Netgear_99:c5:72 (30:46:9a:99:c5:72), Dst: HonHaiPr_be:15:63 (90:4c:e5:be:15:63)
⊞ Internet Protocol Version 4, Src: 198.246.112.54 (198.246.112.54), Dst: 192.168.1.17 (192.168.1.17)
⊞ Transmission Control Protocol, Src Port: ftp (21), Dst Port: 49243 (49243), Seq: 1, Ack: 1, Len: 27
⊟ File Transfer Protocol (FTP)
  ⊟ 220 Microsoft FTP Service\r\n
      Response code: Service ready for new user (220)
      Response arg: Microsoft FTP Service
```

Когда сеанс FTP завершается, FTP-клиент отправляет команду quit (завершить). FTP-сервер подтверждает прекращение сеанса FTP, отправляя ответ Response: 221 Goodbye. В этот раз сеанс TCP FTP-сервера отправляет датаграмму TCP FTP-клиенту, сообщая о прекращении сеанса TCP. Сеанс TCP FTP-клиента подтверждает получение датаграммы прекращения, после чего отправляет собственное сообщение о прекращении сеанса TCP. Получив копию сообщения о прекращении, FTP- сервер, инициировавший прекращение сеанса TCP, отправляет датаграмму ACK с подтверждением прекращения, и сеанс TCP завершается. Эту последовательность можно увидеть в приведённой ниже схеме и результатах захвата данных.



Применение фильтра **ftp** позволяет изучить всю последовательность трафика FTP с помощью программы Wireshark. Обратите внимание на последовательность событий во время этого сеанса FTP. Для загрузки файла справки Readme было использовано имя пользователя anonymous. По окончании передачи файлов пользователь завершил сеанс FTP.

Filter: ftp Expression... Clear Apply Save

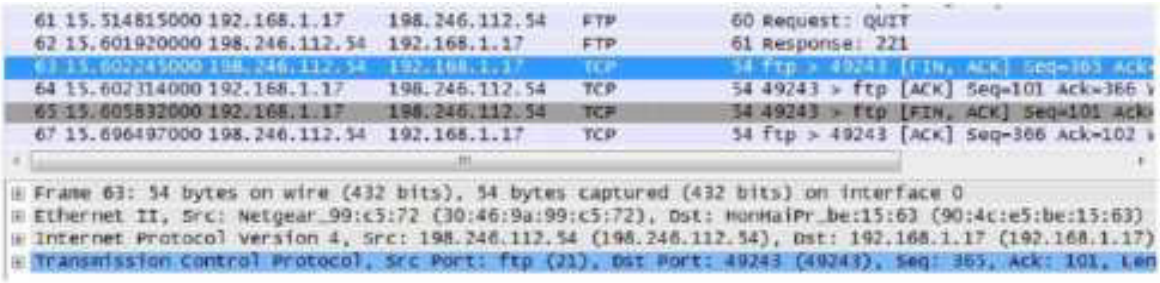
No.	Time	Source	Destination	Protocol	Length	Info
9	1.314568000	198.246.112.54	192.168.1.17	FTP	81	Response: 220 Microsoft FTP Service
12	4.585165000	192.168.1.17	198.246.112.54	FTP	70	Request: USER anonymous
13	4.675040000	198.246.112.54	192.168.1.17	FTP	126	Response: 331 Anonymous access allowe
19	5.961514000	192.168.1.17	198.246.112.54	FTP	61	Request: PASS
20	6.048929000	198.246.112.54	192.168.1.17	FTP	85	Response: 230 Anonymous user logged i
25	8.855223000	192.168.1.17	198.246.112.54	FTP	80	Request: PORT 192,168,1,17,192,92
26	8.945530000	198.246.112.54	192.168.1.17	FTP	84	Response: 200 PORT command successful
27	8.955549000	192.168.1.17	198.246.112.54	FTP	60	Request: NLST
29	9.053034000	198.246.112.54	192.168.1.17	FTP	109	Response: 150 Opening ASCII mode data
39	9.347432000	198.246.112.54	192.168.1.17	FTP	78	Response: 226 Transfer complete.
42	12.621720000	192.168.1.17	198.246.112.54	FTP	80	Request: PORT 192,168,1,17,192,93
43	12.709658000	198.246.112.54	192.168.1.17	FTP	84	Response: 200 PORT command successful
44	12.722592000	192.168.1.17	198.246.112.54	FTP	67	Request: RETR Readme
45	12.811097000	198.246.112.54	192.168.1.17	FTP	118	Response: 150 Opening ASCII mode data
58	13.107294000	198.246.112.54	192.168.1.17	FTP	78	Response: 226 Transfer complete.
61	15.514815000	192.168.1.17	198.246.112.54	FTP	60	Request: QUIT
62	15.601920000	198.246.112.54	192.168.1.17	FTP	61	Response: 221

Практическая работа : изучение захваченных пакетов FTP и TFTP с помощью программы Wireshark

Ещё раз примените фильтр TCP программы Wireshark, чтобы изучить процесс прекращения сеанса TCP. Для завершения сеанса TCP передаются четыре пакета. Поскольку подключение TCP является полнодуплексным, для каждого направления требуется отдельное прекращение сеанса. Изучите адреса источника и назначения.

В этом примере у FTP-сервера больше нет данных для отправки в потоке; он отправляет сегмент с флагом завершения FIN, установленным в кадре 63. Компьютер отправляет ACK, чтобы подтвердить получение FIN для завершения сеанса связи между сервером и клиентом в кадре 64.

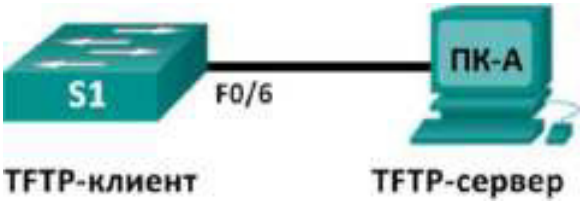
В кадре 65 компьютер посылает FIN FTP-серверу, чтобы завершить сеанс TCP. FTP-сервер отправляет ответ, содержащий ACK в кадре 67, чтобы подтвердить получение FIN от компьютера. После этого сеанс TCP между FTP-сервером и компьютером завершается.



Часть 2: Определение полей и принципа работы заголовков UDP с помощью функции захвата сеанса TFTP программы Wireshark

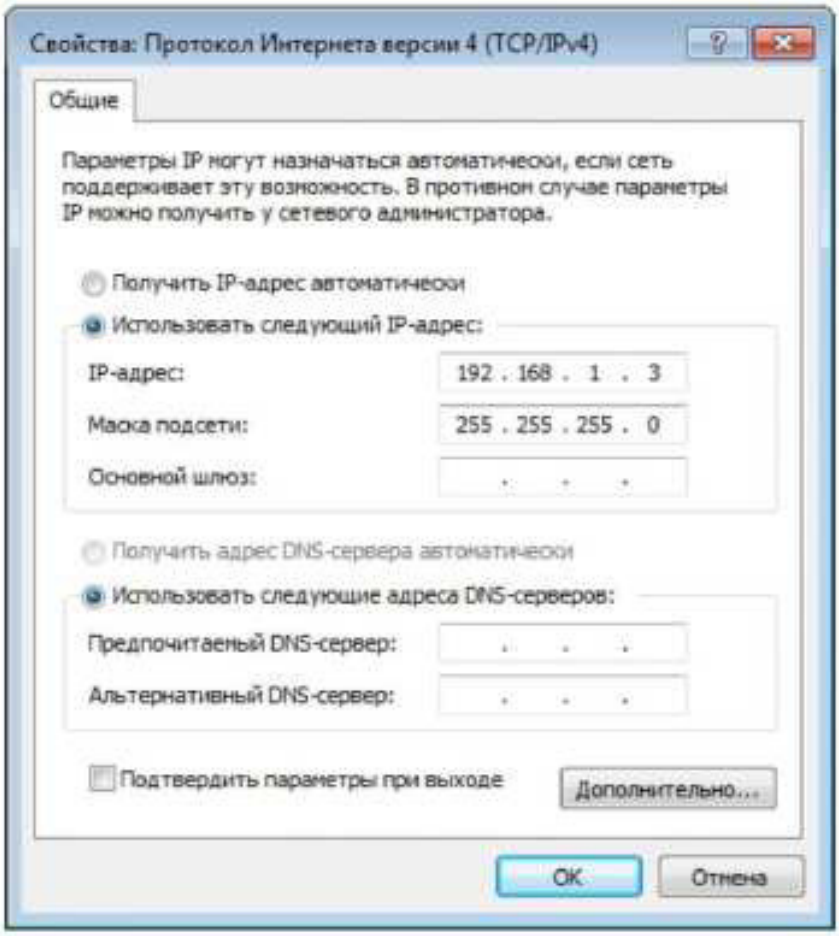
В части 2 вам необходимо с помощью программы Wireshark получить данные о сеансе TFTP и изучить поля заголовков UDP.

Шаг 1: Постройте физическую топологию сети и подготовьте всё необходимое для захвата данных о сеансе TFTP.



a. Установите между компьютером ПК-А и коммутатором S1 Ethernet-подключение и подключение через консоль.

b. Если это ещё не сделано, укажите IP-адрес компьютера (192.168.1.3) вручную. Для настройки шлюза по умолчанию это не требуется.



c. Настройте коммутатор. Для сети VLAN 1 укажите IP-адрес 192.168.1.1. Проверьте подключение к компьютеру, отправив эхо-запрос с помощью команды ping на адрес 192.168.1.3. При необходимости устраните неполадки.

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#host S1
S1(config)#interface vlan 1
S1(config-if)#ip address 192.168.1.1 255.255.255.0
S1(config-if)#no shut
*Mar  1 00:37:50.166: %LINK-3-UPDOWN: Interface Vlan1, changed state to up
*Mar  1 00:37:50.175: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1,
changed state to up
S1(config-if)# end
S1# ping 192.168.1.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/203/1007 ms
```

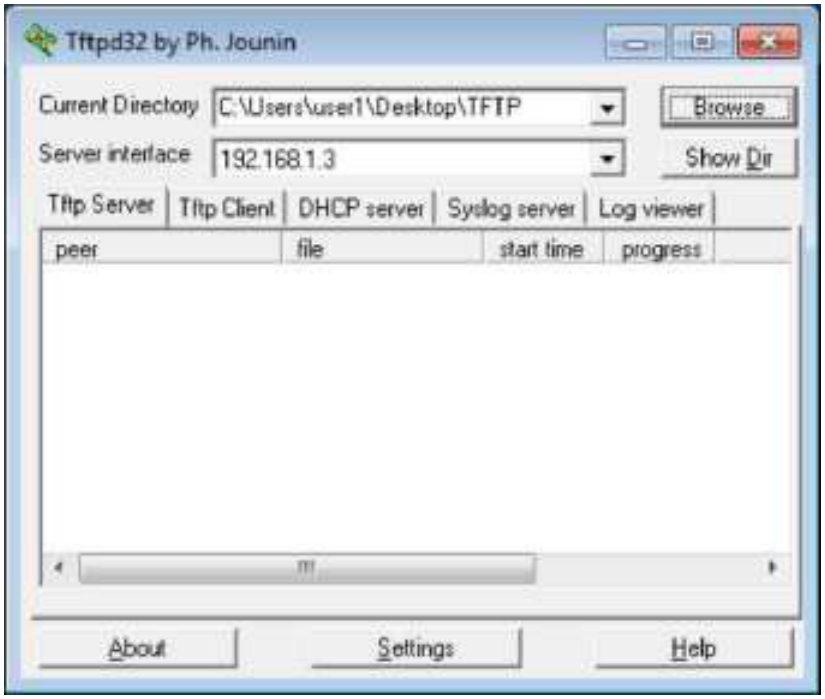
Шаг 2: Подготовьте TFTP-сервер на компьютере.

a. На рабочем столе создайте папку **TFTP,** если такой ещё нет. В неё будут скопированы файлы с коммутатора.

b. На компьютере запустите программу **Tftpd32.**

c. Нажмите кнопку **Browse** (Обзор) и вместо выбранной папки укажите **C:\Users\user1\Desktop\TFTP,** заменив user1 на своё имя пользователя.

TFTP-сервер должен иметь следующий вид:



Обратите внимание на то, что в поле Current Directory (Текущий каталог) указаны пользователь и интерфейс сервера Server (ПК-А) в виде IP-адреса **192.168.1.3.**

d. Проверьте возможность копирования файлов с коммутатора на компьютер с помощью TFTP. При необходимости устраните неполадки.

```
S1# copy start tftp
Address or name of remote host []? 192.168.1.3
Destination filename [s1-confg]?
!!
1638 bytes copied in 0.026 secs (63000 bytes/sec)
```

Если вы видите, что файл скопирован (как в приведённом выше примере), переходите к следующему шагу. В противном случае устраните неполадки. Если появится сообщение об ошибке `%Error opening tftp (Permission denied)` (%Невозможно открыть tftp (нет прав доступа)), проверьте, не блокирует ли ваш межсетевой экран протокол TFTP, и убедитесь в том, что копирование выполняется в папку с правами доступа для вашего имени пользователя, например, в папку на рабочем столе.

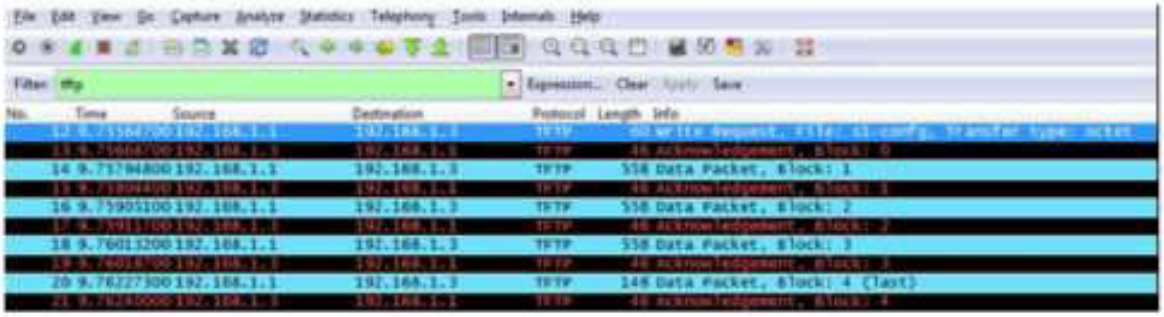
Шаг 3: Захватите данные о сеансе TFTP с помощью программы Wireshark.

a. Откройте Wireshark. В меню **Edit** (Правка) выберите пункт **Preferences** (Установки) и нажмите на значок «плюс» (+), чтобы раскрыть меню **Protocols** (Протоколы). Прокрутите экран вниз и выберите **UDP.** Установите флажок **Validate the UDP checksum if possible** (Проверять контрольную сумму UDP, если возможно) и нажмите **Apply** (Применить). Затем нажмите кнопку **OK.**

b. Начните захват данных программой Wireshark.

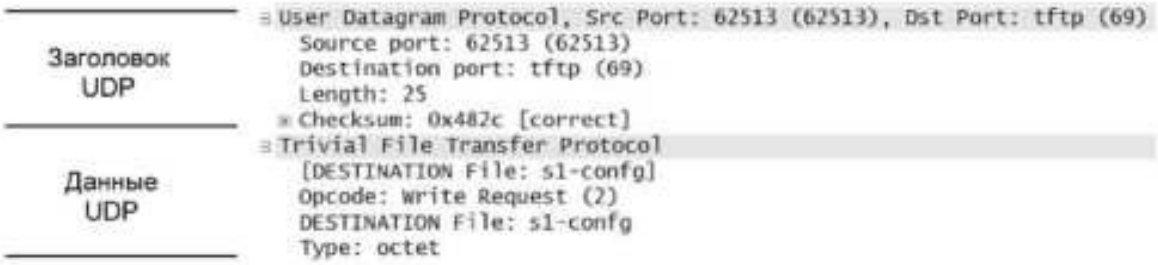
c. На коммутаторе введите команду `copy start tftp.`

d. Остановите сбор данных программой Wireshark.



e. Для фильтра выберите значение **tftp.** Полученные результаты должны выглядеть примерно так, как показано выше. Эта передача TFTP используется для анализа работы UDP транспортного уровня.

Программа Wireshark отображает подробные данные UDP на панели сведений о пакетах. Выделите первую датаграмму UDP, полученную с главного компьютера, и наведите указатель мыши на панель сведений о пакетах. При необходимости скорректируйте эту панель и разверните строку UDP, нажав на соответствующее поле. Расширенная датаграмма UDP должна выглядеть подобно приведённой ниже схеме.



На приведённ атаграммой
TCP информа мма UDP
обозначается

СЕГМЕНТ UDP

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

Используя данные, захваченные программой Wireshark для первой датаграммы UDP, заполните информацию о заголовке UDP. Значение контрольной суммы имеет формат шестнадцатеричного числа (основание 16) с предшествующим кодом 0x.

IP-адрес источника:	
IP-адрес назначения:	
Номер порта источника:	
Номер порта назначения:	
Длина сообщения UDP:	
Контрольная сумма UDP:	

Как протокол UDP проверяет правильность датаграммы?

Изучите первый кадр, возвращённый TFTPD-сервером. Заполните приведённую ниже таблицу данными заголовка UDP.

IP-адрес источника:	
IP-адрес назначения:	
Номер порта источника:	
Номер порта назначения:	
Длина сообщения UDP:	
Контрольная сумма UDP:	

```
-User Datagram Protocol, Src Port: 58565 (58565), Dst Port: 62513 (62513) Ш Checksum: 0x8372 [incorrect, should be 0xa385

(maybe caused by "UDP checksum offload"?)]
```

Обратите внимание на то, что в возвращённой датаграмме UDP указывается другой порт источника UDP, который, однако, используется до конца пересылки данных по TFTP. Поскольку надёжное соединение отсутствует, для пересылки данных по TFTP используется только исходный порт источника, предназначенный для начала сеанса TFTP.

Кроме того, необходимо учитывать, что значение в поле UDP Checksum (Контрольная сумма UDP) указано неверно. Скорее всего, это вызвано выгрузкой контрольной суммы UDP (UDP checksum offload). Дополнительную информацию о причинах этого явления можно найти в Интернете, выполнив поиск по словам «UDP checksum offload» или «выгрузка контрольной суммы UDP».

Вопросы на закрепление

В ходе лабораторной работы вы получили возможность проанализировать функциональные особенности протоколов TCP и UDP, используя захват данных во время сеансов FTP и TFTP. Чем управление соединением с помощью TCP отличается от UDP?

Проблема

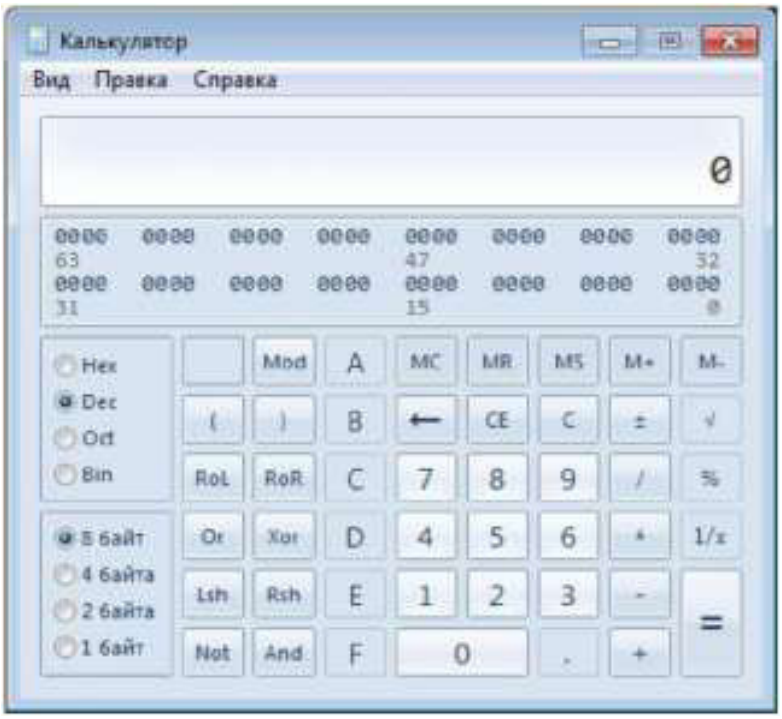
Так как ни FTP, ни TFTP не являются безопасными протоколами, все данные пересылаются в виде открытого текста. Сюда входят все идентификаторы пользователей, пароли и содержание текстовых файлов. Анализ сеанса FTP верхнего уровня позволит быстро определить идентификатор и пароль пользователя, а также пароли файла конфигурации. Получить доступ к данным TFTP верхнего уровня и извлечь идентификатор и пароль пользователя конфигурации сложнее, но тоже можно.

Очистка

Если инструктор не дал иные инструкции, выполните следующие действия:

1) Удалите файлы, скопированные на ваш ПК.
2) Удалите параметры конфигурации на коммутаторе **S1.**
3) Удалите введённый вручную IP-адрес с ПК и восстановите подключение к Интернету.

Практическая работа 18: использование калькулятора Windows в работе с сетевыми адресами



Задачи

Часть 1. Доступ к калькулятору Windows

Часть 2. Перевод чисел из одной системы счисления в другую

Часть 3. Перевод ^4-адресов узлов и масок подсети в двоичную систему счисления

Часть 4. Определение количества узлов в сети с помощью двух цифр

Часть 5. Преобразование MAC- и ^6-адресов в двоичную форму

Исходные данные/сценарий

При работе с компьютерами и сетевыми устройствами сетевые специалисты используют двоичные, десятичные и шестнадцатеричные числа. В операционную

систему компании Microsoft входит встроенный калькулятор. Версия калькулятора в ОС Windows 7 включает обычный режим, который можно использовать для выполнения простейших арифметических задач, например сложения, вычитания, умножения и деления, а также расширенные возможности для программных, научных и статистических расчётов.

В данной лабораторной работе вы будете переводить числа в двоичную, десятичную и шестнадцатеричную системы счисления и обратно в режиме «Программист» калькулятора ОС Windows 7 и определять количество узлов, к которым можно обратиться, исходя из количества доступных узловых бит, в режиме «Инженерный».

Необходимые ресурсы

• Один ПК (Windows 7, Vista или XP)

Примечание. В других операционных системах, отличных от Windows 7, функционал калькулятора для программистов может выглядеть иначе, чем в данной лабораторной работе. Произведение расчётов при этом возможно.

Часть 1: Доступ к калькулятору Windows

В части 1 вы познакомитесь с встроенным приложением калькулятора Microsoft Windows и изучите доступные режимы.

Шаг 1: Нажмите кнопку Пуск в ОС Windows и выберите пункт «Все программы».

Шаг 2: Откройте папку «Стандартные» и нажмите на «Калькулятор».

Шаг 3: Когда калькулятор откроется, выберите меню «Вид».

Какие четыре режима доступны?

Примечание. В данной лабораторной работе используются режимы «Программист» и «Инженерный».

Часть 2: Перевод чисел из одной системы счисления в другую

В режиме «Программист» калькулятора Windows доступны несколько систем счисления: Hex (шестнадцатеричная с основанием 16), Dec (десятичная с основанием 10), Ой (восьмеричная с основанием 8) и Bin (двоичная с основанием 2).

Мы привыкли использовать десятичную систему счисления с цифрами от 0 до 9. Она применяется в повседневной жизни для всех подсчётов и финансовых операций. Компьютеры и прочие электронные устройства для хранения и передачи данных, а также числовых вычислений, используют двоичную систему, состоящую только из нулей и единиц. Все компьютерные расчёты выполняются в двоичной (цифровой) форме, независимо от того, в каком виде они отображаются.

Недостаток этой системы в том, что двоичный эквивалент большого десятичного числа может быть очень длинным. Это усложняет чтение и написание чисел. Один из способов решения этой проблемы — организация двоичных чисел в группы по четыре шестнадцатеричных числа. Шестнадцатеричные числа имеют основание 16, а для представления двоичных или десятичных эквивалентов используется комбинация цифр от 0 до 9 и букв от A до F. Шестнадцатеричные символы используются при записи или отображении IPv6- и MAC-адресов.

Восьмеричная система счисления мало чем отличается от шестнадцатеричной. Восьмеричные числа представляют собой двоичные числа в группах по три цифры. В этой системе счисления используются цифры от 0 до 7. Восьмеричные числа — это ещё один удобный способ представления большого двоичного числа маленькими группами, однако данная система счисления не так распространена.

В этой лабораторной работе калькулятор Windows 7 используется для перевода чисел между различными системами счисления в режиме «Программист».

a. Откройтеменю **Вид** и выберите режим **Программист.**

Примечание. В Windows XP и Vista доступны только два режима — «Обычный» и «Инженерный». Для выполнения лабораторной работы в такой операционной системе подойдёт режим «Инженерный».

Какая система счисления используется в данный момент?

Какие цифры на цифровой клавиатуре активны в десятичном режиме?

b. Установите переключатель **Bin** (Двоичная система). Какие цифры на цифровой клавиатуре активны теперь?

Почему другие цифры недоступны?

c. Установите переключатель **Hex** (Шестнадцатеричная система). Какие символы на цифровой клавиатуре активны теперь?

d. Установите переключатель **йес**(Десятичная система). С помощью мыши нажмите на цифру **1,** а затем — на цифру **5**на цифровой клавиатуре. Вы ввели десятичное число 15.

Примечание. Для ввода значений можно также использовать цифры и буквы на клавиатуре. Если вы пользуетесь вспомогательной цифровой клавиатурой, введите число **15.** Если число не появляется в поле калькулятора, нажмите клавишу **Num Lock,** чтобы включить вспомогательную цифровую клавиатуру.

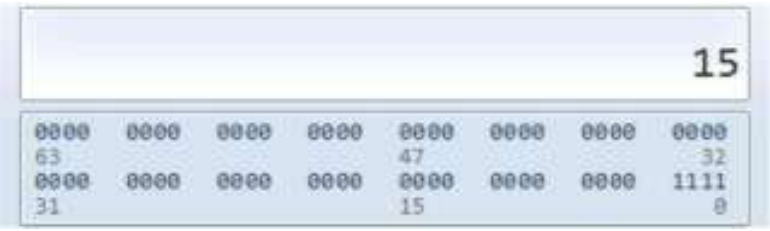
Установите переключатель **Bin** (Двоичная система). Что случилось с числом 15?

e. Числа переводятся из одной системы счисления в другую путём выбора нужного режима. Снова установите переключатель **Dec** (Десятичная система). Число будет снова конвертировано

в десятичный формат.

f. Установите переключатель **Hex,** чтобы включить режим шестнадцатеричной системы. Какой шестнадцатеричный символ (от 0 до 9 и от A до F) соответствует десятичному числу 15?

g. Переключаясь между системами счисления, вы могли заметить, что во время преобразования отображалось двоичное число 1111. Это позволяет соотносить двоичные числа со значениями в других системах счисления. Каждый набор из четырёх бит представляет шестнадцатеричный символ или несколько десятичных символов.



h. Сотрите значение в окне, нажав на кнопку **C** над цифрой 9 на клавиатуре калькулятора.

Переведите в двоичную, десятичную и шестнадцатеричную системы счисления следующие числа:

Десятичное	Двоичное	Шестнадцатеричное
86		
175		
204		
	0001 0011	
	0100 1101	
	0010 1010	
		38
		93
		E4

i. Заполняя приведённую выше таблицу, заметили вы что-либо общее между двоичными и шестнадцатеричными числами?

Часть 3: Перевод ^4-адресов узлов и масок подсети в двоичную систему счисления

^4-адреса и маски подсети выражаются в десятичном формате с точкой-разделителем (четыре октета), например 192.168.1.10 и 255.255.255.0 соответственно. Так людям легче их читать. Каждый десятичный октет в адресе или маске можно преобразовать в 8 двоичных разрядов. Октет всегда представляет собой 8 двоичных битов. Если все 4 октета преобразовать в двоичную форму, сколько разрядов получится?

a. С помощью калькулятора Windows переведите IP-адрес 192.168.1.10 в двоичный формат и запишите его в следующую таблицу:

Десятичное	Двоичное
192	
168	
1	
10	

b. Маски подсетей, такие как 255.255.255.0, также отображаются в десятичном формате с точкой- разделителем. Маска подсети всегда состоит из четырёх 8-разрядных октетов, каждый из которых выражается десятичным числом. С помощью калькулятора Windows преобразуйте восемь возможных десятичных значений октетов маски подсети в двоичные числа и запишите их в следующую таблицу:

Десятичное	Двоичное
0	
128	
192	
224	
240	
248	
252	
254	
255	

с. Используя комбинацию ^4-адреса и маски подсети, можно определить сетевую часть

и рассчитать количество узлов, доступных в данной ^4-подсети. Этот процесс рассматривается в части 4.

Часть 4: Определение количества узлов в сети с помощью двух цифр

С адресом ^4-сети и маской подсети можно определить сетевую часть, а также количество доступных в сети узлов.

а. Чтобы вычислить количество узлов в сети, необходимо определить сетевую и узловую части адреса.

Адрес и маска подсети переводятся в двоичные числа на примере адреса 192.168.1.10 с подсетью 255.255.248.0. Записывая результаты перевода данных в двоичные числа, выставляйте биты.

IP-адрес и маска подсети в десятичном формате	IP-адрес и маска подсети в двоичном формате
192.168.1.10	
255.255.248.0	

Поскольку первые 21 бит в маске подсети представляют собой идущие подряд единицы, соответствующие 21 бит IP-адреса в двоичном формате выглядят как 110000001010100000000 и соответствуют сетевой части адреса. Остальные 11 бит имеют вид 00100001010 — это узловая часть адреса.

Назовите десятичный и двоичный номера сети для данного адреса.

Назовите десятичную и двоичную узловые части для данного адреса.

Поскольку номер сети и широковещательный адрес используют два адреса из подсети, для определения количества доступных узлов в ^4-подсети нужно цифру 2 произвести в степень количества узловых битов и вычесть 2.

Количество доступных узлов = $2^{(\text{число битов узла})}$- 2

b. На калькуляторе Windows переключитесь в режим «Инженерный», открыв меню **Вид** и выбрав параметр **Инженерный.**

c. Введите число **2.**Нажмите кнопку**x^y.** Эта команда возводит число в степень.

d. Введите число **11**.Нажмите=или клавишу ВВОД на клавиатуре, чтобы получить результат.

e. Из результата вычтите**2,** при желании используя калькулятор.

11

f. В данной сети доступны примерно 2046 узлов (2 -2).

g. Зная количество узловых битов, определите количество доступных узлов и запишите это значение в приведённую ниже таблицу.

Количество доступных узловых битов	Количество доступных узлов
5	
14	
24	
10	

h. Для данной маски подсети определите количество доступных узлов и запишите ответ в приведённую ниже таблицу.

Маска подсети	Двоичная маска подсети	Количество доступных узловых битов	Количество доступных узлов
255.255.255.0	11111111.11111111.11111111.00000000		
255.255.240.0	11111111.11111111.11110000.00000000		
255.255.255.128	11111111.11111111.11111111.10000000		
255.255.255.252	11111111.11111111.11111111.11111100		
255.255.0.0	11111111.11111111.00000000.00000000		

Часть 5: Преобразование MAC- и ^6-адресов в двоичную форму

Для удобства адреса управления доступом к среде передачи данных (MAC) и адреса интернет- протокола версии 6 (IPv6) выражаются шестнадцатеричными цифрами. Однако компьютеры способны распознавать и используют для вычислений только двоичные цифры. В этой части занятия вам предстоит перевести шестнадцатеричные адреса в двоичные.

Шаг 1: Переведите MAC-адреса в двоичные числа.

a. MAC-адрес (или физический адрес) обычно выражается 12 шестнадцатеричными цифрами, сгруппированными в пары и разделёнными дефисами (-). В компьютерах на базе ОС Windows физические адреса обычно имеют формат xx-xx-xx-xx-xx-xx, где x — это цифра от 0 до 9 или латинская буква от A до F. Каждую шестнадцатеричную цифру в адресе можно конвертировать в четыре двоичных разряда, понятных компьютеру. Если все 12 шестнадцатеричных цифр перевести в двоичную форму, сколько разрядов получится?

b. Запишите MAC-адрес своего ПК.

c. С помощью калькулятора Windows переведите MAC-адрес в двоичное число.

Шаг 2: Переведите IPve-адрес в двоичное число.

Для удобства ^6-адреса также записывают шестнадцатеричными символами. Для компьютеров эти ^6-адреса можно переводить в двоичные цифры.

a. ^6-адреса — это двоичные числа, представленные в виде понятной для человека записи: 2001:0DB8:ACAD:0001:0000:0000:0000:0001 или в короткой форме: 2001:DB8:ACAD:1::1.

.Шестнадцатеричное	Двоичное
2001	
0DB8	
ACAD	
0001	
0000	
0000	
0000	
0001	

Вопросы на закрепление

1. Можете ли вы выполнить все эти операции без помощи калькулятора? Что для этого требуется?

2. В большинстве ^6-адресов длина сетевой части составляет 64 бита. Сколько узлов доступно в подсети, где первые 64 бита соответствуют сети? Подсказка: для узлов подсети доступны все узловые адреса.

Практическая работа . Преобразование!Ру4-адресов в двоичный формат

Задачи

Часть 1. Преобразование !Ру4-адресов из разделенных точками десятичных чисел в двоичный формат

Часть 2. Использование побитовой операции И для определения сетевых адресов Часть 3. Применение расчетов сетевых адресов

Общие сведения/сценарий

Каждый Р4-адрес состоит из двух частей — сетевой и узловой. Сетевая часть адреса одинакова для всех устройств, которые находятся в одной и той же сети. Узловая часть определяет конкретный узел в пределах соответствующей сети. Маска подсети используется для определения сетевой части IP- адреса. Устройства в одной сети могут обмениваться данными напрямую; для взаимодействия между устройствами из разных сетей требуется промежуточное устройство уровня 3, например маршрутизатор.

Чтобы понять принцип работы устройств в сети, нам необходимо увидеть адреса в том виде, в котором с ними работают устройства — в двоичном представлении. Для этого необходимо перевести IP-адрес и его маску подсети из десятичного представления с точками в двоичное значение. После этого можно определить сетевой адрес с помощью побитовой операции И.

В этой лабораторной работе описывается порядок определения сетевой и узловой частей IP-адресов. Для этого нужно перевести адреса и маски подсети из десятичного представления с точками в двоичный формат, а затем применить побитовую операцию И. После этого вы воспользуетесь полученной информацией для определения адресов в сети.

Часть 1: Преобразование !Ру4-адресов из десятичной системы счисления с точкой -разделителем в двоичный формат

В части 1 вам необходимо перевести десятичные числа в двоичный эквивалент. Выполнив это задание, вы займетесь преобразованием !Ру4-адресов и масок подсети из десятичного представления с точкой-разделителем в двоичную систему.

Шаг 1: Переведите числа из десятичной в двоичную систему счисления.

Заполните таблицу, преобразовав десятичное число в 8-битное двоичное значение. Первое число уже преобразовано для примера. Помните, что восемь двоичных битовых значений в октете имеют основание 2 и слева направо выглядят как 128, 64, 32, 16, 8, 4, 2 и 1.

Десятичные	Двоичные
192	11000000
168	10101000 101 0 11111111
10	
255	
2	10

Шаг 2: Преобразуйте !Ру4-адреса в двоичный формат.

!Ру4-адреса преобразуются точно так же, как было описано выше. Заполните приведенную ниже таблицу двоичными эквивалентами указанных адресов. Чтобы ваши ответы было проще воспринимать, разделяйте двоичные октеты точками.

Десятичные	Двоичные
192.168.10.10	11000000.10101000.00001010.00001010
209.165.200.229	11010001.10100101.11001000.11100101
172.16.18.183	10101100.00010000.00010010.10110111
10.86.252.17	00001010.01010110.11111100.00010001
255.255.255.128	11111111.11111111.11111111.10000000
255.255.192.0	11111111.11111111.110 0 0 0 0 0.0 0 0 0 0 0 0 0

Часть 2: Использование побитовой операции И для определения сетевых адресов

В части 2 вы будете рассчитывать сетевой адрес для имеющихся адресов узлов с помощью побитовой операции И. Сначала вам необходимо перевести десятичный Р4-адрес и маску подсети в их двоичный эквивалент. Получив сетевой адрес в двоичном формате, переведите его в десятичный.

Примечание. При использовании операции И десятичное значение в каждой битовой позиции 32- битного IP-адреса узла сравнивается с

соответствующей позицией в 32-битной маске подсети. При наличии двух нулей или 0 и 1 результатом операции И будет 0. При наличии двух единиц результатом будет 1, как показано в приведенном примере.

Шаг 1: Определите, сколько бит нужно использовать для расчета сетевого адреса.

Описание	Десятичные	Двоичные
IP-адрес	192.168.10.131	11000000.10101000.00001010.10000011
Маска подсети	255.255.255.192	11111111.11111111.11111111.11000000
Сетевой адрес	192.168.10.128	11000000.10101000.00001010.10000000

Как определить, сколько бит нужно использовать для расчета сетевого адреса?

Перевести маску подсети в двоичный вид и посчитать количество единиц.

Сколько бит в приведенном выше примере используется для расчета сетевого адреса? 2 6

Шаг 2: Выполните операцию И, чтобы определить сетевой адрес.

a. Введите отсутствующую информацию в таблицу ниже:

Описание	Десятичные	Двоичные
IP-адрес	172.16.145.29	10101100.00010000.10010001.00011101
Маска подсети	255.255.0.0	11111111.11111111.00000000.00000000
Сетевой адрес	172.16.0.0	10101100.00010000.00000000.00000000

b. Введите отсутствующую информацию в таблицу ниже:

Описание	Десятичные	Двоичные
IP-адрес	192.168.10.10	11000000.10101000.00001010.00001010
Маска подсети	255.255.255.0	11111111.11111111.11111111.00000000
Сетевой адрес	192.168.10.0	11000000.10101000.00001010.00000000

c. Введите отсутствующую информацию в таблицу ниже:

Описание	Десятичные	Двоичные
IP-адрес	192.168.68.210	11000000.10101000.01000100.11010010
Маска подсети	255.255.255.128	11111111.11111111.11111111.10000000
Сетевой адрес	192.168.68.128	11000000.10101000.01000100.10000000

d. Введите отсутствующую информацию в таблицу ниже:

Описание	Десятичные	Двоичные
IP-адрес	172.16.188.15	10101100.00010000.10111100.00001111
Маска подсети	255.255.240.0	11111111.11111111.11110000.00000000
Сетевой адрес	172.16.176.0	10101100.00010000.10110000.00000000

e. Введите отсутствующую информацию в таблицу ниже:

Описание	Десятичные	Двоичные
IP-адрес	10.172.2.8	00001010.10101100.00000010.00001000
Маска подсети	255.224.0.0	11111111.11100000.00000000.00000000
Сетевой адрес	10.160.0.0	00001010.10100000.00000000.00000000

Часть 3: Применение расчетов сетевых адресов

В части 3 вам необходимо рассчитать сетевой адрес для указанных IP-адресов и масок подсети. Получив сетевой адрес, вы должны определить ответы, необходимые для выполнения этой лабораторной работы.

Шаг 1: Определите, находятся ли IP-адреса в одной и той же сети.

a. Вы настраиваете два ПК для своей сети. Компьютеру PC-A присвоен IP-адрес 192.168.1.18, а компьютеру PC-B — IP-адрес 192.168.1.33. Маска подсети обоих компьютеров — 255.255.255.240.

Какой сетевой адрес у PC-A? 192.168.1.16 Какой сетевой адрес у PC-B? . 1912.166.1.32

Смогут ли эти ПК взаимодействовать друг с другом напрямую? Нет, они находятся в разных подсетях.

Какой наибольший адрес, присвоенный компьютеру PC-B, позволит ему находиться в одной сети с PC-A? 192.168.1.224

b. Вы настраиваете два ПК для своей сети. Компьютеру PC-A присвоен IP-адрес 10.0.0.16, а компьютеру PC-B — IP-адрес 10.1.14.68. Маска подсети обоих компьютеров — 255.254.0.0.

Какой сетевой адрес у PC-A? . 10.6.0.0

Какой сетевой адрес у PC-B? . 10.0.0.6

Смогут ли эти ПК взаимодействовать друг с другом напрямую? Да, они находятся в одной подсети.

Какой наименьший адрес, присвоенный компьютеру PC-B, позволит ему находиться в одной сети с PC-A? 10.0.0.1

Шаг 2: Установите адрес шлюза по умолчанию.

a. В вашей компании действует политика использования первого IP-адреса в сети в качестве адреса шлюза по умолчанию. Узел в локальной сети (LAN) имеет IP-адрес 172.16.140.24 и маску подсети 255.255.192.0.

Какой у этой сети сетевой адрес?

172.16.128.0

Какой адрес имеет шлюз по умолчанию для этого узла?

170.16.128.1

b. В вашей компании действует политика использования первого IP-адреса в сети в качестве адреса шлюза по умолчанию. Вы получили указание настроить новый сервер с IP-адресом 192.168.184.227 и маской подсети 255.255.255.248.

Какой у этой сети сетевой адрес?

192.168.184.024

Каким будет шлюз по умолчанию для этого сервера?

192.168.184.225

Вопросы для повторения

Почему при определении сетевого адреса важна маска подсети?

Маска подсети позволяет отделить узловую часть адреса от сетевой.

Практическая работа 20: настройка ^6-адресов на сетевых устройствах

Топология

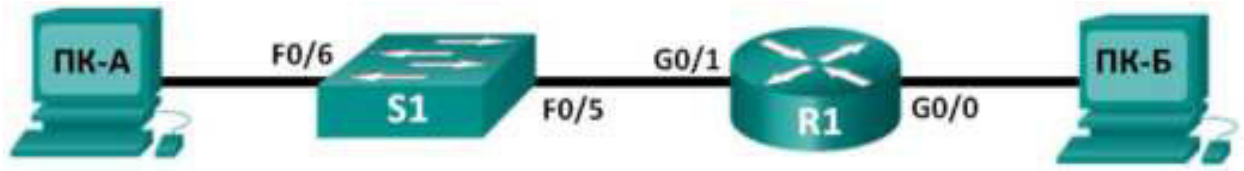


Таблица адресации

Устройство	Интерфейс	^6-адрес	Длина префикса	Шлюз по умолчанию
R1	G0/0	2001 :DB8:ACAD:A::1	64	Недоступно
	G0/1	2001 :DB8:ACAD:1::1	64	Недоступно
S1	VLAN 1	2001 :DB8:ACAD:1::B	64	Недоступно
ПК-А	Сетевой адаптер	2001 :DB8:ACAD:1::3	64	FE80::1
ПК-Б	Сетевой адаптер	2001 :DB8:ACAD:A::3	64	FE80::1

Задачи

Часть 1. Настройка топологии и конфигурация основных параметров маршрутизатора и коммутатора

Часть 2. Ручная настройка ^6-адресов Часть 3. Проверка сквозного подключения

Исходные данные/сценарий

Знание особенностей групп многоадресной рассылки протокола Интернета версии 6 (IPv6) пригодится при назначении ^6-адресов вручную. Понимание того, как назначается многоадресная группа для всех маршрутизаторов и как контролируется назначение адресов для многоадресной группы запрошенных узлов, поможет избежать некоторых проблем маршрутизации IPv6 и обеспечить использование наиболее эффективных методов.

В ходе лабораторной работы вы настроите ^6-адреса для узлов и интерфейсов устройств и выясните, как назначить маршрутизатору многоадресную группу для всех маршрутизаторов. Для отображения ^6-адресов одноадресной передачи и многоадресной рассылки используются команды **show.** Проверить сквозное подключение позволяют команды **ping** и **tracerPPПOoute.**

Примечание. Маршрутизаторы, используемые на практических занятиях CCNA, — Cisco 1941, ПО Cisco IOS версии 15.2(4)M3 (образ universalk9). Используемые коммутаторы: семейство коммутаторов Cisco Catalyst 2960 версии CISCO IOS 15.0(2) (образ lanbasek9). Можно использовать другие маршрутизаторы, коммутаторы и версии ПО CISCO IOS. В зависимости от модели и версии Cisco IOS выполняемые доступные команды и выводы могут отличаться от данных, полученных в ходе

лабораторных работ. Точные идентификаторы интерфейсов указаны в сводной таблице интерфейсов маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что информация, имеющаяся на маршрутизаторе и коммутаторе, удалена и они не содержат файлов

загрузочной конфигурации. Если вы не уверены, что сможете это сделать, обратитесь к инструктору.

Необходимые ресурсы

- 1 маршрутизатор (серия Cisco 1941 с программным обеспечением Cisco IOS версии 15.2(4)M3, универсальный или совместимый образ)
- 1 коммутатор (серия Cisco 2960, с программным обеспечением Cisco IOS версии 15.0(2), образ lanbasek9 или аналогичный)
- Два ПК (Windows 7 с эмулятором терминала, например Tera Term)
- Консольные кабели для настройки устройств Cisco IOS через консольные порты
- Кабели Ethernet в соответствии с топологией

Примечание. Интерфейсы Gigabit Ethernet на маршрутизаторах Cisco 1941 определяют скорость автоматически, поэтому для подключения маршрутизатора к ПК-Б можно использовать прямой кабель Ethernet. При использовании другой модели маршрутизатора Cisco может возникнуть необходимость использовать кроссовый кабель Ethernet.

Примечание. Активация протокола IPv6 в ОС Windows 7 и Vista установлена по умолчанию. В операционной системе Windows XP протокол IPv6 по умолчанию не активирован, поэтому данную ОС на этом практическом занятии использовать не рекомендуется. В данном практическом занятии используются узлы ПК с ОС Windows 7.

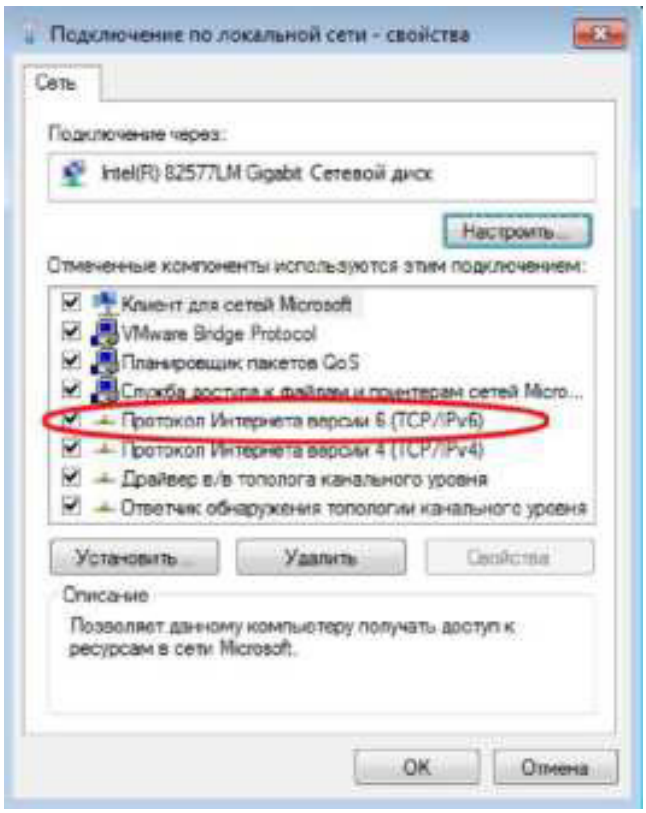
Часть 1: Настройка топологии и конфигурация основных параметров маршрутизатора и коммутатора

Шаг 1: Создайте сеть в соответствии с изображенной на схеме топологией.

Шаг 2: Выполните инициализацию и перезагрузку маршрутизатора и коммутатора.

Шаг 3: Убедитесь в том, что интерфейсы ПК настроены на использование протокола IPv6.

Убедитесь в том, что протокол IPv6 активирован на обоих компьютерах. Для этого проверьте, установлен ли флажок **Протокол Интернета версии 6 (TCP/IPv6)** в окне «Свойства подключения по локальной сети».



Шаг 4: Настройте маршрутизатор.

a. Подключите консоль к маршрутизатору и активируйте привилегированный режим.

b. Назначьте маршрутизатору имя устройства.

c. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверного преобразования введённых команд так, как если бы они были узлами.

d. Назначьте **class** в качестве пароля привилегированного режима.

e. Назначьте **cisco** в качестве пароля консоли и включите вход по паролю.

f. Назначьте **cisco** в качестве пароля виртуального терминала и включите вход по паролю.

g. Зашифруйте пароли, хранящиеся в открытом виде.

h. Создайте баннер с предупреждением о запрете несанкционированного доступа к устройству.

i. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

Шаг 5: Настройте коммутатор.

a. Подключите консоль к коммутатору и активируйте привилегированный режим.

b. Назначьте имя коммутатору.

c. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверного преобразования введённых команд так, как если бы они были узлами.

d. Назначьте **class** в качестве пароля привилегированного режима.

e. Назначьте **cisco** в качестве пароля консоли и включите вход по паролю.

f. Назначьте **cisco** в качестве пароля виртуального терминала и включите вход по паролю

g. Зашифруйте пароли, хранящиеся в открытом виде.

h. Создайте баннер с предупреждением о запрете несанкционированного доступа к устройству.

i. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

Часть 2: Ручная настройка ^6-адресов

a. Назначьте глобальные ^6-адреса одноадресной передачи из таблицы маршрутизации каждому из двух Ethernet-интерфейсов маршрутизатора R1.

```
R1(config)# interface g0/0
R1(config-if)# ipv6 address 2001:db8:acad:a::1/64
R1(config-if)# no shutdown
R1(config-if)# interface g0/1
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# no shutdown
R1(config-if)# end
R1#
```

b. Введите команду **show ipv6 interface brief,** чтобы проверить, назначен ли каждому интерфейсу действительный ^6-адрес одноадресной передачи.

```
R1# show ipv6 interface brief
Em0/0                  [administratively down/down]
    unassigned
GigabitEthernet0/0     [up/up]
    FE80::D68C:B5FF:FECE:A0C0
    2001:DB8:ACAD:A::1
GigabitEthernet0/1     [up/up]
    FE80::D68C:B5FF:FECE:A0C1
    2001:DB8:ACAD:1::1
Serial0/0/0            [administratively down/down]
    unassigned
Serial0/0/1            [administratively down/down]
    unassigned
R1#
```

Шаг 1: Присвойте IPve-адреса Ethernet-интерфейсам на маршрутизаторе R1.

c. Введите команду **show ipv6 interface g0/0.** Обратите внимание на то, что в интерфейсе

содержатся две многоадресные группы запрошенных узлов, поскольку идентификатор интерфейса локального канала (FE80) IPv6-адреса не был настроен в соответствии с идентификатором интерфейса ^6-адреса одноадресной передачи вручную.

Примечание. Отображаемый локальный адрес канала основан на адресации EUI-64, которая автоматически использует для создания 128-битного локального ^6-адреса канала MAC-адрес интерфейса.

```
R1# show ipv6 interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::D68C:B5FF:FECE:A0C0
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
```

```
  Joined group address(es):
    FF02::1
    FF02::1:FF00:1
    FF02::1:FFCE:A0C0
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND advertised reachable time is 0 (unspecified)
  ND advertised retransmit interval is 0 (unspecified)
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
R1#
```

d. Чтобы локальный адрес канала соответствовал адресу одноадресной передачи в интерфейсе, вручную введите локальные адреса каналов для каждого из двух Ethernet-интерфейсов маршрутизатора R1.

```
R1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# interface g0/0
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# interface g0/1
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# end
R1#
```

Примечание. Каждый интерфейс маршрутизатора находится в отдельной сети. Пакеты с локальным адресом канала никогда не покидают локальную сеть, а значит, для обоих интерфейсов можно указывать один и тот же локальный адрес канала.

e. Еще раз введите команду **show ipv6interface g0/0.** Обратите внимание на то, что локальный адрес канала изменился на **FE80::1** и осталась только одна многоадресная группа запрошенных узлов.

```
R1# show ipv6 interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::1
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
  Joined group address(es):
    FF02::1
    FF02::1:FF00:1
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1

    ND reachable time is 30000 milliseconds (using 30000)
    ND advertised reachable time is 0 (unspecified)
    ND advertised retransmit interval is 0 (unspecified)
    ND router advertisements are sent every 200 seconds
    ND router advertisements live for 1800 seconds
    ND advertised default router preference is Medium
    Hosts use stateless autoconfig for addresses.
  R1#
```

Какие многоадресные группы назначены интерфейсу G0/0?

Шаг 2: Активируйте ^6-маршрутизацию на маршрутизаторе R1.

Присвоен ли IPv6-адрес одноадресной передачи сетевому адаптеру ПК-Б?

b. Активируйте ^6-маршрутизацию на маршрутизаторе R1 с помощью команды **IPv6 unicast- routing.**

```
R1 # configure terminal
R1(config)# ipv6 unicast-routing
R1(config)# exit
R1#
*Dec 17 18:29:07.415: %SYS-5-CONFIG_I: Configured from console by console
```

a. В окне командной строки компьютера ПК-Б введите команду **ipconfig,** чтобы получить данные !Руб-адреса, присвоенного интерфейсу компьютера.

```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::dd0e:67fb:d14f:1288%11
   Autoconfiguration IPv4 Address. . : 169.254.18.136
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :

Tunnel adapter isatap.{E2FC1866-B195-460A-BF40-F04F42A38FFE}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter Local Area Connection* 11:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\>_
```

c. Введите команду **show ipv6 interface g0/0,** чтобы узнать, какие многоадресные группы присвоены интерфейсу G0/0. Обратите внимание на то, что теперь в списке групп для интерфейса G0/0 отображается многоадресная группа всех маршрутизаторов (FF02::2).

```
R1# show ipv6 interface g0/0
GigabitEthernet0/0 is up, line protocol is up
```

Примечание. Это позволит компьютерам получать IP-адреса и данные основного шлюза автоматически с помощью функции SLAAC (Автоконфигурация без сохранения состояния адреса).

```
  IPv6 is enabled, link-local address is FE80::1
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64 [EUI]
  Joined group address(es):
    FF02::1
FF02::2
    FF02::1:FF00:1
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND advertised reachable time is 0 (unspecified)
  ND advertised retransmit interval is 0 (unspecified)
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
R1#
```

d. Теперь, когда маршрутизатор R1 входит в многоадресную группу всех маршрутизаторов, ещё раз введите команду **ipconfig** на компьютере ПК-Б. Изучите данные IPv6-адреса.

```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:db8:acad:a:dd0e:67fb:d14f:1288
   Temporary IPv6 Address. . . . . . : 2001:db8:acad:a:6082:dcb0:5fb2:3ece
   Link-local IPv6 Address . . . . . : fe80::dd0e:67fb:d14f:1288%11
   Autoconfiguration IPv4 Address. . : 169.254.18.136
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : fe80::1%11

Tunnel adapter isatap.{E2FC1866-B195-460A-BF40-F04F42A38FFE}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter Local Area Connection* 11:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\>
```

Почему компьютер ПК-Б получил глобальный префикс маршрутизации и идентификатор подсети, который вы настроили на маршрутизаторе R1?

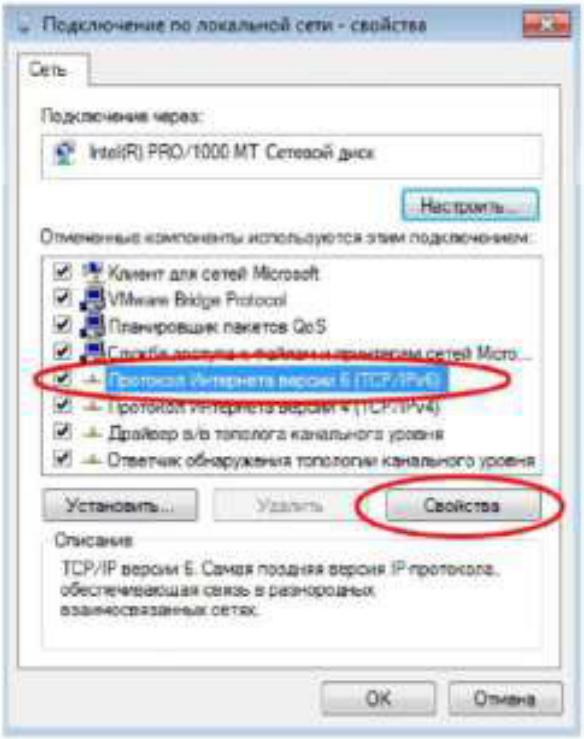
Шаг 3: Назначьте ^6-адреса интерфейсу управления (SVI) на коммутаторе S1.

a. Назначьте полученный IPv6-адрес интерфейсу управления (VLAN 1) на коммутаторе S1. Также назначьте этому интерфейсу локальный адрес канала. Синтаксис команды IPv6 точно такой же, как и на маршрутизаторе.

b. Проверьте правильность назначения IPv6-адресов интерфейсу управления с помощью команды **show ipv6 interface vlan1.**

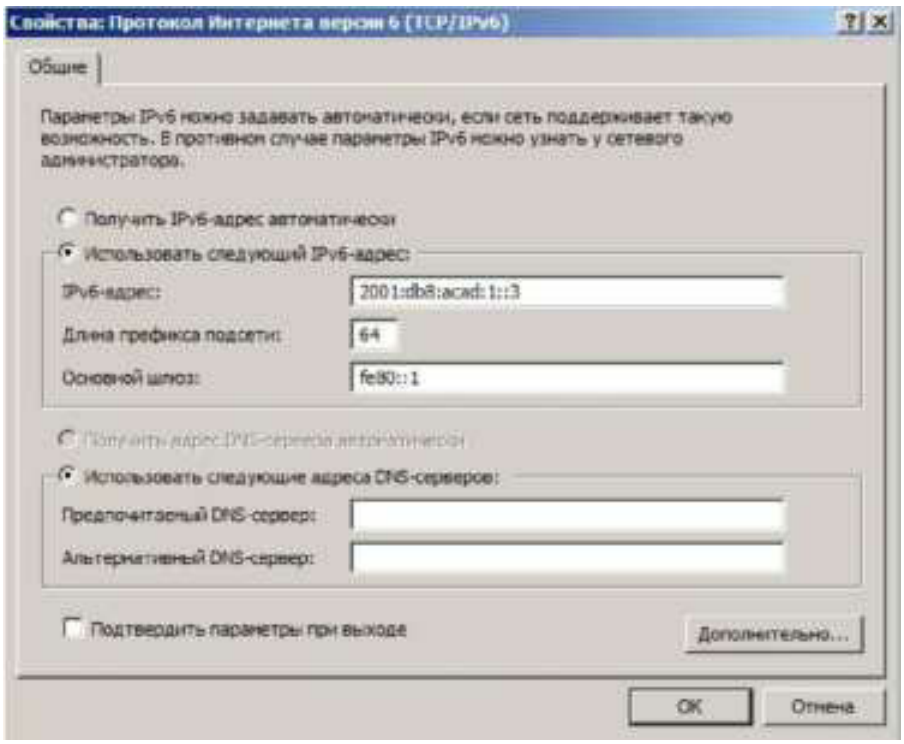
Шаг 4: Назначьте компьютерам статические ^6-адреса.

a. На компьютереПК-А откройте окно «Свойства подключения по локальной сети». Выберите **Протокол Интернета версии 6 (TCP/IPv6)** и нажмите кнопку **Свойства.**



b. Установите переключатель **Использовать следующий ^6-адрес.** Пользуясь таблицей

адресации, укажите следующие параметры: **^6-адрес, Длина префикса подсети** и **Основной шлюз.** Нажмите OK



.

c. Нажмите кнопку **Закрыть,** чтобы закрыть окно свойств подключения по локальной сети.

d. Повторите шаги с 4a по 4c, чтобы указать статический ^6-адрес на компьютере ПК-Б. Правильный IPv6-адрес можно найти в таблице адресации.

e. Введите команду **ipconfig** в окне командной строки на компьютере ПК-Б, чтобы проверить данные !Руб-адреса.

```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:db8:acad:a::3
   IPv6 Address. . . . . . . . . . . : 2001:db8:acad:a:d428:7de2:997c:b05a
   Temporary IPv6 Address. . . . . . : 2001:db8:acad:a:e19e:db9f:e38e:9252
   Link-local IPv6 Address . . . . . : fe80::d428:7de2:997c:b05a%11
   Default Gateway . . . . . . . . . : fe80::1%11

Tunnel adapter isatap.{E2FC1866-B195-460A-BF40-F04F42A38FFE}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter Local Area Connection* 11:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\>
```

Часть 3: Проверка сквозного подключения

a. На компьютере ПК^введите эхо-запрос **FE80::1**. Это локальный адрес канала, назначенный интерфейсу G0/1 на маршрутизаторе R1.

```
C:\>ping fe80::1

Pinging fe80::1 with 32 bytes of data:
Reply from fe80::1: time<1ms
Reply from fe80::1: time<1ms
Reply from fe80::1: time<1ms
Reply from fe80::1: time<1ms

Ping statistics for fe80::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Примечание. Для проверки подключения вместо локального адреса канала можно использовать глобальный адрес одноадресной передачи.

b. Отправьте эхо-запрос с помощью команды ping в интерфейс управления коммутатора S1 с компьютера ПК-A.

```
C:\>ping 2001:db8:acad:1::b

Pinging 2001:db8:acad:1::b with 32 bytes of data:
Reply from 2001:db8:acad:1::b: time=14ms
Reply from 2001:db8:acad:1::b: time=2ms
Reply from 2001:db8:acad:1::b: time=2ms
Reply from 2001:db8:acad:1::b: time=3ms

Ping statistics for 2001:db8:acad:1::b:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 14ms, Average = 5ms

C:\>_
```

c. Введите команду **tracert** на ПК-А, чтобы проверить наличие сквозного подключения к компьютеру ПК-Б.

```
C:\>tracert 2001:db8:acad:a::3

Tracing route to 2001:db8:acad:a::3 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms  2001:db8:acad:1::1
  2     5 ms    <1 ms    <1 ms  2001:db8:acad:a::3

Trace complete.

C:\>
```

d. С компьютера ПК-Б отправьте эхо-запрос с помощью команды ping на компьютер ПК-А.

```
C:\>ping 2001:db8:acad:1::3

Pinging 2001:db8:acad:1::3 with 32 bytes of data:
Reply from 2001:db8:acad:1::3: time<1ms
Reply from 2001:db8:acad:1::3: time<1ms
Reply from 2001:db8:acad:1::3: time<1ms
Reply from 2001:db8:acad:1::3: time<1ms

Ping statistics for 2001:db8:acad:1::3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

e. С компьютера ПК-Б отправьте эхо-запрос с помощью команды ping на локальный адрес канала интерфейса G0/0 на маршрутизаторе R1.

```
C:\>ping fe80::1

Pinging fe80::1 with 32 bytes of data:
Reply from fe80::1: time<1ms
Reply from fe80::1: time<1ms
Reply from fe80::1: time<1ms
Reply from fe80::1: time<1ms

Ping statistics for fe80::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>_
```

Примечание. В случае отсутствия сквозного подключения проверьте, правильно ли указаны IPv6- адреса на всех устройствах.

Вопросы на закрепление

1. Почему один и тот же локальный адрес канала FE80::1 можно присвоить каждому из двух Ethernet- интерфейсов маршрутизатора R1?

2. Назовите идентификатор подсети в P6-адресе одноадресной передачи 2001:db8:acad::aaaa:1234/64. Сводная таблица интерфейса маршрутизатора

Общие сведения об интерфейсах маршрутизаторов				
Модель маршрутизатора	Интерфейс Ethernet #1	Интерфейс Ethernet #2	Последовательный интерфейс #1	Последовательный интерфейс #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/0/0)	Serial 0/1/1 (S0/0/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы для определения типа маршрутизатора и количества имеющихся на нём интерфейсов. Не существует эффективного способа перечислить все комбинации настроек для каждого класса маршрутизаторов. Эта таблица включает в себя идентификаторы возможных сочетаний Ethernet и последовательных интерфейсов в устройстве. В таблицу интерфейсов не включены иные типы интерфейсов, даже если они присутствуют на каком-либо определённом маршрутизаторе. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое может использоваться в командах IOS для представления интерфейса.				

Основная литература:

1. Кузин, А.В. Компьютерные сети : учеб. пособие / А.В. Кузин, Д.А. Кузин. — 4-е изд., перераб. и доп. — М. : ФОРУМ : ИНФРА-М, 2019. — 190 с. — (Среднее профессиональное образование). - Режим доступа: http://znanium.com/catalog/product/983172 - Договор № 5669 от 10.01.2022 г.

Дополнительная литература:

1. Максимов, Н.В. Компьютерные сети : учеб. пособие / Н.В. Максимов, И.И. Попов. — 6-е изд., перераб. и доп. — М. : ФОРУМ : ИНФРА-М, 2018. — 464 с. — (Среднее профессиональное образование). - Режим доступа: http://znanium.com/catalog/product/792686 - Договор № 5669 от 10.01.2022 г.
2. Сысоев, Э.В. Администрирование компьютерных сетей /Э.В. Сысоев, А.В. Терехов, Е.В. Бурцева; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего образования «Тамбовский государственный технический университет». – Тамбов: Издательство ФГБОУ ВПО «ТГТУ», 2017. – 80 с. : ил. – Режим доступа:– URL: http://biblioclub.ru/index.php?page=book&id=499414. – Библиогр. в кн. – ЭБС Университетская библиотека

Интернет-источники:

1. Журнал сетевых решений LAN [Электронный ресурс]. — Режим доступа: URL:http://www.osp.ru/lan/#/home
2. Журнал о компьютерных сетях и телекоммуникационных технологиях «Сети и системы связи» [Электронный ресурс]. — Режим доступа: URL: http://www.ccc.ru/
3. Научно-технический и научно-производственный журнал «Информационные технологии» [Электронный ресурс]. — Режим доступа: URL: http://www.novtex.ru/IT/
4. Национальный Открытый Университет «ИНТУИТ» [Электронный ресурс]. — Режим доступа: URL: http://www.intuit.ru/
5. Журнал CHIP [Электронный ресурс]. — Режим доступа: URL: http://www.ichip.ru/
6. Журнал "ComputerBild" [Электронный ресурс]. — Режим доступа: URL: http://www.computerbild.ru

7. Проектирование сетевой инфраструктуры на базе Windows Server 2008: видеокурс <Электронный ресурс>. - Режим доступа: http://soft-wins.net/video-lessons/4495-video-kurs-m6435-proektirovanie-setevoy-infrastruktury-na-baze-windjws-server-2008.html.