Лабораторные работы

по дисциплине «Компьютерные сети»

Оглавление

[Методические указания к лабораторному практикуму 2](#_Toc94804542)

[Лабораторная работа №1. Знакомство со средой Cisco Packet Tracer 3](#_Toc94804543)

[Лабораторная работа №2. Протоколы ARP и ICMP (программы ping и tracert) 14](#_Toc94804544)

[Лабораторная работа №3. Протоколы SMTP и POP3 52](#_Toc94804545)

[Лабораторная работа 4. «Работа с сетевым анализатором» 74](#_Toc94804546)

[СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ 91](#_Toc94804547)

[ПРИЛОЖЕНИЕ 1 92](#_Toc94804548)

[ПРИЛОЖЕНИЕ 2 93](#_Toc94804549)

# Методические указания к лабораторному практикуму

Основной целью лабораторного практикума является изучение построения компьютерных сетей и сетевых протоколов, приобретение навыков работы в режиме реального времени и симуляции Packet Tracer. В рамках лабораторного практикума изучаются построение топологии сети, проверка ее работоспособности посредством ICMP-сообщений, протокол разрешения адреса, прикладные протоколы электронной почты, вопросы содержимого пакетов заданного протокола.

Работы выполняются с помощью симулятора Cisco Packet Tracer, необходимое программное обеспечение установлено на компьютеры в лаборатории. Все лабораторные работы содержат необходимые теоретические сведения, общую часть работы, обязательную для выполнения, и индивидуальные задания.

В содержании лабораторных работ при настройке сетевых устройств есть упоминание о службе DNS. В первых двух работах служба DNS непосредственно не участвует, а значит, присваивать IP-адрес DNS-серверу необязательно. В лабораторной работе №3 задействован DNS-сервер, поэтому теоретические сведения этой работы содержат необходимую информацию.

# Лабораторная работа №1. Знакомство со средой Cisco Packet Tracer

**Цель работы:** познакомиться с интерфейсом симулятора, изучить режим реального времени, основные операции c устройствами.

**Программа работы:**

1. Создание топологии сети;
2. Добавление конечных узлов;
3. Подключение к конечным узлам сетевых устройств;
4. Настройка IP-адресов и масок сети на узлах;
5. Проверка работы сети в режиме реального времени

**Выполнение работы:**

Запускаем среду Cisco Packet Tracer. При запуске программы открывается главное окно симулятора (см. рис. 3.5).

1. Построение топологии сети

Создаем новую топологию сети, выбираем необходимые устройства и соединения.

Топология сети может быть сконфигурирована из различных устройств и связей. В данной лабораторной работе мы используем простые сетевые устройства: концентратор, коммутатор, конечные устройства (компьютеры).

Network Component Box содержит все представленное оборудование, с помощью которого можно построить сеть (см. рис.3.6). С помощью одного клика по каждой группе устройств и соединений можно отобразить различные их варианты, отличающиеся между собой (рис. 4.1).

Рис. 4.1 Виды устройств и соединений

1. Построение топологии, добавление узлов

Один клик по конечным устройствам (рис. 4.2).



Рис. 4.2 Виды конечных устройств

Один клик по выбранному устройству, для нашей работы это PC (рис. 4.3).



Рис. 4.3 Выбор конечного устройства

Переместите курсор на рабочую область симулятора. Курсор должен превратиться в знак “+”. Щелкните мышью в любом месте на области и выбранное вами устройство скопируется. Проделайте эту процедуру еще три раза, на рабочей области у вас будет 4 PC (рис. 4.4).



Рис. 4.4. Вид рабочей области

1. Подключение к узлам концентратора и коммутатора

Выберите группу устройств концентраторы (Hubs), из этой группы выберите первую модель (Hub-PT). Разместите концентратор между PC0 и PC1 (рис. 4.5).

Задача концентратора довольно проста: он повторяет пакет, принятый на одном порту на всех остальных портах.



Рис. 4.5 Вид рабочей области

Подключим PC0 к Hub0, выбрав сначала тип подключения. Для этого случая подойдет медный кабель с прямым подключением (рис. 4.6).



Рис. 4.6 Выбор соединения с прямым подключением

Для подключения PC0 к Hub0 выполните следующие действия (рис. 4.7):

1. Один раз щелкните мышью на PC0
2. Выберите тип интерфейса FastEthernet
3. Переместите курсор на Hub0
4. Нажмите на Hub0 один раз и выберите порт 0
5. Обратите внимание на зеленые индикаторы двух устройств на соединении, что значит, оба устройства готовы к работе.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 |
|  |  |  |  |  |

Рис. 4.7 Подключение PC0 к Hub0

Повторите описанные выше действия для подключения PC1 к Hub0, выбрав на концентраторе порт 1 (рис.4.8). Фактически номер порта значения не имеет, однако удобнее занимать порты последовательно.



Рис. 4.8 Вид рабочей области

Далее размещаем на рабочей области симулятора коммутатор, например, модель 2950-24 (рис. 4.9). Описание семейства коммутаторов серии 2950 можно найти на сайте компании Cisco Systems. [Электронный ресурс]. URL:

<http://www.cisco.com/web/RU/products/hw/switches/ps628/ps627/index.html>.

Коммутаторы - это устройства, работающие на канальном уровне модели OSI и предназначенные для объединения нескольких узлов в пределах одного или нескольких сегментах сети. Коммутатор передает пакеты на основании внутренней таблицы - таблицы коммутации, следовательно, трафик идёт только на тот порт, которому он предназначается, а не повторяется на всех портах, в отличие от концентратора.



Рис. 4.9 Вид рабочей области

Подключим PC2 к Switch0, выбрав тип соединения медный кабель с прямым подключением.

Для подключения выполните следующие действия (рис. 4.10):

1. Щелкните мышью один раз на PC2
2. Выберите тип интерфейса FastEthernet
3. Переместите курсор на Switch0
4. Нажмите один раз на Switch0 и выберите FastEthernet0/1
5. Обратите внимание, что для правильной работы сети оба подключенных устройства должны быть готовы, о чем свидетельствуют зеленые индикаторы. В отличие от подключения к концентратору, это может занять некоторое время.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 |  |
|  |  |  |  |  |  |

Рис. 4.10 Подключение PC2 к Switch0

Повторите описанные выше действия для подключения PC3 к Switch0, выбрав один из его интерфейсов FastEthernet0/2 (рис. 4.11).

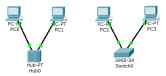


Рис. 4.11 Вид рабочей области

Если навести курсор на один из индикаторов, можно посмотреть, какой интерфейс задействован при данном подключении (рис. 4.12).



Рис. 4.12 Вид рабочей области

1. Настройка IP-адреса и маски подсети на хостах

Прежде чем мы сможем общаться между хостами по сети, нам нужно настроить IP-адреса и маски подсети на устройствах.

Щелкните мышью один раз на PC0. Откроется окно свойств конечного узла на вкладке Physical (рис. 4.13).



Рис. 4.13 Вкладка Physical конечного устройства (компьютера)

Физический вид устройства мы менять не будем, поэтому сразу переходим к настройке в вкладке Config (рис. 4.14).

Именно здесь вы можете изменить название PC0 (например, ввести IP-адрес этого компьютера, чтобы не подглядывать его каждый раз в настройках). Кроме того, здесь вы можете указать IP-адрес шлюза, также известный как шлюз по умолчанию, и IP-адрес DNS-сервера. Мы обсудим это позже, но это будет IP-адрес локального маршрутизатора. Если вы хотите, вы можете ввести IP-адрес шлюза 192.168.1.1 и IP-адрес DNS-сервера 192.168.1.100, хотя он не будет использоваться в этой лабораторной работе.



Рис. 4.14 Вкладка Config конечного устройства (компьютера)

Кликните мышью на интерфейсе FastEthernet (рис. 4.15). Укажите IP-адрес компьютера 192.168.1.10. Нажмите на поле для ввода маски подсети, она определится автоматически 255.255.255.0.



Рис. 4.15 Настройки интерфейса конечного устройства

Информация автоматически сохраняется после ввода.

Закройте окно настройки PC0 и повторите указанные выше действия для остальных узлов сети, используя информацию о IP-адресах и маски подсети, представленную в таблице 4.1

Таблица 4.1

|  |  |  |
| --- | --- | --- |
| Хост | IP-адрес | Маска подсети |
| PC0 | 192.168.1.10 | 255.255.255.0 |
| PC1 | 192.168.1.11 | 255.255.255.0 |
| PC2 | 192.168.1.12 | 255.255.255.0 |
| PC3 | 192.168.1.13 | 255.255.255.0 |

После настройки узлов рабочая область симулятора будет выглядеть следующим образом (рис. 4.16):

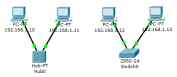


Рис. 4.16 Вид рабочей области

Можно проверить введенную вами информацию на узлах (рис. 4.17). Для этого наведите курсор на интересующее вас устройство.



Рис. 4.17 Проверка настроек конечного устройства (компьютера)

Если при построении сети какие-либо устройства или связи оказались лишними, их можно удалить при помощи инструмента Delete на боковой панели симулятора (Common Tools Bar). Для удаления нужно щелкнуть один раз на инструмент Delete, затем на элемент сети.

1. Соединение концентратора и коммутатора

Для подключения такого типа устройств, как коммутатора и концентратора, используется перекрестный кабель (рис. 4.18).



Рис. 4.18. Выбор соединения

Для подключения Hub0 к Switch0 выполните следующие действия:

1. Щелкните один раз на Hub0, выберите порт 2 (рис. 4.19).

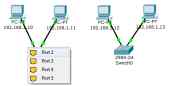


Рис. 4.19 Вид рабочей области

1. Переместите курсор на Switch0, щелкните на нем мышью и выберите интерфейс FastEthernet0/3 (рис. 4.20).

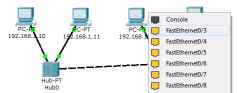


Рис. 4.20. Вид рабочей области

1. Когда оба устройства будут готовы к работе, индикаторы состояния станут зелеными (рис. 4.21).

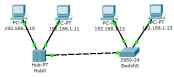


Рис. 4.21. Вид рабочей области

1. Выполним проверку в режиме реального времени

Убедитесь, что вы находитесь в режиме реального времени.



Сформируем простой пакет ping-запроса для проверки работы сети, воспользовавшись Add Simple PDU. Нажмите один раз на Add Simple PDU.



Теперь нужно выбрать два узла: источник и приемник ping-запроса. Наведите курсор на PC0 (192.168.1.10) и щелкните на нем мышью (источник ping-запроса), затем переместите курсор на PC3 (192.168.1.13) (приемник ping-запроса) и кликните на нем.

Так как все интерфейсы и связи сети настроены правильно (о чем говорят зеленые индикаторы состояния), то ping-запрос должен пройти успешно. В окне управления пакетами User Created Packet Window (см. рис. 3.6) появится соответствующая запись (рис. 4.22).



Рис. 4.22 Окно управления пакетами

Важно: измените IP-адрес 192.168.1.13 узла PC3 на IP-адрес 192.168.2.13, с той же маской подсети 255.255.255.0. Выполните ping-запрос от PC0 к PC3. Какой получился результат? Каковы причины?

Чтобы очистить список выполненных операций моделирования, необходимо удалить соответствующий сценарий симуляции.

Нажмите на кнопку Delete на панели User Created Packet Window (рис. 4.23).



Рис. 4.23 Окно управления пакетами

Все записи сценария удалятся.

1. Сохранение созданной топологии

Выберите в Menu Bar вкладку File, далее Save as. Выберите соответствующую директорию. Все файлы симулятора Cisco Packet Tracer имеют расширение .pkt.

1. Построение топологии сети, состоящей из двух подсетей

В результате первой работы мы изучили основные операции с устройствами. Для подготовки к выполнению следующей лабораторной работы у нас есть соответствующие знания и навыки для построения топологии сети следующего вида (рис. 4.24):

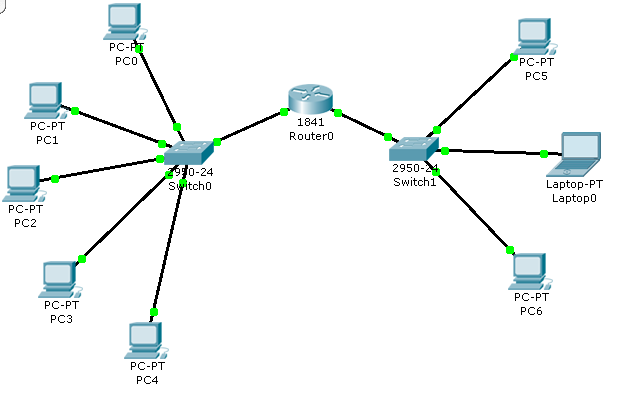


Рис. 4.24. Топология сети для лабораторной работы №2

такой топологии нужно добавить в рабочую область симулятора конечные узлы, два коммутатора и маршрутизатор. При добавлении маршрутизатора выберите модель 1841, т.к. она имеет два интерфейса. Описание маршрутизаторов серии 1841 можно найти на сайте компании Cisco Systems. [Электронный ресурс]. URL: <http://www.cisco.com/en/US/products/ps5875/index.html>. При соединении устройств между собой воспользуйтесь медным кабелем с прямым подключением.

# Лабораторная работа №2. Протоколы ARP и ICMP (программы ping и tracert)

**Цель работы:** изучить режим симуляции Cisco Packet Tracer, протоколы ARP и ICMP на примере программ ping и tracert.

**Программа работы:**

1. Построение топологии сети, настройка конечных узлов;
2. Настройка маршрутизатора;
3. Проверка работы сети в режиме симуляции;
4. Посылка ping-запроса внутри сети;
5. Посылка ping-запроса во внешнюю сеть;
6. Посылка ping-запроса на несуществующий IP-адрес узла;
7. Выполнение индивидуального задания.

**Теоретические сведения:**

**Протокол ARP**

Для определения физического адреса по IP-адресу используется протокол разрешения адреса Address Resolution Protocol (ARP). Протокол ARP работает различным образом в зависимости от того, какой протокол канального уровня работает в данной сети с возможностью широковещательного доступа одновременно ко всем узлам сети. [1]

Протокол ARP позволяет динамически определить МАС-адрес по IP-адресу. МАС-адрес – это уникальный серийный номер, присваиваемый каждому сетевому устройству для идентификации его в сети, так же называется физическим или аппаратным адресом. Протокол локальной сети, поддерживаемый в лабораторной работе – Ethernet. В Ethernet сетях, использующих стек TCP/IP, сетевой интерфейс имеет физический адрес длиной в 48 бит. Кадры, которыми обмениваются на канальном уровне, должны содержать аппаратный адрес сетевого интерфейса. Однако TCP/IP использует собственную схему адресации: 32-битные IP-адреса. Значение IP-адреса приемника недостаточно, чтобы отправить дейтаграмму этому хосту. Драйвер Ethernet должен знать МАС-адрес интерфейса назначения, чтобы послать туда данные. В задачу ARP входит обеспечение динамического соответствия между 32-битными IP-адресами и 48-битными МАС-адресами, используемыми различными сетевыми технологиями. Протокол ARP работает в пределах одной подсети и автоматически запускается, когда возникает необходимость преобразования IP-адреса в аппаратный адрес. [2]

Работа протокола ARP поясняется на рис. 4.25.

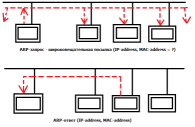


Рис. 4.25 ARP-запрос и ARP-ответ

Узел, которому нужно выполнить отображение IP-адреса на локальный адрес, формирует ARP-запрос, вкладывает его в кадр протокола канального уровня, указывая в нем известный IP-адрес, и рассылает запрос широковещательно. Все узлы локальной сети получают ARP запрос и сравнивают указанный там IP-адрес с собственным. В случае их совпадения узел формирует ARP-ответ, в котором указывает свой IP-адрес и свой локальный адрес и отправляет его уже направленно, так как в ARP запросе отправитель указывает свой локальный адрес.

Для того чтобы уменьшить количество посылаемых запросов ARP, каждое устройство в сети, использующее протокол ARP, должно иметь специальную буферную память. В ней хранятся пары адресов (IP-адрес, физический адрес) устройств в сети. Всякий раз, когда устройство получает ARP-ответ, оно сохраняет в буферной памяти соответствующую пару. Если адрес есть в списке пар, то нет необходимости посылать ARP-запрос. Эта буферная память называется ARP-таблицей.

В ARP-таблице могут содержаться как статические, так и динамические записи. Динамические записи добавляются и удаляются автоматически, статические заносятся вручную.

Так как большинство устройств в сети поддерживает динамическое разрешение адресов, то администратору, как правило, нет необходимости вручную указывать записи протокола ARP в таблице адресов.

Каждая запись в ARP-таблице имеет свое время жизни. Политики очистки ARP-таблицы продиктованы используемой операционной системой. При добавлении записи для нее активируется таймер.

Сообщения протокола ARP при передаче по сети инкапсулируются в поле данных кадра. Они не содержат IP-заголовка. В отличие от сообщений большинства протоколов, сообщения ARP не имеют фиксированного формата заголовка. Это объясняется тем, что протокол был разработан таким образом, чтобы он был применим для разрешения адресов в различных сетях. [3]

ARP-запросы и ответы используют один и тот же формат пакета. Так как локальные адреса могут в различных типах сетей иметь различную длину, то формат пакета протокола ARP зависит от типа сети. На рис. 4.26 показана структура пакета запросов и ответов. [4]



Рис. 4.26 Формат пакета ARP

* Network Type – тип канального протокола

Для Ethernet – 1.

* Protocol - протокол сетевого уровня
* HAL - длина канального адреса
* PAL - длина сетевого адреса
* Operation - тип операции (1 – запрос, 2 – ответ)

Узел, отправляющий ARP-запрос, заполняет в пакете все поля, кроме поля искомого локального адреса. Значение этого поля заполняется узлом, опознавшим свой IP-адрес.

**Протокол ICMP**

Протокол ICMP предназначен для передачи управляющих и диагностических сообщений. С его помощью передаются сообщения об ошибках, а также о возникновении ситуаций, требующих повышенного внимания. Протокол относится к сетевому уровню модели TCP/IP. Сообщения ICMP генерируются и обрабатываются протоколами сетевого (IP) и более высоких уровней (TCP или UDP). При появлении некоторых ICMP-сообщений генерируются сообщения об ошибках, которые передаются пользовательским процессам. ICMP-сообщения передаются внутри IP-дейтаграмм (рис. 4.27). [2]



Рис. 4.27 Инкапсуляция ICMP-сообщений в IP-дейтаграммы

Формат ICMP-сообщения показан на рис. 4.28. Заголовок ICMP включает 8 байт, но только первые 4 байта одинаковы для всех сообщений, остальные поля заголовка и тела сообщения определяются типом сообщения.



Рис. 4.28 Формат ICMP-сообщения

Поле контрольной суммы охватывает ICMP-сообщение целиком.

Тип сообщения определяется значением поля “Тип” заголовка. Некоторые типы ICMP-сообщений имеют внутреннюю детализацию (код), при этом конкретный вид сообщения определяется как типом, так и кодом сообщения. Подробнее с видами типов и кодов ICMP-сообщений можно ознакомиться в спецификации протокола ICMP RFC 792. [Электронный ресурс]. URL: <http://tools.ietf.org/html/rfc792>.

**Программа ping**

Программа ping была разработана для проверки доступности удаленного узла. Программа посылает ICMP-эхо-запрос на узел и ожидает возврата ICMP-эхо-отклика. Программа рing является обычно первым диагностическим средством, с помощью которого начинается идентификация какой-либо проблемы в сетях. Помимо доступности, с помощью ping можно оценить время возврата пакета от узла, что дает представление о том, "насколько далеко" находится узел. Кроме этого, Ping имеет опции записи маршрута и временной метки. Сообщения эхо-запроса и эхо-отклика имеют один формат (рис 4.29). [2]



Рис. 4.29 Формат пакета ICMP-сообщения

* Тип – тип пакета

8 – запрос эха

0 – ответ на запрос эха

* Код – расшифровка назначения пакета внутри типа (в данном случае 0)
* Контрольная сумма вычисляется для всего пакета
* Идентификатор – номер потока сообщений
* Последовательный номер – номер пакета в потоке [3]

Так же, как в случае других ICMP-запросов, в эхо-отклике должны содержаться поля идентификатора и номера последовательности. Кроме того, любые дополнительные данные, посланные компьютером, должны быть отражены эхом.

В поле идентификатора ICMP сообщения устанавливается идентификатор процесса, отправляющего запрос. Это позволяет программе ping идентифицировать вернувшийся ответ, если на одном и том же хосте в одно и то же время запущено несколько программ ping.

Номер последовательности начинается с 0 и инкрементируется каждый раз, когда посылается следующий эхо-запрос. Вывод программы показан на рис. 4.30. Первая строка вывода содержит IP-адрес хоста назначения, даже если было указано имя. Поэтому программа рing часто используется для определения IP-адреса удаленного узла. [2]

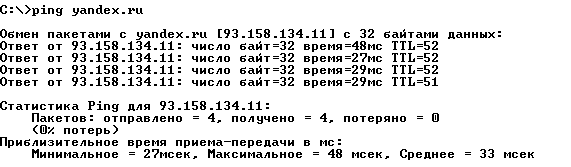


Рис. 4.30 Вывод программы ping

**Программа tracert**

Программа tracert позволяет посмотреть маршрут, по которому двигаются IP-дейтаграммы от одного хоста к другому.

Программа tracert не требует никаких специальных серверных приложений. В ее работе используются стандартные функции протоколов ICMP и IP. Для понимания работы программы следует вспомнить порядок обработки поля TTL в заголовке IP-дейтаграммы.

Каждый маршрутизатор, обрабатывающий дейтаграмму, уменьшает значение поля TTL в ее заголовке на единицу. При получении дейтаграммы с TTL равным 1, маршрутизатор уничтожает ее и посылает хосту, который ее отправил, ICMP-сообщение "время истекло". При этом дейтаграмма, содержащая это ICMP-сообщение, имеет в качестве адреса источника IP-адрес маршрутизатора.

Это и используется в программе tracert. На хост назначения отправляется IP-дейтаграмма, в которой поле TTL, установлено в единицу. Первый маршрутизатор на пути дейтаграммы, уничтожает ее (так как TTL равно 1) и отправляет ICMP-сообщение об истечении времени. Таким образом, определяется первый маршрутизатор в маршруте. Затем tracert отправляет дейтаграмму с полем TTL равным 2, что позволяет получить IP-адрес второго маршрутизатора. Аналогичные действия продолжаются до тех пор, пока дейтаграмма не достигнет хоста назначения. При получении ответа от этого узла процесс трассировки считается завершённым.

Пример вывода программы показан на рис. 4.31.



Рис. 4.31 Вывод программы tracert

Первая строка, без номера содержит имя и IP адрес пункта назначения и указывает на то, что величина TTL не может быть больше 30.

Следующие строки вывода начинаются с распечатки значения TTL (1, 2, 3 и т.д.) и содержат имя (IP-адрес) хоста или маршрутизатора и время возврата ICMP-сообщения.

Для каждого значения TTL отправляется 3 дейтаграммы. Для каждого возвращенного ICMP-сообщения рассчитывается и печатается время возврата.

Если ответ на дейтаграмму не получен в течение пяти секунд, печатается звездочка, после чего отправляется следующая дейтаграмма. [2]

**Выполнение работы:**

1. Построение топологии сети

В конце вводной лабораторной работы мы создали следующую топологию сети, состоящую из конечных узлов (PC), коммутаторов и маршрутизатора (рис. 4.32):

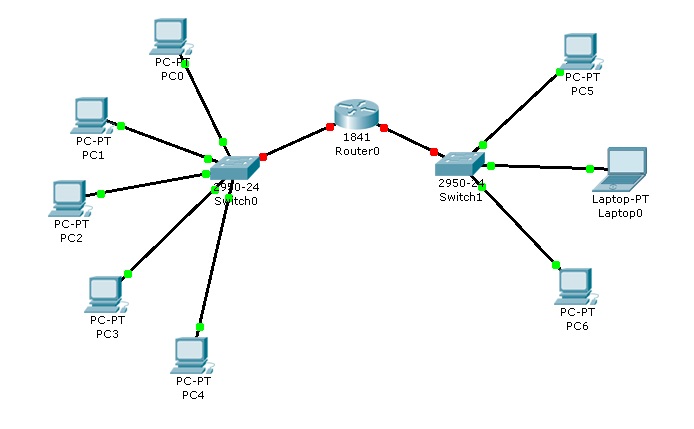


Рис. 4.32 Тестовая топология сети

Маршрутизатор Router0 имеет два интерфейса и соединяет две подсети. Произведем настройку конечных узлов.

1. Настройка конечных узлов

На устройствах PC0-PC4 установим заданные IP-адреса и маску подсети (таблица 4.2). IP-адрес шлюза для всех узлов – 192.168.3.1. IP-адрес DNS-сервера указывать необязательно, т.к. в данной работе он использоваться не будет.

Таблица 4.2

|  |  |  |
| --- | --- | --- |
| Хост | IP-адрес | Маска подсети |
| PC0 | 192.168.3.3 | 255.255.255.0 |
| PC1 | 192.168.3.4 | 255.255.255.0 |
| PC2 | 192.168.3.5 | 255.255.255.0 |
| PC3 | 192.168.3.6 | 255.255.255.0 |
| PC4 | 192.168.3.7 | 255.255.255.0 |

На устройствах PC5, Laptop0, PC6 установим заданные IP-адреса и маску подсети (таблица 4.3). IP-адрес шлюза для всех узлов – 192.168.5.1. IP-адрес DNS-сервера указывать необязательно.

Таблица 4.3

|  |  |  |
| --- | --- | --- |
| Хост | IP-адрес | Маска подсети |
| PC5 | 192.168.5.3 | 255.255.255.0 |
| Laptop0 | 192.168.5.4 | 255.255.255.0 |
| PC6 | 192.168.5.5 | 255.255.255.0 |

Каждый узел переименуем его же IP-адресом, получится следующее (рис. 4.33):

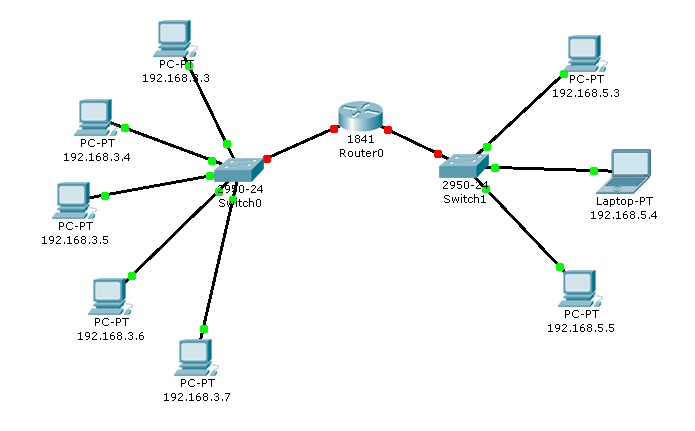


Рис. 4.33 Вид рабочей области

1. Настройка маршрутизатора

При настройке конечных узлов уже упоминалось о том, что маршрутизатор в данной топологии сети имеет два интерфейса. Произведем настройку интерфейса FastEthernet0/0:

1. Один клик по устройству (маршрутизатору);
2. Выбираем вкладку “Config”;
3. Находим интерфейс FastEthernet0/0, задаем нужный IP-адрес и маску подсети (рис. 4.34).

**Важно: интерфейс маршрутизатора, по умолчанию, отключен; необходимо его включить, кликнув мышкой рядом с “On”.**

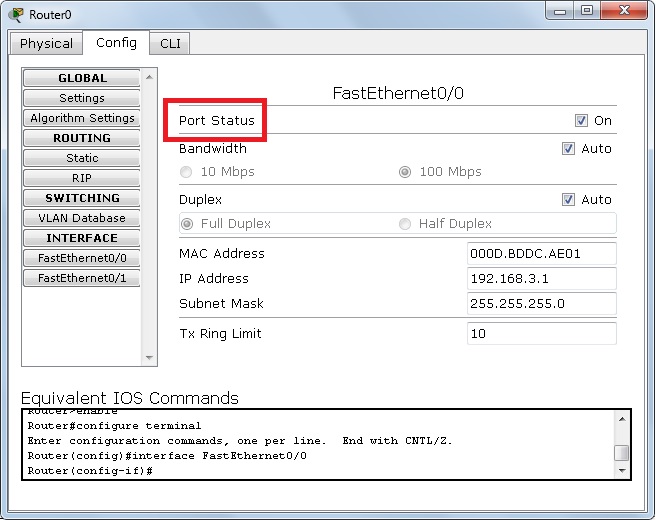


Рис. 4.34 Настройка интерфейса маршрутизатора

1. Закрываем окно, смотрим на всю топологию сети. Зеленые индикаторы состояния на линии связи между Router0 и Switch0 сигнализируют, что интерфейс подключен правильно (рис. 4.35).

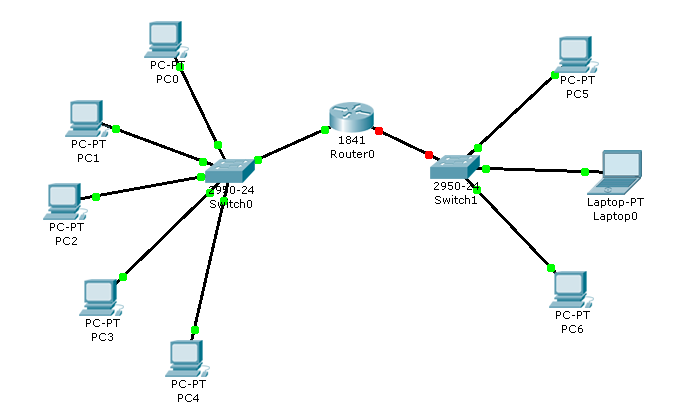


Рис. 4.35 Вид рабочей области

Аналогично производим настройку интерфейса FastEthernet0/1 (рис. 4.36).

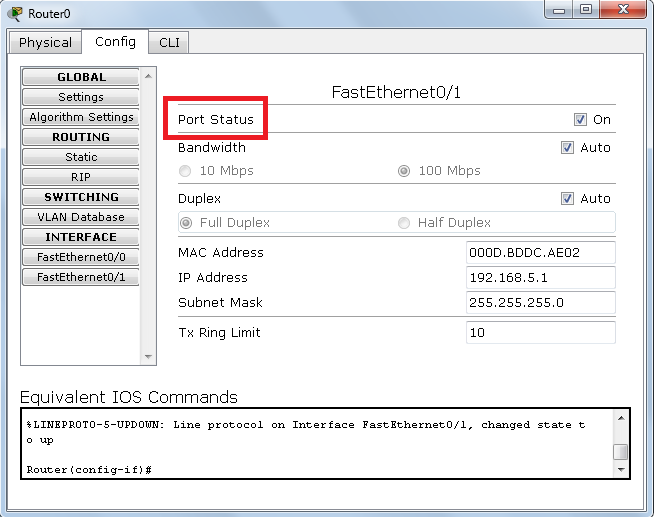


Рис. 4.36 Настройка интерфейса маршрутизатора

Сделать надписи к интерфейсам маршрутизатора, можно с помощью инструмента Place Note на панели Common Tools . Необходимо кликнуть на инструмент, затем сделать клик в нужном месте на рабочей области.

1. Режим симуляции Cisco Packet Tracer

Убедитесь, что вы находитесь в режиме симуляции. Для этого кликните на иконку симуляции в правом нижнем углу рабочей области симулятора. Описание: 8.png

Откроется окно событий, в котором вы увидите список событий, управляющие кнопки, заданные фильтры (рис. 4.37). По умолчанию, фильтруются, т.е. будут отображаться, пакеты всех возможных протоколов, необходимо поправить и ограничить этот список до исследуемых протоколов.

Управляющие кнопки:

* Back – назад
* Auto Capture/Play – автоматический захват пакетов от источника до приемника и обратно
* Capture/Forward – захват пакетов только от одного устройства до другого

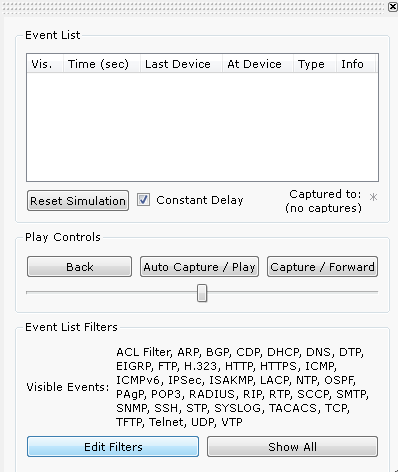


Рис. 4.37 Окно событий режима симуляции

В данной лабораторной работе нас интересуют пакету двух типов ARP и ICMP.

Следовательно, нужно поставить фильтр только на сообщения заданного типа (рис. 4.38):

1. Нажимаем на кнопку “Edit Filters”
2. Снимаем метку с “Show All/None”
3. Выбираем ARP и ICMP

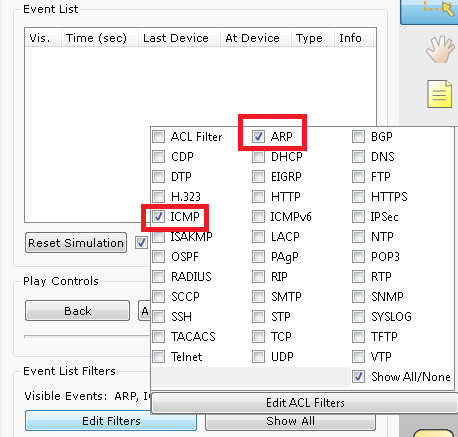


Рис. 4.38 Добавление фильтров на протоколы ARP и ICMP

1. Убедимся, что заданные протоколы для фильтрации назначены (рис. 4.39)

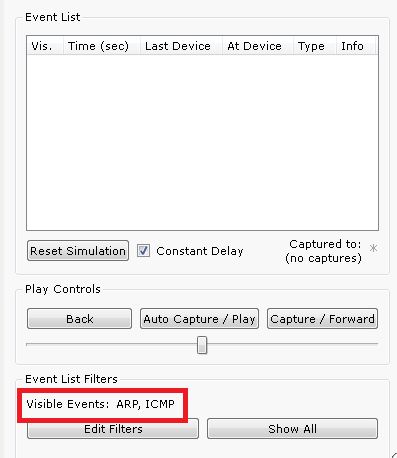


Рис. 4.39 Окно событий режима симуляции

1. Проверка работы сети в режиме симуляции

Отправим тестовый ping-запрос с конечного узла c IP-адресом 192.168.3.3 на хост с IP-адресом 192.168.3.5.

**Важно: оба узла находятся в пределах одного сегмента сети**

1. Один клик по выбранному устройству (рис. 4.40)

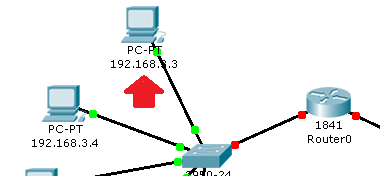


Рис. 4.40 Выбор узла 192.168.3.3

1. Выбираем вкладку Desktop, в которой содержатся симуляторы некоторых программ, доступных на компьютере (см. рис. 3.4).
2. Выбираем “Command Prompt”, программу, имитирующую командную строку компьютера.
3. С помощью утилиты ping отправляем ping-запрос (рис. 4.41). (Не забудьте нажать Enter).

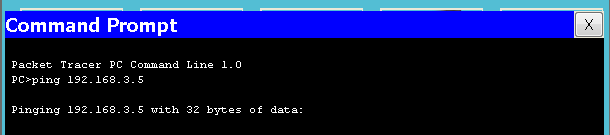


Рис. 4.41 Командная строка узла 192.168.3.3

На устройстве-источнике формируются два пакета протокола ARP и ICMP (рис. 4.42). ARP-запрос возникает всегда, когда хост пытается связаться с другим хостом.

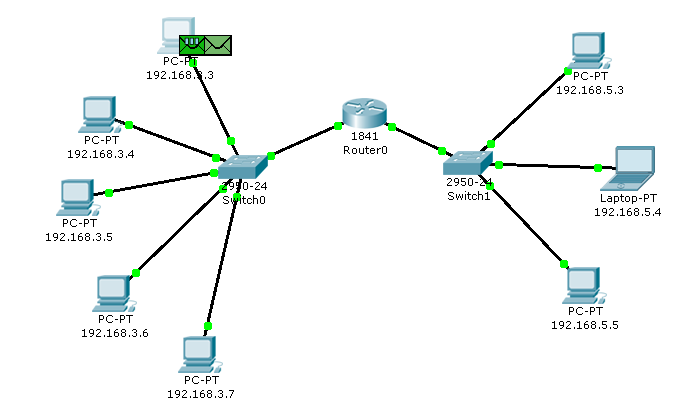


Рис. 4.42 Вид рабочей области

Нажимаем на кнопку “Auto Capture/play” или “Capture/Forward”, последняя позволит вам управлять движением пакетов от устройства к устройству самим. Видим, что первым отправляется пакет протокола ARP, так как ARP-таблица хоста 192.168.3.3 пуста, и он еще «не знает», кому отправлять ping-запрос. Сделайте один клик по самому пакету (конверту), ознакомьтесь, какие уровни модели OSI задействованы. Перейдите к вкладке “Inbound PDU Details”, которая содержит структуру пакета (рис. 4.43).

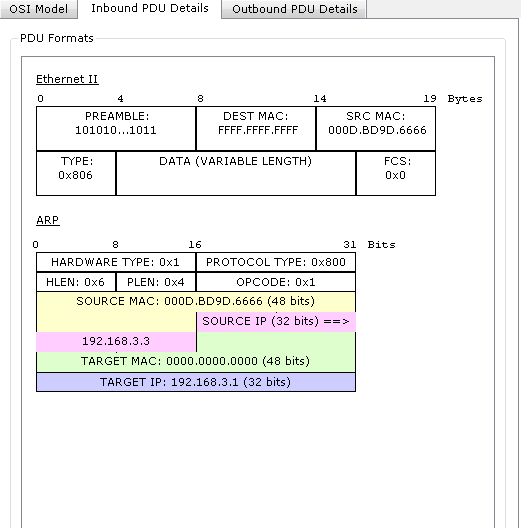


Рис. 4.43 Формат пакета ARP-запроса

Узел 192.168.3.3 построил запрос и посылает его широковещательным сообщением всем хостам подсети. Помимо IP-адреса назначения, запрос содержит IP-адрес и МАС-адрес отправителя, чтобы приемная сторона могла ответить.

При просмотре прохождения пакетов убедитесь, что на ARP-запрос ответит только хост 192.168.3.5. Каждый хост в подсети получает запрос и проверяет на соответствие свой IP-адрес. Если он не совпадает с указанным адресом в запросе, то запрос игнорируется (рис. 4.44).

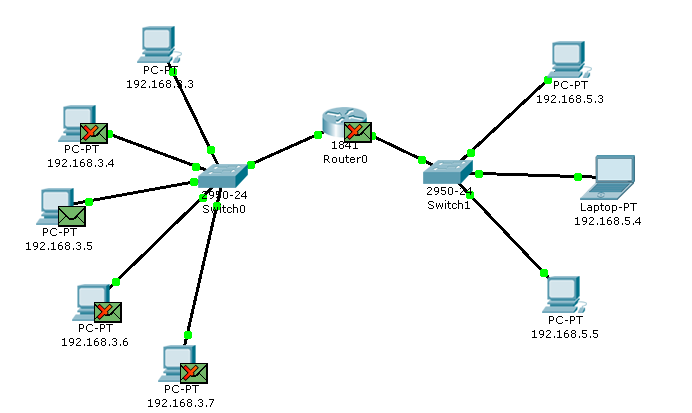


Рис. 4.44 Вид рабочей области

Посмотрите содержимое пакета ARP-ответа, пришедшего на хост 192.168.3.3 (рис. 4.45).

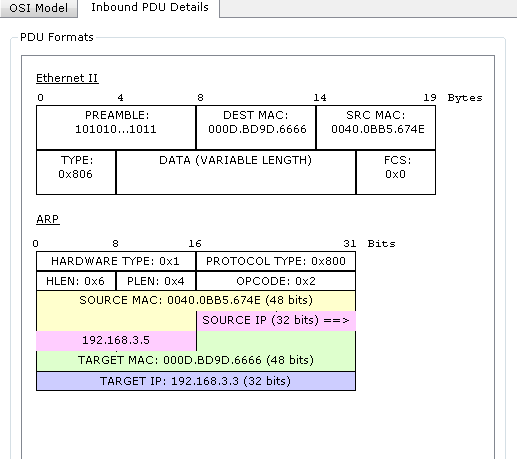


Рис. 4.45 Формат пакета ARP-ответа

Узел 192.168.3.5. послал ARP-ответ непосредственно отправителю, используя его МАС-адрес, с указанием собственного МАС-адреса в поле “Target МАС”.

Далее отправляется ICMP-сообщение ping-запроса. Посмотрите содержимое пакета, сделав клик по пакету (конверту) (рис. 4.46).

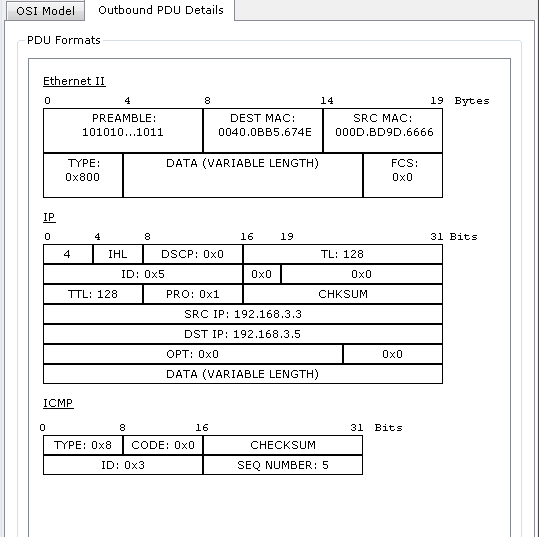


Рис. 4.46 Формат пакета ICMP-эхо-запроса

Физические адреса узлов известны. IP-адрес источника – 192.168.3.3. IP-адрес назначения – 192.168.3.5. Тип ICMP-сообщения – 8 (эхо-запрос).

Запрос производится на хост 192.168.3.5 через коммутатор (рис. 4.47).

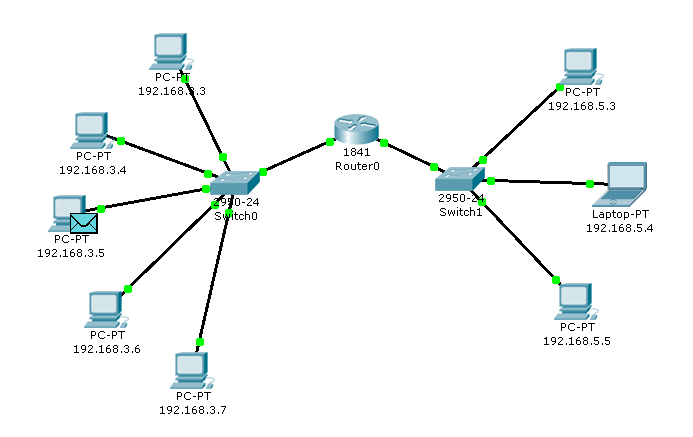


Рис. 4.47 Вид рабочей области

Посмотрите содержимое пакета ping-ответа, пришедшего на хост 192.168.3.3 (рис. 4.48).

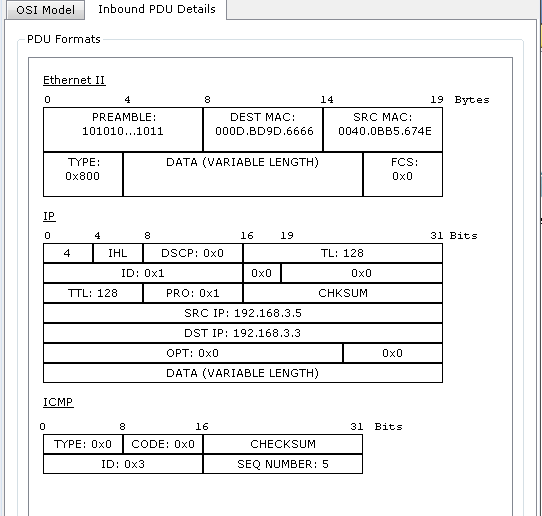


Рис. 4.48 Формат пакета ICMP-эхо-ответа

IP-адрес источника – 192.168.3.5. IP-адрес назначения – 192.168.3.3. Тип ICMP-сообщения – 0 (эхо-ответ).

Посмотрите ping-ответ в командной строке хоста 192.168.3.3 (рис. 4.49).

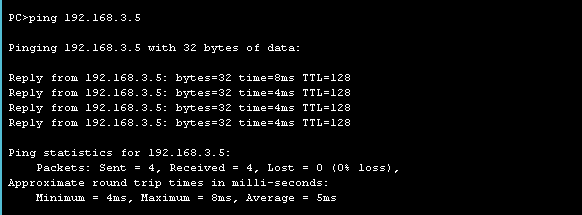


Рис. 4.49 Вывод программы ping

В окне событий так же указаны маршруты запроса ARP и ICMP: через какие устройства прошли пакеты (рис. 4.50).

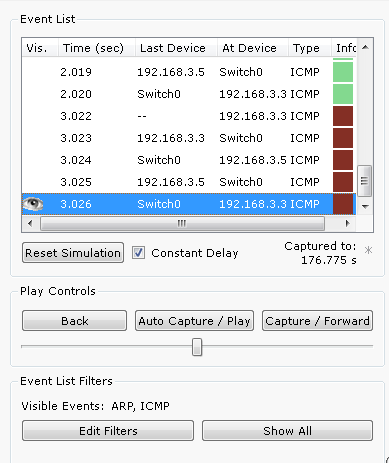


Рис. 4.50 Окно событий режима симуляции

Удалить сценарий симуляции можно с помощью кнопки “Reset Simulation” или воспользоваться кнопкой “Delete” в области User Created Packet Window.

Теперь ARP-таблицы хостов 192.168.3.3 и 192.168.3.5 не пусты, в них содержится одна запись. Чтобы просмотреть содержимое ARP-таблицы, нужно выполнить команду

“arp –a” в командной строке.

Содержимое ARP-таблицы узла 192.168.3.3 (рис. 4.51):

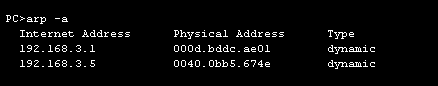


Рис. 4.51 ARP-таблица узла 192.168.3.3 в командной строке

Можно воспользоваться другим способом: нажать на кнопку «Inspect» , нажать на выбранное устройство, выбрать «ARP table» и просмотреть записи ARP-таблицы узла (рис. 4.52).

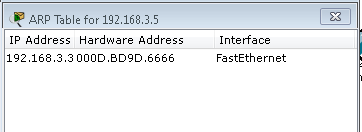


Рис. 4.52 ARP-таблица узла 192.168.3.5, показанная с помощью инструмента «Inspect»

Если снова задать ping-запрос на хост 192.168.3.5, то сразу будет сформирован только один пакет ICMP-сообщения, т.к. в ARP-таблице компьютера-источника уже хранится соответствующий локальный адрес.

Попробуйте отправить ping-запрос снова.

Чтобы удалить все записи ARP-таблицы, следует воспользоваться командой “arp –d”.

1. Посылка ping-запроса во внешнюю сеть

Отправим тестовый ping-запрос с конечного узла c IP-адресом 192.168.3.4 на хост с IP-адресом 192.168.5.5.

**Важно: один узел пытается передать пакет другому узлу, находящемуся с ним в разных сетях.**

В пункте 5 лабораторной работы был рассмотрен случай посылки ARP-запроса внутри локальной сети. Протокол ARP в этом случае определял непосредственно МАС-адрес узла-приемника запроса. Теперь рассмотрим ситуацию, когда узел-источник и узел-приемник находятся в разных сетях. Протокол ARP работает в пределах сегмента сети, поэтому в данном случае он будет использоваться для определения МАС-адреса маршрутизатора. Таким образом, пакет будет передан маршрутизатору для дальнейшей ретрансляции.

Открываем “Command Promt”, имитирующую командную строку, на компьютере 192.168.3.4 и посылаем на хост 192.168.5.5. ping-запрос (рис. 4.53).

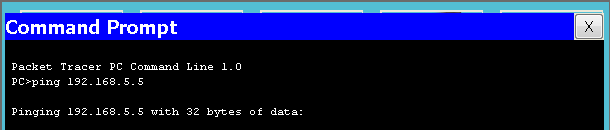


Рис. 4.53 Командная строка узла 192.168.3.4

В этом случае инициируется ARP-запрос маршрутизатору, который пересылает пакеты в сеть назначения. На узле-источнике формируются два пакета протокола ARP и ICMP (рис. 4.54).

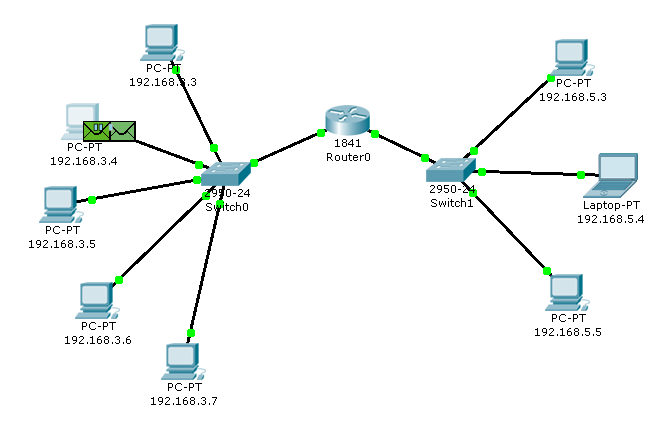


Рис. 4.54 Вид рабочей области

Формат пакета ARP-запроса содержит те же сведения, что и для разрешения локального адреса устройства, и рассылается широковещательно всем узлам подсети (рис. 4.55).

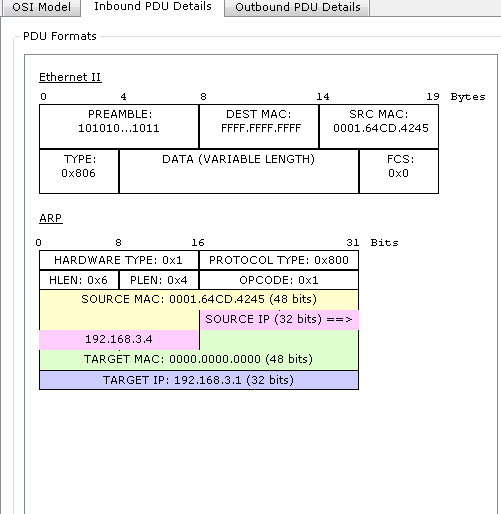


Рис. 4.55 Формат пакета ARP-запроса

Все узлы игнорируют пакет, кроме маршрутизатора, которому этот пакет предназначался (рис. 4.56).

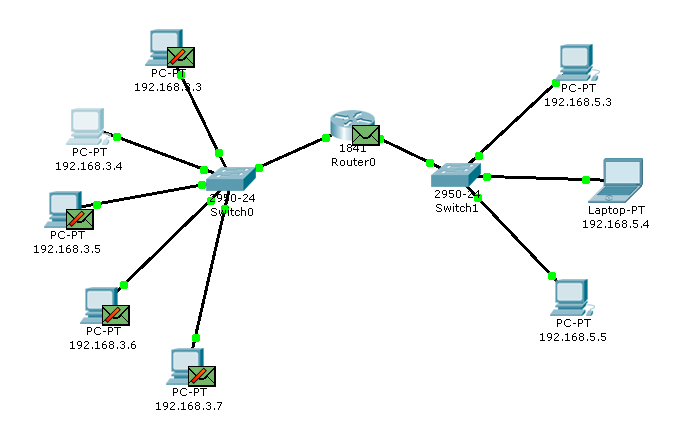


Рис. 4.56 Вид рабочей области

Маршрутизатор формирует ARP-ответ, указывая свой физический адрес, и отправляет его узлу 192.168.3.4 (рис. 4.57).

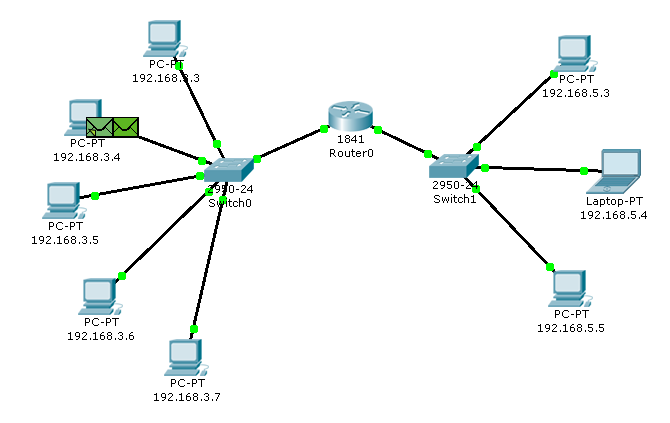


Рис. 4.57 Вид рабочей области

После получения ARP-ответа хост 192.168.3.4 посылает ICMP-сообщение ping-запроса через маршрутизатор в сеть назначения.

Посмотрите содержимое пакета, сделав клик по пакету (конверту) (рис. 4.58).

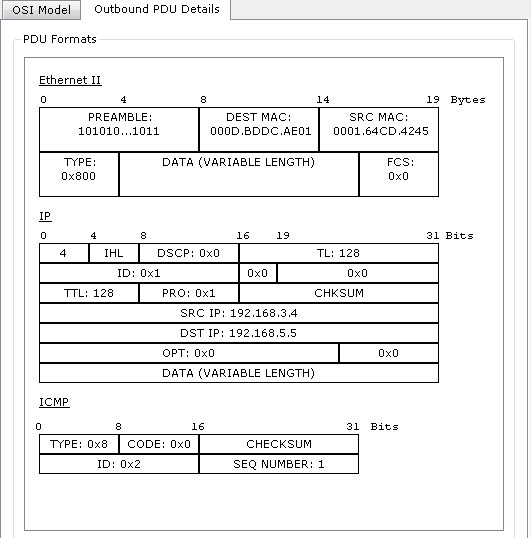


Рис. 4.58 Формат пакета ICMP-эхо-запроса

IP-адрес источника – 192.168.3.4. IP-адрес назначения – 192.168.5.5. Тип ICMP-сообщения – 8 (эхо-запрос).

Когда запрос приходит в сеть назначения, то маршрутизатор определяет МАС-адрес получателя, если такового нет в ARP-таблице маршрутизатора. Таким образом, снова решается задача разрешения локального адреса (рис. 4.59).

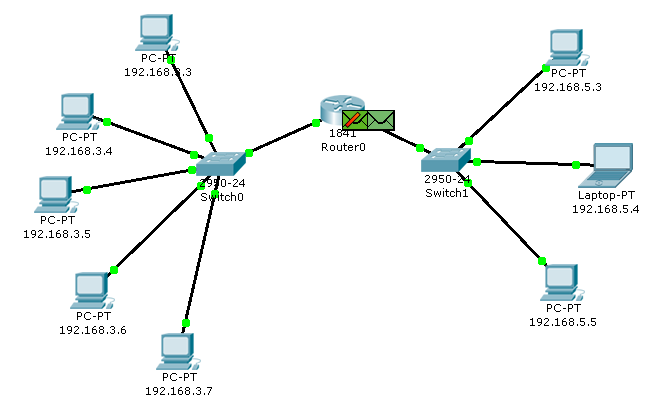


Рис. 4.59 Вид рабочей области

Маршрутизатор вынужден сперва узнать физический адрес получателя, прежде чем он сможет отправить ping-запрос по назначению, поэтому пакет с ping-запросом, пришедший на маршрутизатор, отклонен.

Новый ARP-запрос отправляется широковещательным сообщением от маршрутизатора, содержит его IP-адрес и МАС-адрес (рис. 4.60). IP-адрес назначения – узел 192.168.5.5.

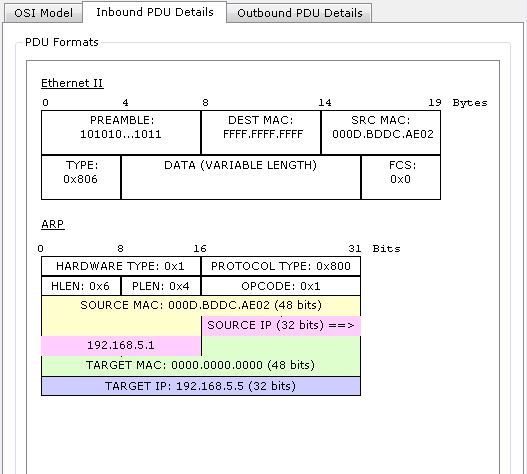


Рис. 4.60 Формат пакета ARP-запроса

Узлы подсети, которым пакет не предназначен, его игнорируют (рис. 4.61).

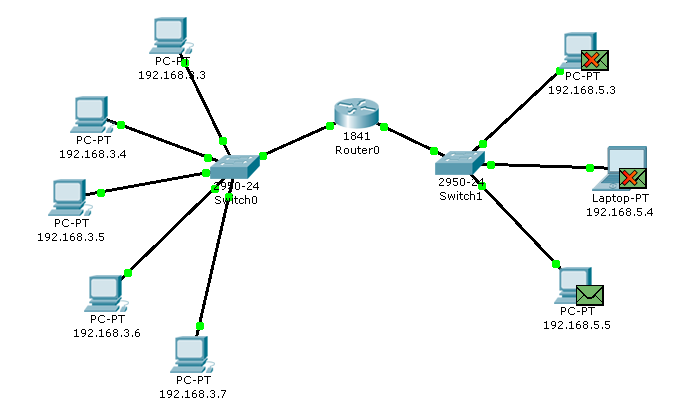


Рис. 4.61 Вид рабочей области

Узел 192.168.5.5. формирует ARP-ответ и отправляет его обратно маршрутизатору (рис. 4.62), указав свой МАС-адрес, о чем свидетельствует содержимое пакета (рис. 4.63).

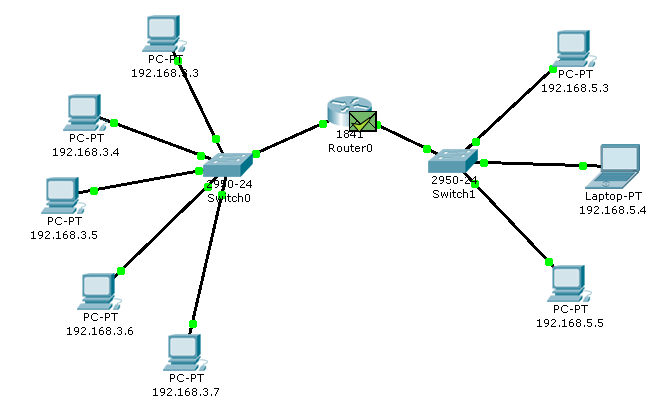


Рис. 4.62 Вид рабочей области

После того, как маршрутизатор определил МАС-адрес получателя входящего ping-запроса, он посылает ICMP-ответ маршрутизатору хоста отправителя. (В данном случае это тот же маршрутизатор Router0).

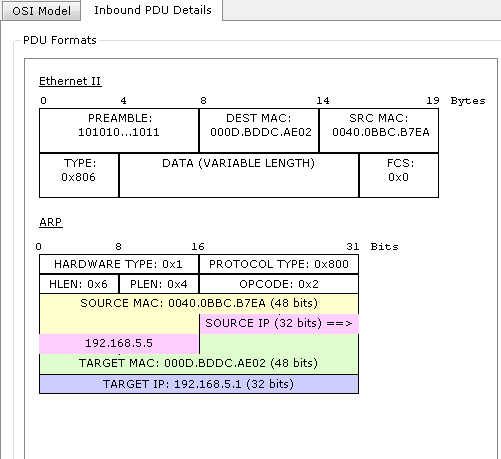


Рис. 4.63 Формат пакета ARP-ответа

Узел 192.168.3.4. снова пытается отправить ping-запрос во внешнюю сеть узлу 192.168.5.5. Его маршрут должен лежать через коммутатор Switch0, маршрутизатор Router0, коммутатор Switch1 и достигнуть узла назначения (рис. 4.64). Проследите маршрут пакета самостоятельно.

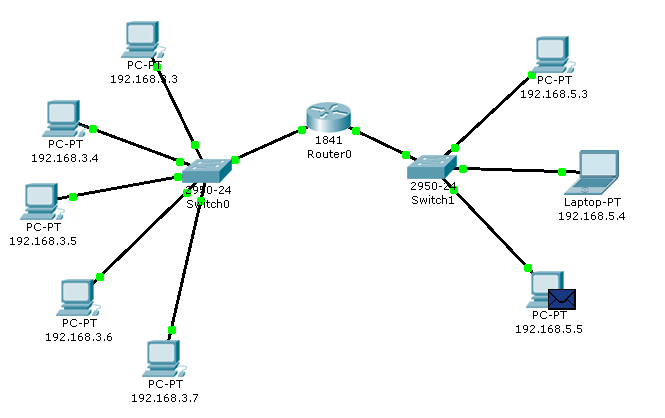


Рис. 4.64 Вид рабочей области

Узел формирует ping-ответ, который отправляется обратно узлу 192.168.3.4 (рис. 4.65).

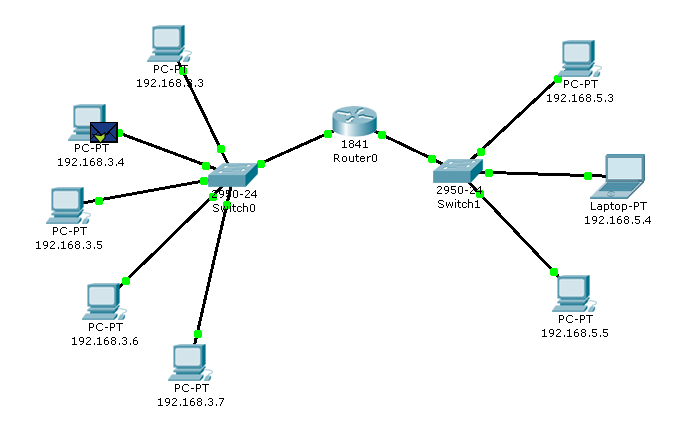


Рис. 4.65 Вид рабочей области

Посмотрите содержимое пакета ping-ответа, пришедшего на хост 192.168.3.4 (рис. 4.66).

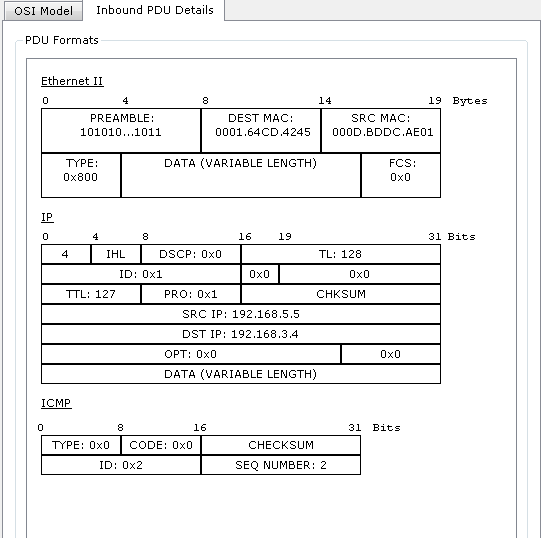


Рис. 4.66 Формат пакета ICMP-эхо-ответа

IP-адрес источника – 192.168.5.5. IP-адрес назначения – 192.168.3.4. Тип ICMP-сообщения – 0 (эхо-ответ).

Посмотрите ping-ответ в командной строке хоста 192.168.3.4 (рис. 4.67).

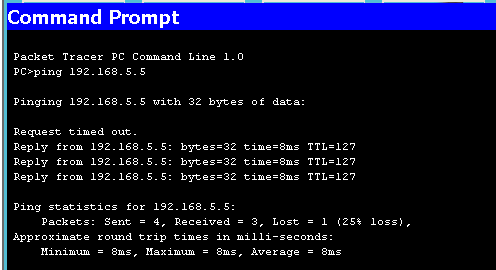


Рис. 4.67 Вывод программы ping

Маршрут пакета можно посмотреть с помощью команды tracert. Выполним эту команду, например, в командной строке компьютера 192.168.3.5 (рис. 4.68):

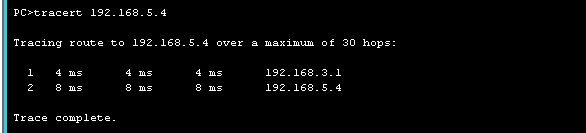


Рис. 4.68 Вывод программы tracert

На пути пакета до хоста 192.168.5.4 один промежуточный маршрутизатор.

1. Посылка ping-запроса на несуществующий хост

Отправим ping-запрос на несуществующий адрес в сеть 192.168.5.0/24.

Откроем программу “Command Promt” на узле 192.168.3.7 и попробуем отправить ping-запрос на несуществующий хост с IP-адресом 192.168.5.6 (рис. 4.69).

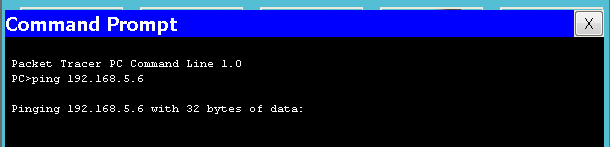


Рис. 4.69 Командная строка узла 192.168.3.7

ARP-таблица на узле-источнике не содержит соответствующей записи о МАС-адресе узла 192.168.5.6, поэтому формируется ARP-запрос (рис. 4.70).

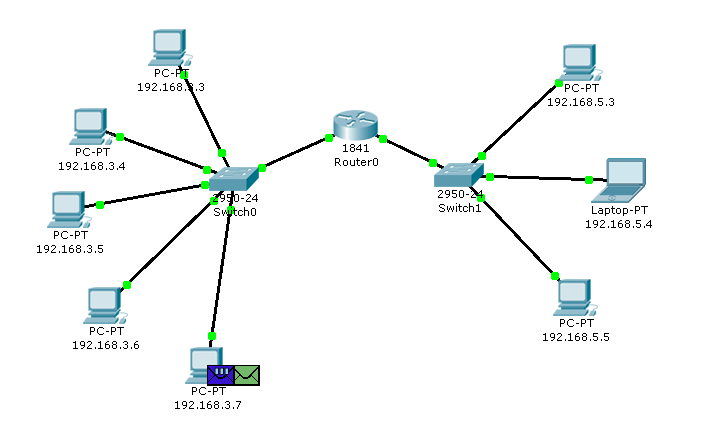


Рис. 4.70 Вид рабочей области

Все узлы игнорируют пакет, кроме маршрутизатора, которому этот пакет предназначался (рис. 4.71).

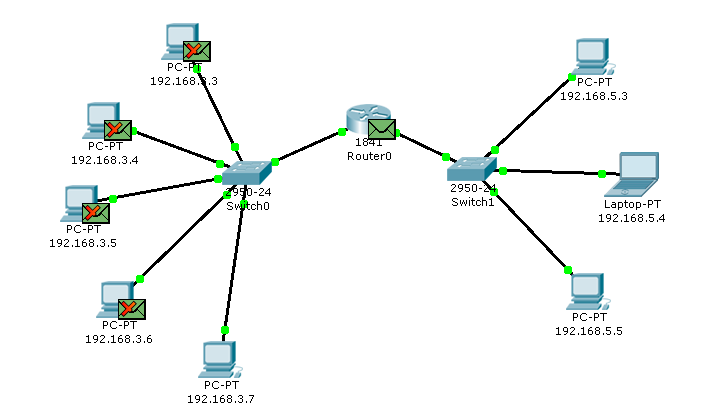


Рис. 4.71 Вид рабочей области

Узел 192.168.3.7 получает ARP-ответ с МАС-адресом маршрутизатора. Теперь, зная его аппаратный адрес, хост отправляет ping-запрос на узел 192.168.5.6 (рис. 4.72).

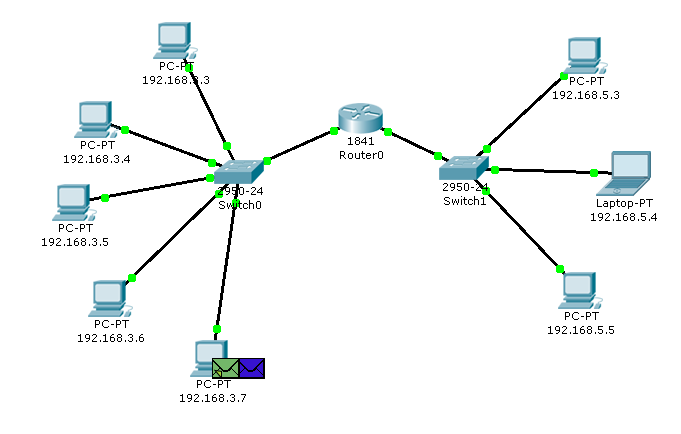


Рис. 4.72 Вид рабочей области

Маршрутизатор пришедший пакет уничтожает, т.к. не может его перенаправить на указанный адрес, потому что соответствующего МАС-адреса он «не знает». В связи с этим маршрутизатор формирует ARP-запрос по адресу 192.168.5.6 (рис. 4.73).

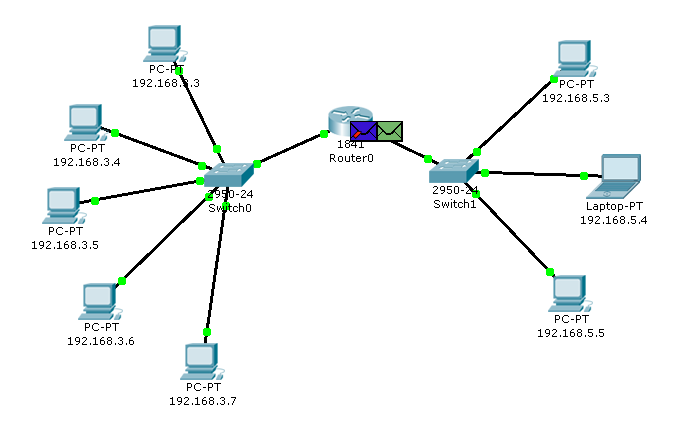
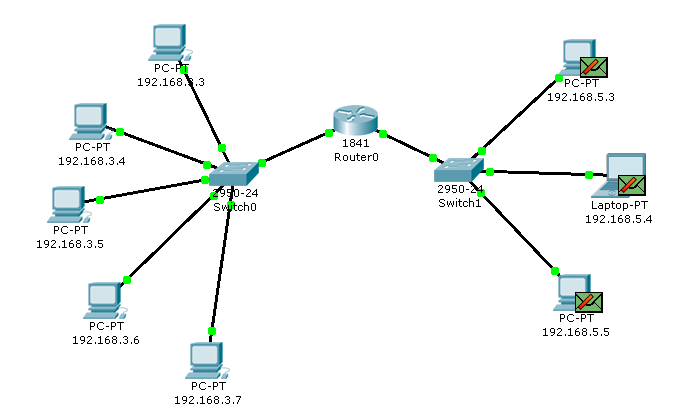


Рис. 4.73 Вид рабочей области

Все узлы подсети игнорируют пакет, потому что IP-адрес в запросе не соответствует их собственным (рис. 4.74). Маршрутизатор ни какого ответа ни от кого не получает.

программный лабоРис. 4.74 Вид рабочей области

Процедура прохождения пакетов повторяется в течение всего сценария симуляции: маршрутизатор по-прежнему «не знает» МАС-адрес указанного в ping-запросе IP-адреса 192.168.5.6 и продолжает рассылать ARP-запросы. Ни один из узлов подсети на эти запросы не реагирует. Не получив ответа, маршрутизатор и сам «молчит», никак не уведомляя об ошибке хост-источник ping-запроса.

Примечание: на самом деле в данном случае маршрутизатору следует отправить ICMP-сообщение «хост недостижим»: сообщение типа 3 с кодом 1. Однако проведенный эксперимент с теорией разошелся.

Посмотрим ответ на ping-запрос в командной строке узла-источника 192.168.3.7: «превышено время ожидания» (рис. 4.75).

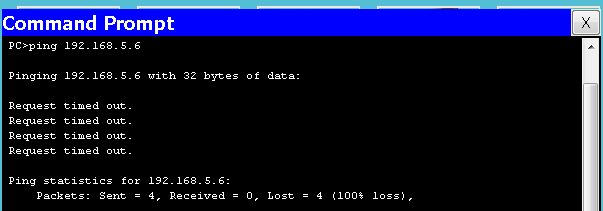


Рис. 4.75 Вывод программы ping

Попробуем отправить ping-запрос, содержащий IP-адрес узла, в сеть, на которую нет маршрута.

Откроем программу “Command Promt” на узле 192.168.3.6 и попробуем отправить ping-запрос на несуществующий хост с IP-адресом 192.168.6.6 (рис. 4.76).

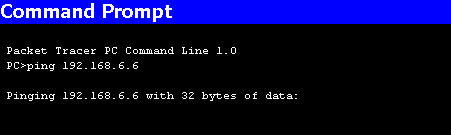


Рис. 4.76 Командная строка узла 192.168.3.6

Так как ARP-таблица узла-источника соответствующей записи не имеет, формируется ARP-запрос на заданный узел с IP-адресом 192.168.6.6 (рис. 4.77).

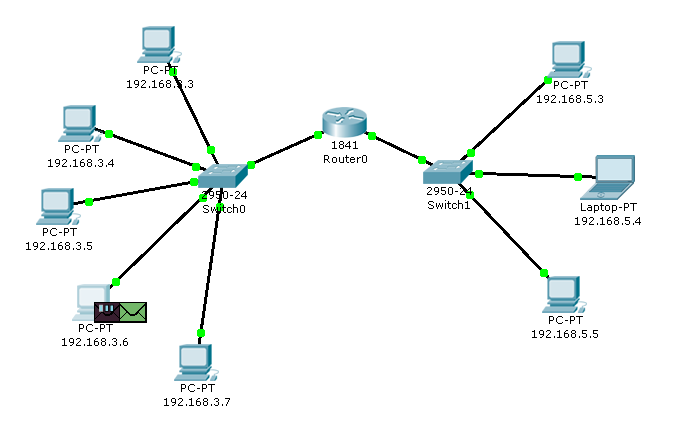


Рис. 4.77 Вид рабочей области

Все узлы игнорируют пакет, кроме маршрутизатора, которому этот пакет предназначался (рис. 4.78).

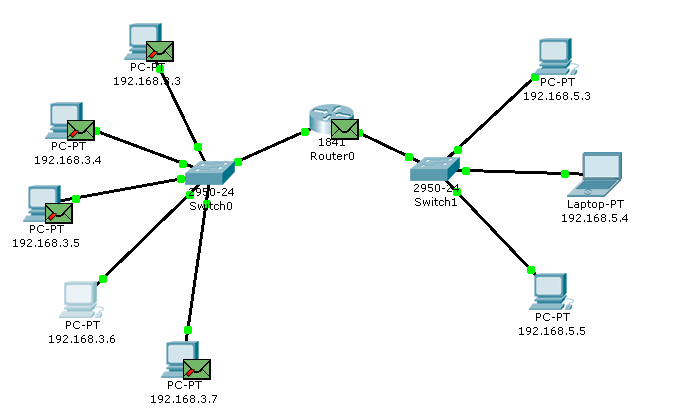


Рис. 4.78 Вид рабочей области

Узел 192.168.3.6 получает ARP-ответ с МАС-адресом маршрутизатора. Теперь, зная его аппаратный адрес, хост отправляет ping-запрос (рис. 4.79).

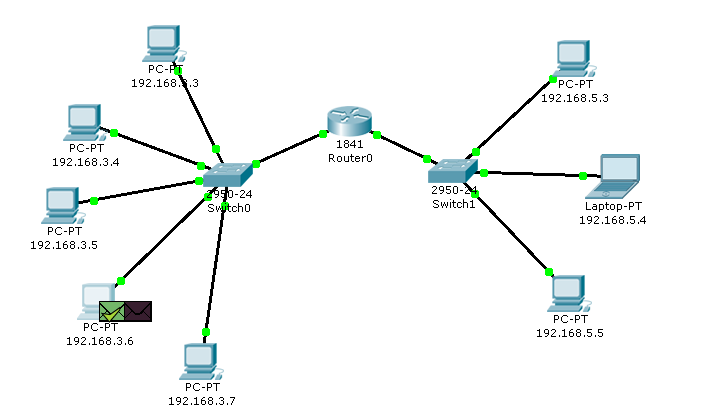


Рис. 4.79 Вид рабочей области

Когда ping-запрос попадает на маршрутизатор, тот не может его перенаправить не на какой из своих интерфейсов, т.к. IP-адреса его интерфейсов не совпадают с тем адресом, который указан в ping-запросе. Соответственно, этот пакет уничтожается и формируется новое ICMP-сообщение (рис. 4.80).

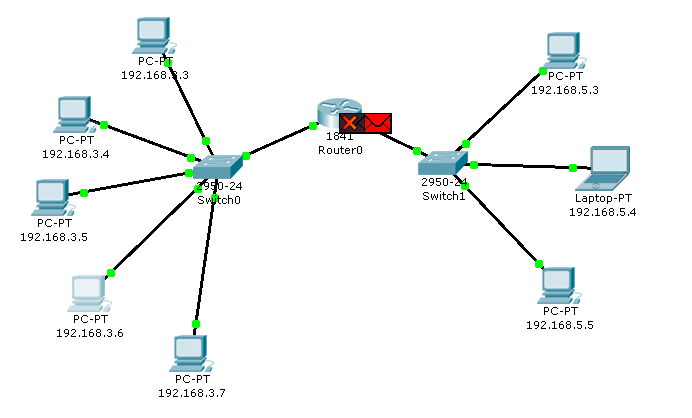


Рис. 4.80 Вид рабочей области

Посмотрим содержимое пакета, сформированного маршрутизатором (рис. 4.81).

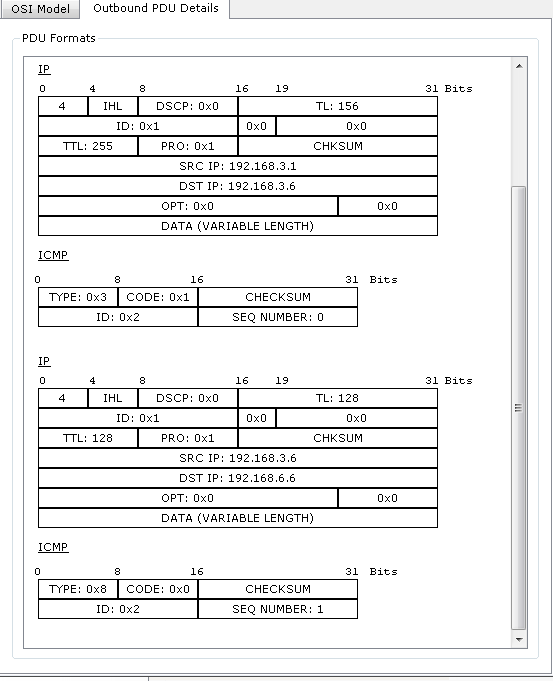


Рис. 4.81 Формат пакета ICMP «хост недостижим»

IP-адрес источника – 192.168.3.1. IP-адрес назначения – 192.168.3.6. Тип ICMP-сообщения – 3 с кодом 1, что означает «хост недостижим». Этот пакет приходит на узел 192.168.3.6.

Результат ping-запроса в командной строке узла 192.168.3.6: «хост назначения недостижим» (рис. 4.82).

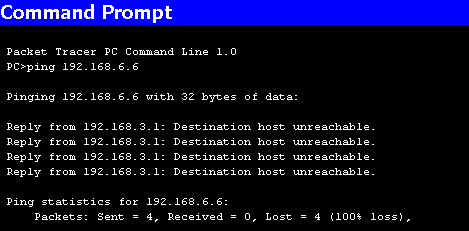


Рис. 4.82 Вывод программы ping

Таким образом, маршрутизатор «ответил» на ping-запрос, для которого у него не было соответствующего маршрута, новым ICMP-сообщением «хост недостижим».

Примечание: корректно ли отреагировал маршрутизатор в данной ситуации, отправив на хост-источник ping-запроса ICMP-сообщение «хост недостижим»? Чтобы ответить на этот вопрос, необходимо обратиться к спецификации протокола ICMP RFC 792 и ознакомится с другими типами ICMP-сообщений. [Электронный ресурс]. URL: <http://tools.ietf.org/html/rfc792>.

1. **Индивидуальные задания**

В соответствии с вариантом отфильтруйте ARP и ICMP сообщения для указанных пар «источник – приемник». В каждом варианте предусмотрены 2 варианта ping-запроса: внутри сети и во внешнюю сеть. С помощью команды tracert посмотрите маршрут пакета, адресованного во внешнюю сеть.

В отчете для каждого теста приведите маршруты пакетов, их содержимое и объясните полученные результаты.

Варианты заданий представлены в приложении 1.

# Лабораторная работа №3. Протоколы SMTP и POP3

**Цель работы:** изучить принципы организации взаимодействия прикладных программ с помощью протоколов электронной почты SMTP и POP3 в режиме симуляции Cisco Packet Tracer.

**Программа работы:**

1. Построение топологии сети, настройка сетевых устройств;
2. Настройка почтового сервера;
3. Исследование прикладных почтовых протоколов в режиме симуляции;
4. Отправка письма по протоколу SMTP на сервер;
5. Получение письма по протоколу POP3 от сервера;
6. Выполнение индивидуального задания.

**Теоретические сведения:**

**Протоколы SMTP и POP3**

Схема взаимодействия с прикладными почтовыми протоколами представлена на рис. 4.83.

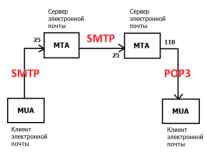


Рис. 4.83 Схема взаимодействия с прикладными почтовыми протоколами

Mail Transfer Agent (MTA) – агент передачи почты, являющийся основным компонентом системы передачи почты, представляет данный компьютер для сетевой системы электронной почты. Обычно пользователи не работают непосредственно с MTA, а используют Mail User Agent (MUA) – клиент электронной почты.

Для передачи сообщений по TCP-соединению большинство почтовых агентов пользуются протоколом Simple Mail Transfer Protocol (SMTP).

SMTP принят в качестве стандартного метода передачи электронной почты в сети Internet. Действующий стандарт протокола описан в RFC 2821. В качестве транспортного протокола SMTP использует TCP, соединение устанавливается через порт с номером 25. Для обслуживания этого соединения используется специальная программа, которая именуется почтовым сервером. Для формирования сообщения и установления соединения используется почтовая программа пользователя. После установления соединения обмен информацией происходит посредством команд. Для пользователя эти команды не доступны, если при работе он использует клиент электронной почты [5].

Главной целью протокола SMTP является надежная и эффективная доставка электронных почтовых сообщений. Для реализации протокола требуется только надежный канал связи. Средой для SMTP может служить отдельная локальная сеть, система сетей или же всемирная сеть Internet.

Эта передача обычно осуществляется непосредственно с хоста отправителя на хост получателя, когда оба хоста используют один транспортный сервис. Если же хосты не подключены к общей транспортной системе, передача осуществляется с использованием одного или нескольких промежуточных серверов SMTP. Сегодня в Internet обычной практикой является представление исходного сообщения промежуточному серверу, который выполняет некоторые дополнительные функции. Промежуточный сервер в таких случаях действует как шлюз в другие среды передачи и выбирается обычно с использованием MX-записей DNS (служба доменных имен).

Протокол SMTP базируется на следующей модели коммуникаций: в ответ на запрос пользователя почтовая программа-отправитель сообщения устанавливает двустороннюю связь с программой-приемником (почтовым сервером). Получателем может быть оконечный или промежуточный адресат. Если необходимо, почтовый сервер может установить соединение с другим сервером и передать сообщение дальше.

Для того чтобы получить сообщение из своего почтового ящика, почтовая программа пользователя соединяется с сервером уже не по протоколу SMTP, а по специальному почтовому протоколу получения сообщений. Такой протокол позволяет работать с почтовым ящиком: забирать сообщения, удалять сообщения, сортировать их и выполнять другие операции. Самым популярным в настоящее время протоколом такого рода является протокол Post Office Protocol v.3 (POP3).

Многие концепции, принципы и понятия протокола POP3 выглядят и функционируют подобно SMTP: взаимодействие происходит посредством команд. Сервер POP3 находится между агентом пользователя и почтовыми ящиками.

Он предусматривает соединение с почтовым сервером на основе транспортного протокола TCP через порт 110. Спецификация РОР3 определена в документе RFC 1939. PОРЗ разработан с учетом специфики доставки почты на персональные компьютеры и имеет соответствующие операции для этого [6].

Конструкция протокола РОР3 обеспечивает возможность пользователю обратиться к своему почтовому серверу и изъять накопившуюся для него почту. Пользователь может получить доступ к РОР3-серверу из любой точки доступа к Internet. При этом он должен запустить специальный почтовый агент, работающий по протоколу РОР3, и настроить его для работы со своим почтовым сервером. Сообщения доставляются клиенту по протоколу POP3, а посылаются при помощи SMTP. То есть на компьютере пользователя существуют два отдельных агента-интерфейса к почтовой системе – доставки (POP3) и отправки (SMTP).

**Служба DNS**

Данная лабораторная работа посвящена изучению прикладных протоколов электронной почты SMTP и POP3. Однако взаимодействие с системой электронной почты невозможно без системы доменных имен (DNS). В задачи службы DNS входит:

1. Преобразование символических имен в IP-адреса;
2. Преобразование IP-адресов в символические имена.

Дополнительной функцией DNS является маршрутизация почты. Основная спецификация распределенной службы DNS указана в RFC 1034 и RFC 1035. [Электронный ресурс]. URL: <http://www.ietf.org/rfc/rfc1034.txt>. URL: <http://www.ietf.org/rfc/rfc1035.txt>.

Единицами хранения и передачи информации в DNS являются ресурсные записи. Существует множество типов ресурсных записей, каждая из которых состоит из определенного числа полей. Для маршрутизации почты используется запись “MX”, при ее отсутствии запись типа “А”. Запись “A” (адресная запись) содержит параметры: доменное имя узла, соответствующий IP-адрес.

Пример: aivt IN A 195.19.212.16, где “IN” – это класс записи (интернет).

Запись “MX” содержит параметры: имя почтового домена, имя почтового сервера, приоритет.

Пример: aivt IN MX 20 mail.stu.neva.ru, где “IN” – это класс записи (интернет). [4]

При получении письма MTA анализирует его служебную информацию, в частности заголовок письма, определяя домен получателя (см. рис. 4.83). Если он относится к домену, который обслуживается данным МТА, производится поиск получателя и письмо помещается в его ящик.Если домен получателя не обслуживается этим MTA, формируется DNS-запрос, запрашивающий MX-записи для данного домена. MX-запись представляет особый вид DNS-записи, которая содержит имена почтовых серверов, обрабатывающих входящую почту для данного домена. MX-записей может быть несколько, в этом случае MTA пробует последовательно установить соединение, начиная с сервера с наибольшим приоритетом. При отсутствии MX-записи запрашивается A-запись (запись адреса, сопоставляющая доменное имя с IP-адресом) и выполняется попытка доставить почту на указанный там хост. При невозможности отправить сообщение, оно возвращается отправителю (помещается в почтовый ящик пользователя) с сообщением об ошибке. [8]

**Выполнение работы:**

1. Построение топологии сети

Для исследования заданных прикладных протоколов построим тестовую топологию сети следующего вида (рис. 4.84):

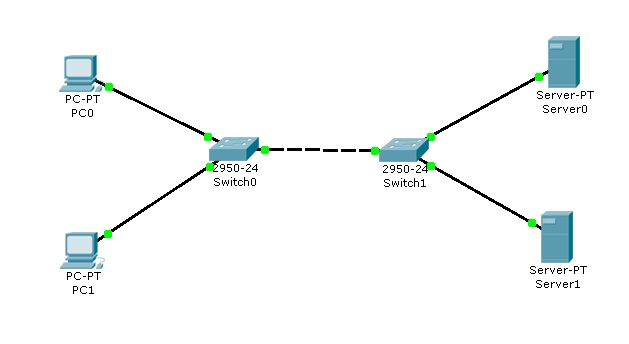


Рис. 4.84 Тестовая топология сети

Производим настройку сетевых устройств согласно заданным параметрам (таблица 4.4, таблица 4.5):

Таблица 4.4

|  |  |  |  |
| --- | --- | --- | --- |
| Конечные узлы | IP-адрес | Маска сети | IP-адрес DNS-сервера |
| PC0 | 172.16.0.90 | 255.255.0.0 | 172.16.0.20 |
| PC1 | 172.16.0.100 | 255.255.0.0 | 172.16.0.20 |

Таблица 4.5

|  |  |  |  |
| --- | --- | --- | --- |
| Серверы | IP-адрес | Маска сети | IP-адрес DNS-сервера |
| Server0 | 172.16.0.20 | 255.255.0.0 | 172.16.0.20 |
| Server1 | 172.16.0.40 | 255.255.0.0 | 172.16.0.20 |

Все устройства расположены в одном сегменте локальной сети, поэтому маршрутизация пакетов не используется, значит, IP-адрес шлюза по умолчанию указывать необязательно.

1. Настройка почтового сервера

В качестве серверов электронной почты выступают сервер 172.16.0.20 и сервер 172.16.0.40. Схема взаимодействия с прикладными почтовыми протоколами применительно к построенной сети представлена на рис. 4.85:

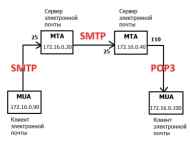


Рис. 4.85 Схема взаимодействия с прикладными почтовыми протоколами в исследуемой сети

На каждом из MTA будет поддерживаться smtp- и pop3-сервер. Подключиться к серверу может любой зарегистрированный пользователь. Чтобы отправить письмо, пользователь на сервере проходит авторизацию, после чего сервер готов отправлять письма от имени пользователя. По адресу назначения письма сервер определяет, кому следует передать его дальше. Нужный адрес сервер определяет с помощью службы DNS, в которой содержится соответствующая ресурсная адресная запись, преобразовывающая имя домена в IP-адрес.

Подключим службу DNS на сервере 172.16.0.20:

1. Один клик по выбранному устройству.
2. Выбираем вкладку Config, Services -> DNS (рис. 4.86). Заносим данные о новой ресурсной записи: имя домена, IP-адрес, тип ресурсной записи. Симулятор не поддерживает ресурсную запись, предназначенную для почтовых серверов, MX, но ее можно заменить адресной (тип А).

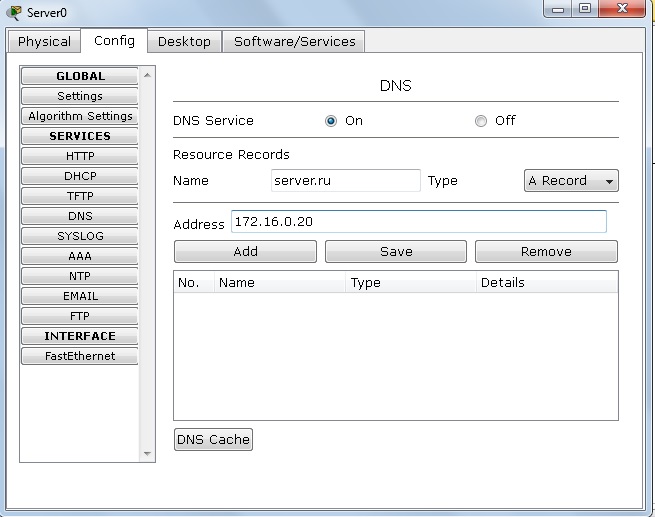


Рис. 4.86 Настройка службы DNS на сервере

1. Нажимаем на кнопку “Add” будет добавлена новая запись в службу DNS (рис. 4.87).

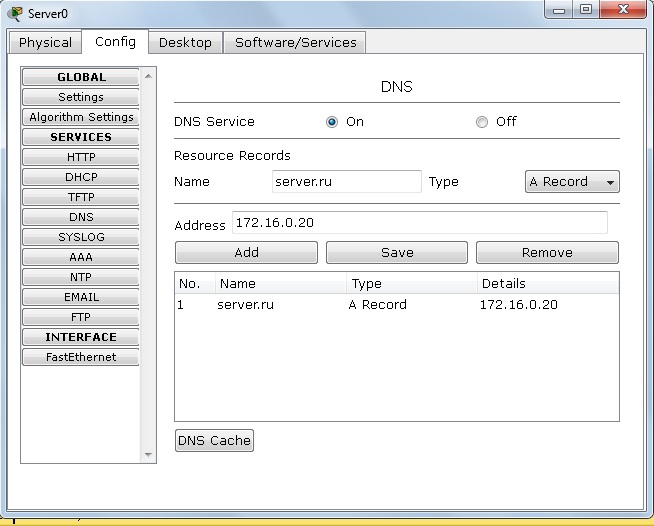


Рис. 4.87 Настройка службы DNS на сервере

Повторим предыдущие действия и добавим еще одну ресурсную запись о почтовом сервере 172.16.0.40 (рис. 4.88).

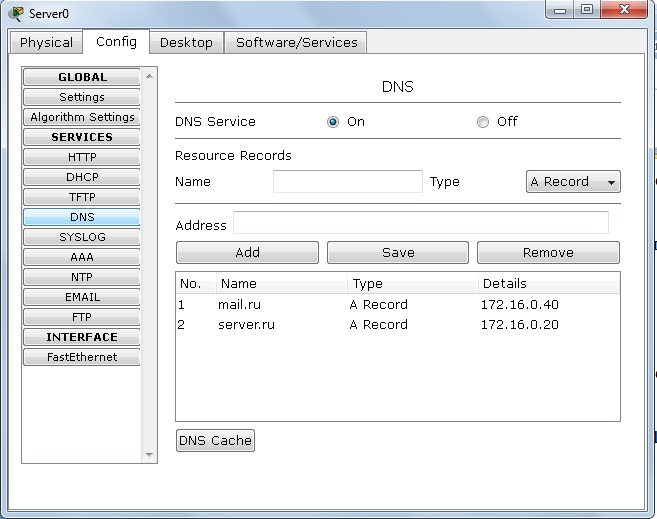


Рис. 4.88 Настройка службы DNS на сервере

Теперь сконфигурируем почтовый сервер 172.16.0.20 с поддержкой smtp- и pop3-сервера:

1. Один клик по выбранному устройству.
2. Выбираем вкладку “Config”, Services -> EMAIL
3. Подключаем протоколы SMTP и POP3 и вводим имя домена электронной почты. Нажимаем кнопку “Set” (рис. 4.89).

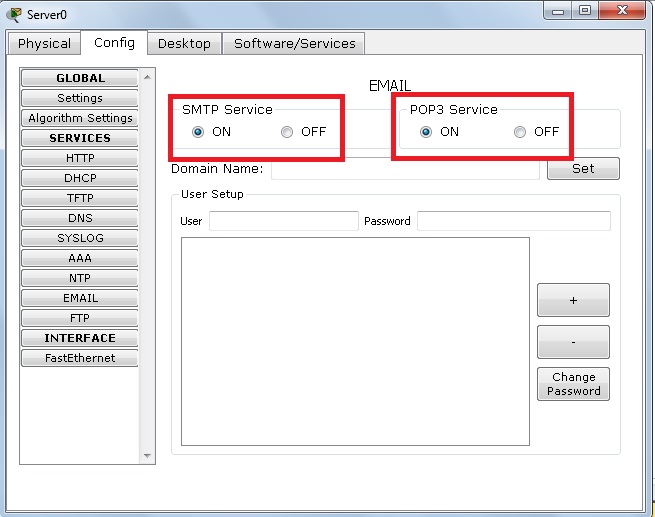


Рис. 4.89 Конфигурация smtp- и pop3-сервера

1. Создадим учетную запись для одного пользователя, вводим логин и пароль. Занести запись в службу можно с помощью кнопки “+” (рис. 4.90).

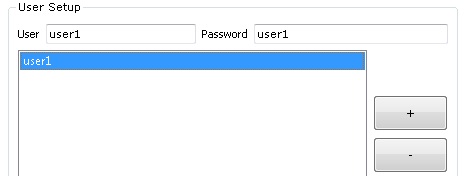


Рис. 4.90 Создание учетной записи

Smtp-сервер и pop3-сервер на машине 172.16.0.20 сконфигурированы, имеют одного зарегистрированного пользователя. Так же на нем поддерживается служба DNS, в которой есть две ресурсных записи.

На сервере 172.16.0.40 так же необходимо настроить почтовый сервер с поддержкой SMTP и POP3 (рис. 4.91). В качестве DNS для него выступает сервер 172.16.0.20.

1. Один клик по выбранному устройству.
2. Выбираем вкладку “Config”, Services -> EMAIL
3. Подключаем протоколы SMTP и POP3 и вводим имя домена электронной почты - mail.ru. Нажимаем кнопку “Set”.
4. Создадим учетную запись для одного пользователя, вводим логин и пароль. Занести запись в службу можно с помощью кнопки “+”.

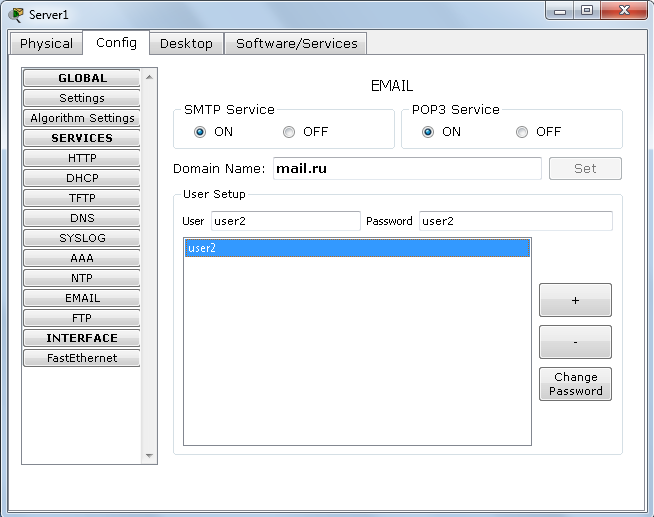


Рис. 4.91 Конфигурация smtp- и pop3-сервера

1. Настройка почтовой службы на конечных узлах

Для работы с почтовым smtp- или pop3-сервером на компьютере пользователя должен быть настроен клиент электронной почты, который и будет взаимодействовать с сервером (см. рис. 4.83).

Настроим на хосте 172.16.0.90 клиент электронной почты (рис. 4.92):

1. Один клик на хосте с IP-адресом 172.16.0.90.
2. Выбираем вкладку Desktop, программу “E-mail”. Появится окно конфигурации почтового сервиса. Вводим пользовательские данные в форму.

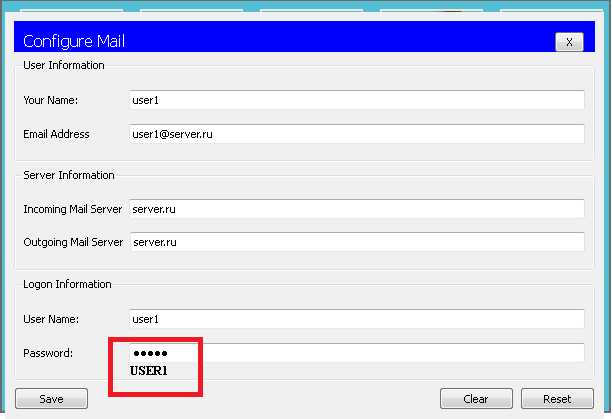


Рис. 4.92 Настройка клиента электронной почты

Нажимаем кнопку “Save”, закрываем окно, конфигурация клиента электронной почты завершена. Теперь для пользователя user1 доступен почтовый сервис в домене server.ru: отправка и получение писем.

Настроим почтовый сервис и на хосте 172.16.0.100, выполнив предыдущие действия (рис. 4.93). Вводим следующие пользовательские данные:

Теперь для пользователя user2 доступен почтовый сервис в домене mail.ru: отправка и получение писем.

Настройка всех устройств и необходимых служб завершена.

1. Исследование прикладных почтовых протоколов в режиме симуляции

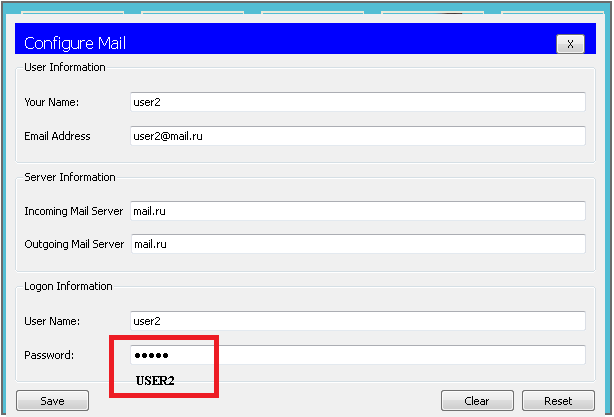


Рис. 4.93 Настройка клиента электронной почты

Переходим в режим симуляции Cisco Packet Tracer. Добавляем фильтры на 2 протокола: SMTP и POP3 (рис. 4.94). Это значит, что пакеты только фильтруемых протоколов будут отображаться в сети.

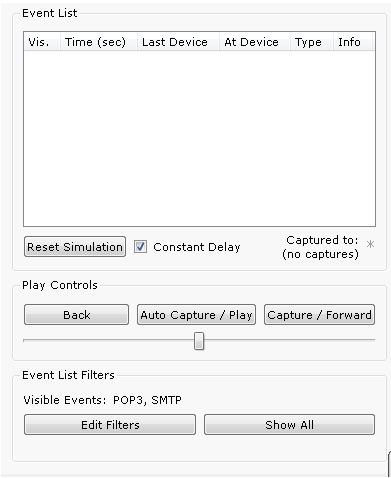


Рис. 4.94 Окно событий режима симуляции

Отправим письмо с хоста 172.16.0.90 от user1 на хост 172.16.0.100 user2 (рис. 4.95):

1. Один клик по выбранному узлу (172.16.0.90).
2. Выбираем на вкладке “Desktop” программу “E-mail”.
3. Чтобы написать и отправить письмо, нажимаем на кнопку “Compose”. Появится форма, которую следует заполнить. В поле “To” задается адрес электронной почты, кому вы отправляете письмо. Поле “Subject” содержит заголовок письма. Текст письма можете сочинить самостоятельно.

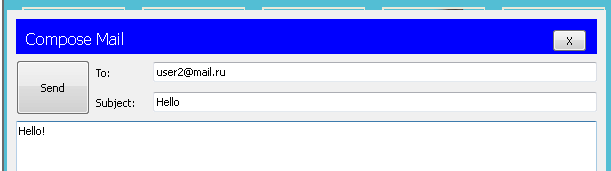


Рис. 4.95 Форма для отправления письма

Нажимаем на кнопку “Send”, начнется отправление письма.

Видим, что на хосте 172.16.0.90 сформировался пакет SMTP (рис. 4.96). Воспользовавшись кнопкой “Capture/Forward”, проследим за маршрутом пакета от устройства к устройству.

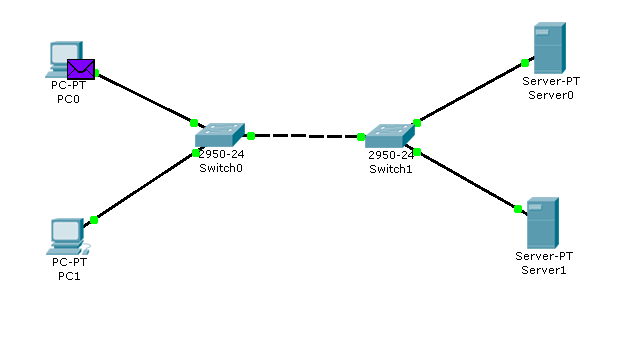


Рис. 4.96 Вид рабочей области

Посмотрим содержимое пакета, сформированного на узле (рис. 4.97).

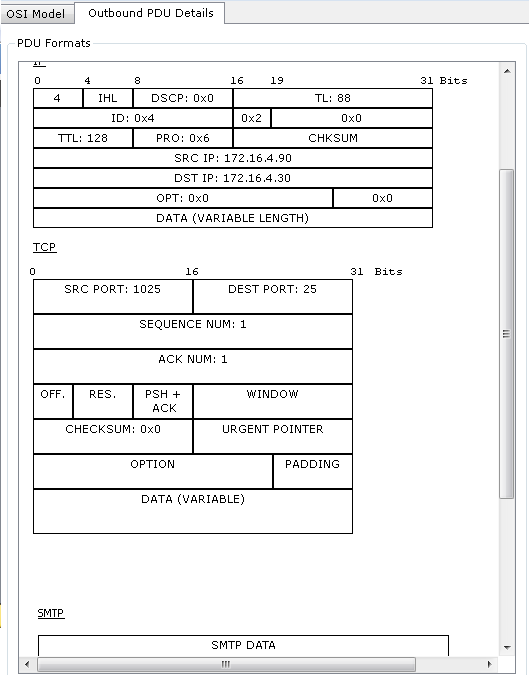


Рис. 4.97 Формат пакета SMTP

Пакет адресован почтовому серверу по IP-адресу 172.16.0.20. В заголовке TCP содержится порт назначения – 25. Можно сделать вывод, что пакет сформирован верно. Пакет на пути своего следования к серверу проходит через два коммутатора (рис. 4.98). Убедитесь, что это так.

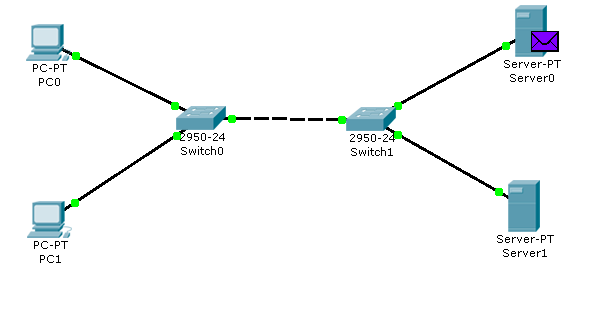
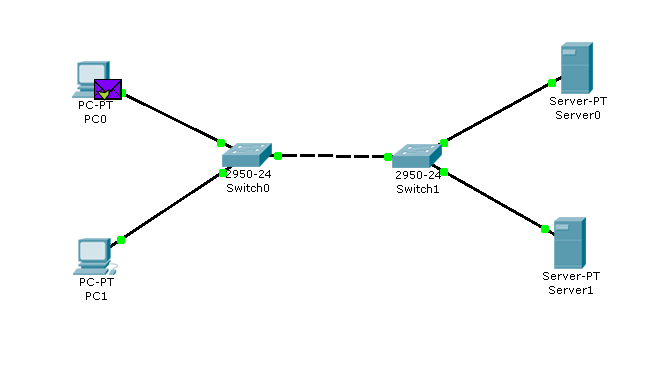


Рис. 4.98 Вид рабочей области

На сервере 172.16.0.20 формируется SMTP-ответ клиенту c IP-адресом 172.16.0.90 и отправляется на указанный адрес.



Когда пакет приходит на сервер, тот, обрабатывая его, определяет, что письмо адресовано домену mail.ru. Сервер 172.16.0.20 обращается к службе DNS за IP-адресом заданного сервера. По указанному адресу письмо перенаправляется на соответствующий почтовый сервер (рис. 4.99).

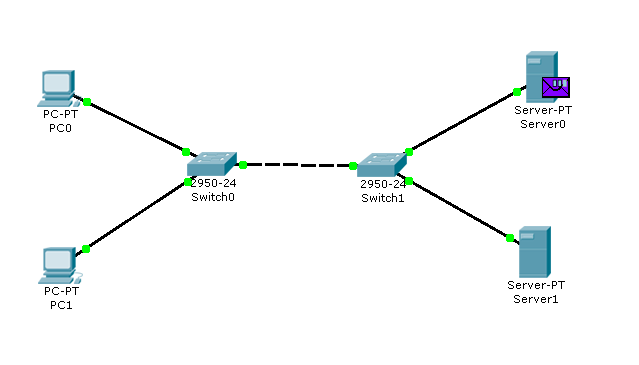


Рис. 4.99 Вид рабочей области

SMTP-пакет, сформированный сервером 172.16.0.20, содержит следующую информацию: IP-адрес назначения – 172.16.0.40, порт назначения – 25 (рис. 4.100).

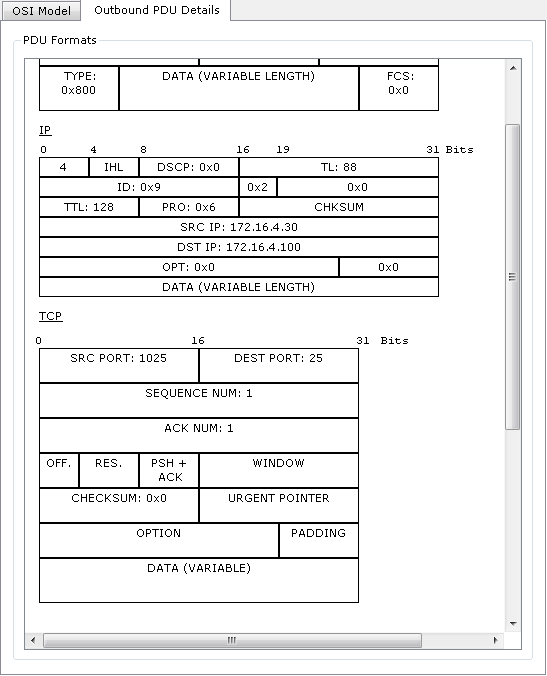


Рис. 4.100 Формат пакета SMTP

Пакет проходит через коммутатор Switch1 и доставляется серверу 172.16.0.40 (рис. 4.101).

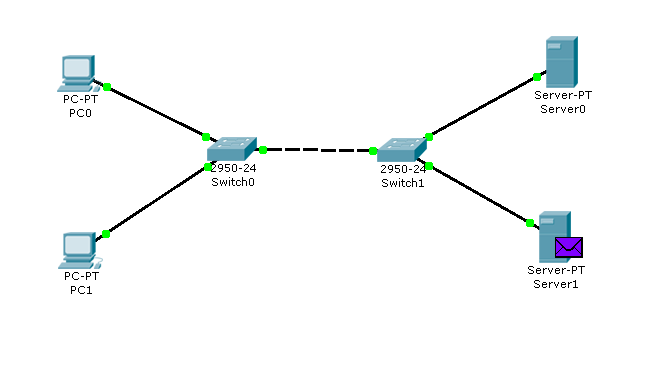


Рис. 4.101 Вид рабочей области

На сервере 172.16.0.40 формируется SMTP-ответ серверу 172.16.0.20 и отправляется на указанный адрес (рис. 4.102).

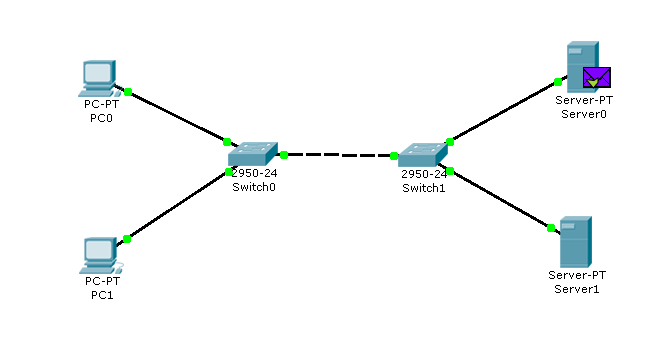


Рис. 4.102 Вид рабочей области

Из содержимого пакета, пришедшего обратно на сервер 172.16.0.20: IP-адрес источника – 172.16.0.40, порт источника – 25 (рис. 4.103).

С помощью протокола SMTP мы отправили письмо на сервер mail.ru, теперь оно хранится там.

Наш адресат (узел 172.16.0.100) еще не получил отправленное письмо, так как на сервер он еще не обратился по протоколу POP3. Для получения письма необходимо проделать следующие действия:

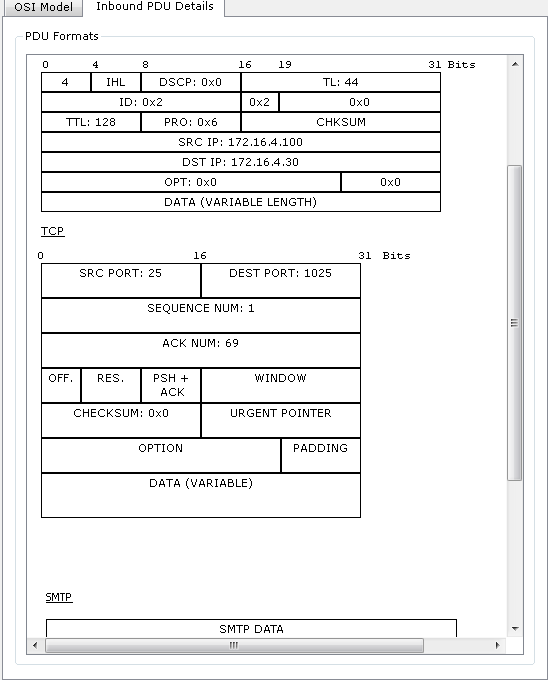


Рис. 4.103 Формат пакета SMTP

1. Один клик по узлу 172.16.0.100.
2. Выбираем на вкладке “Desktop” программу “E-mail”.
3. Нажимаем на кнопку “Receive”, чтобы прочитать письмо.

На хосте формируется пакет протокола POP3 (рис. 4.104). Воспользовавшись кнопкой “Capture/Forward”, проследим за маршрутом пакета от устройства к устройству.

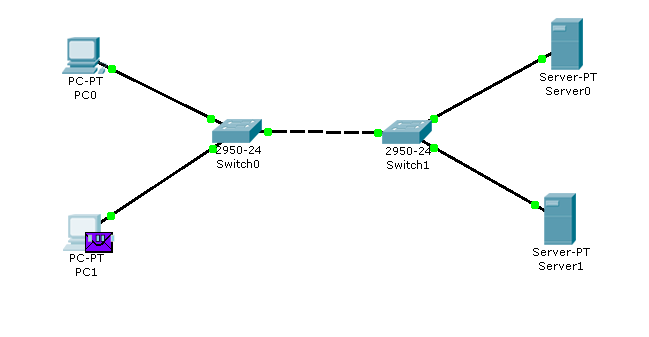


Рис. 4.104 Вид рабочей области

Посмотрим содержимое пакета, сформированного на узле (рис. 4.105).

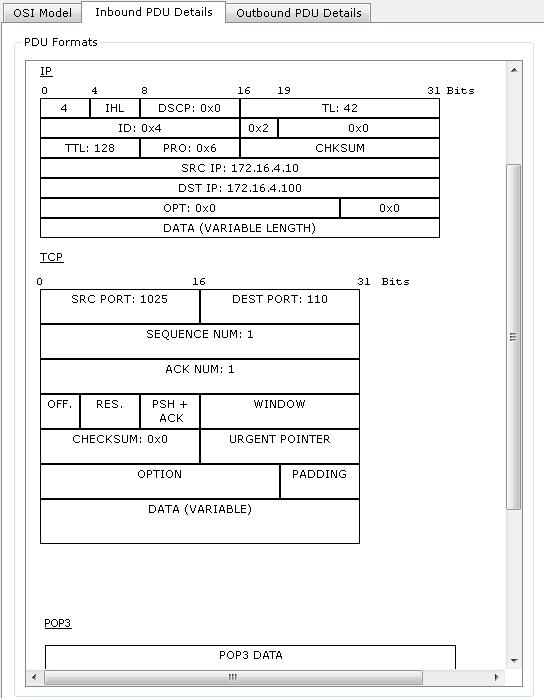


Рис. 4.105 Формат пакета РОР3

Пакет адресован почтовому серверу по IP-адресу 172.16.0.40. В заголовке TCP содержится порт назначения – 110. Можно сделать вывод, что пакет сформирован верно. Пакет на пути своего следования к серверу проходит через два коммутатора. Убедитесь, что это так. Когда пакет приходит на сервер, тот обрабатывает его и формирует пакет-ответ (рис. 4.106).

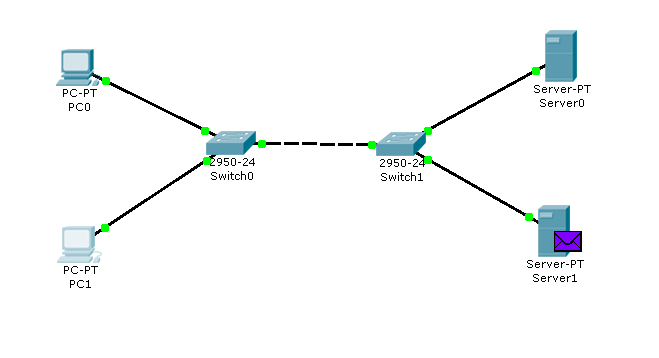


Рис. 4.106 Вид рабочей области

Пакет по тому же маршруту возвращается на узел 172.16.0.100 с ответом (письмом) от сервера. Посмотрим содержимое ответа (рис. 4.107).

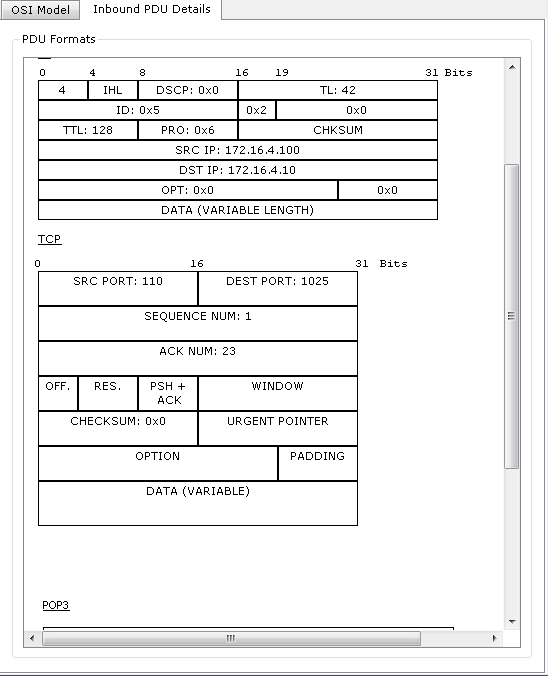


Рис. 4.107 Формат пакета РОР3

Порт-источник – 110. Ответ пришел от сервера 172.16.0.40 с некоторыми POP3-данными. С помощью протокола POP3 узел 172.16.0.100 получил письмо с сервера, отправленное туда узлом 172.16.0.90 (рис. 4.108).

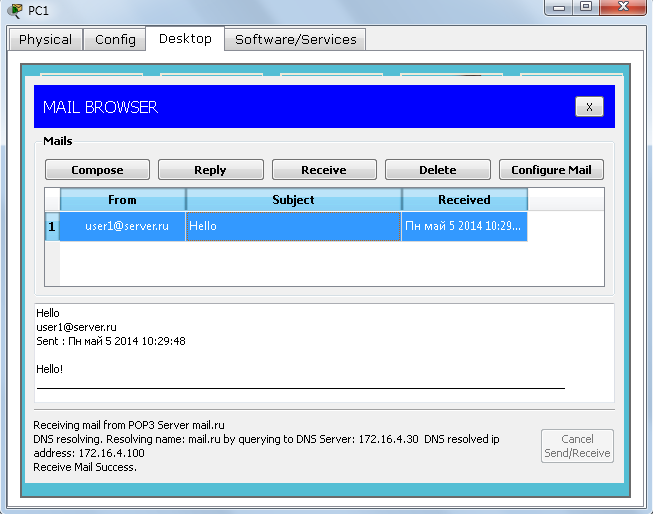


Рис. 4.108 Форма чтения входящих писем

Как уже упоминалось в теоретических сведениях, почтовые протоколы SMTP и POP3 обмениваются информацией с помощью команд. Клиенту электронной почты, чтобы установить соединение с сервером, отправить письмо, разорвать соединение необходимо отправлять серверу соответствующие команды. Сервер электронной почты, в свою очередь, обрабатывает эти команды и формирует отклики для клиента. Отклики smtp-сервера содержат цифровой код ответа: успешно или с ошибкой обработана команда. Отклики pop3-сервера так же содержат два типа сообщений: успех или ошибка.

Обращая внимание на содержимое пакета SMTP или POP3 протокола, видно, что на прикладном уровне пакет детально не рассматривается.

Пример приведен на рис. 4.109.



Рис. 4.109 Данные прикладного уровня

Поэтому эксперимент посылки письма несуществующему пользователю не является содержательным, т.к. подробно увидеть ответ от smtp-сервера нам не удастся. Для подробного изучения взаимодействия между клиентом и smtp- или pop3-сервером следует обратиться к предложенной спецификации RFC 2821 и RFC 1939.

1. **Индивидуальные задания**

Исследуйте прикладные протоколы электронной почты SMTP и POP3 самостоятельно. Топологию сети для исследования оставьте прежней. Настройку сетевых устройств проделайте в соответствии с вариантом.

В отчете приведите маршруты пакетов, их содержимое и объясните полученные результаты. Отправителя и получателя определите сами.

Варианты заданий представлены в приложении 2.

# Лабораторная работа 4. «Работа с сетевым анализатором»

**ЧАСТЬ 1.**

Мы будем использовать «Wireshark packet sniffer» [http://www.wireshark.org/]

Установка Wireshark

Перейдите на сайт http://www.wireshark.org/download.html, загрузите и установите двоичный файл Wireshark на свой компьютер.

В FAQ по Wireshark есть ряд полезных советов и интересных кусочков информации, особенно если у вас возникли проблемы с установкой или запуском Wireshark.

Запуск Wireshark

Когда вы запустите программу Wireshark, вы увидите начальный экран, похожий на экран ниже. В разных версиях Wireshark будут разные заставки, поэтому не паникуйте, если ваш экран выглядит не так, как на экране ниже! В документации Wireshark говорится: «Поскольку Wireshark работает на многих различных платформах с множеством различных оконных менеджеров, применяются разные стили и используются разные версии базового инструментария графического интерфейса пользователя, ваш экран может отличаться от предоставленных снимков экрана. Но поскольку реальных различий в функциональности нет, эти скриншоты все равно должны быть хорошо понятными ».

Graphical user interface, text, application, email

Description automatically generated

На этом экране не так много интересного. Но обратите внимание, что в разделе Capture есть список так называемых интерфейсов. Компьютер, с которого мы делаем эти снимки экрана, имеет только один реальный интерфейс - «Wi-Fi en0», который является интерфейсом для доступа к Wi-Fi. Все пакеты к / от этого компьютера будут проходить через интерфейс Wi-Fi, так что именно здесь мы будем перехватывать пакеты.

Дважды щелкните этот интерфейс (или найдите интерфейс на начальной странице, через который вы подключаетесь к Интернету, например, скорее всего, интерфейс Wi-Fi или Ethernet), и выберите этот интерфейс.

Если вы нажмете на один из этих интерфейсов, чтобы начать захват пакетов (то есть, чтобы Wireshark начал захват всех пакетов, отправляемых в / из этого интерфейса), отобразится экран, подобный приведенному ниже, с информацией о захватываемых пакетах. Как только вы начнете захват пакета, вы можете остановить его, используя раскрывающееся меню Capture и выбрав Stop.

Graphical user interface, text

Description automatically generated

Интерфейс Wireshark состоит из пяти основных компонентов:

• Командные меню представляют собой стандартные раскрывающиеся меню, расположенные в верхней части окна. Сейчас нас интересуют меню «Файл» и «Захват». Меню «Файл» позволяет сохранить захваченные пакетные данные или открыть файл, содержащий ранее захваченные пакетные данные, и выйти из приложения Wireshark. Меню Capture позволяет начать захват пакета.

• В окне со списком пакетов отображается однострочная сводка для каждого захваченного пакета, включая номер пакета (номер, назначенный Wireshark; это не номер пакета, содержащийся в заголовке какого-либо протокола), время захвата пакета, адреса источника и получателя, тип протокола и информация о протоколе, содержащаяся в пакете. Список пакетов можно отсортировать по любой из этих категорий, щелкнув имя столбца. В поле типа протокола указан протокол самого высокого уровня, который отправил или получил этот пакет, то есть протокол, который является источником или конечным приемником для этого пакета.

• Окно деталей заголовка пакета предоставляет подробную информацию о пакете, выбранном (выделенном) в окне списка пакетов. (Чтобы выбрать пакет в окне списка пакетов, поместите курсор на однострочную сводку пакета в окне списка пакетов и щелкните левой кнопкой мыши.) Эти сведения включают информацию о кадре Ethernet (при условии, что пакет был отправлен / получен через интерфейс Ethernet) и дейтаграмме IP, содержащей этот пакет. Количество отображаемых сведений об Ethernet и IP-уровне можно расширить или минимизировать, щелкнув поля «плюс-минус» слева от кадра Ethernet или строки IP-дейтаграммы в окне сведений о пакете. Если пакет был передан по TCP или UDP, также будут отображаться сведения о TCP или UDP, которые аналогичным образом могут быть расширены или минимизированы. Наконец, также предоставляются сведения о протоколе самого высокого уровня, который отправил или получил этот пакет.

• В окне содержимого пакета отображается все содержимое захваченного кадра как в ASCII, так и в шестнадцатеричном формате.

• Вверху графического пользовательского интерфейса Wireshark находится поле фильтра отображения пакетов, в которое можно ввести имя протокола или другую информацию, чтобы отфильтровать информацию, отображаемую в окне списка пакетов (и, следовательно, заголовок пакета и окна содержимого пакета). В приведенном ниже примере мы будем использовать поле фильтра отображения пакетов, чтобы программа Wireshark скрывала (не отображала) пакеты, кроме тех, которые соответствуют сообщениям HTTP.

Тестовый запуск

Сделайте следующее:

1. Запустите ваш любимый веб-браузер, в котором отобразится выбранная вами домашняя страница.

2. Запустите программное обеспечение Wireshark. Сначала вы увидите окно, подобное тому, что показано на рисунке. Wireshark еще не приступил к захвату пакетов.

3. Чтобы начать захват пакета, выберите раскрывающееся меню «Захват» и выберите «Интерфейсы». Это приведет к отображению окна «Wireshark: Capture Interfaces».

Graphical user interface, text, application

Description automatically generated

4. Вы увидите список интерфейсов на вашем компьютере, а также количество пакетов, которые были замечены на этом интерфейсе на данный момент. Нажмите «Пуск» для интерфейса, на котором вы хотите начать захват пакетов (в случае Gigabit Network Connection). Теперь начнется захват пакетов - Wireshark теперь захватывает все пакеты, отправляемые / получаемые с / с вашего компьютера

5. Как только вы начнете захват пакета, появится окно, в котором отображаются захваченные пакеты. Выбрав раскрывающееся меню «Захват» и выбрав «Стоп», вы можете остановить захват пакетов. Но пока не останавливайте захват пакетов. Давайте сначала захватим несколько интересных пакетов. Для этого нам потребуется сгенерировать сетевой трафик. Давайте сделаем это с помощью веб-браузера, который будет использовать протокол HTTP для загрузки контента с веб-сайта.

6. Во время работы Wireshark введите URL-адрес:

<http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html>

и эта страница должна отображаться в вашем браузере. Чтобы отобразить эту страницу, ваш браузер свяжется с HTTP-сервером на gaia.cs.umass.edu и обменивается HTTP-сообщениями с сервером, чтобы загрузить эту страницу. Кадры Ethernet, содержащие эти HTTP-сообщения (а также все другие кадры, проходящие через адаптер Ethernet), будут захвачены Wireshark. Должен появиться обмен сообщениями HTTP с веб-сервером gaia.cs.umass.edu где-то в списке захваченных пакетов. Но будет отображаться и много других типов пакетов.

7. Введите «http» (без кавычек и в нижнем регистре - все имена протоколов в Wireshark в нижнем регистре) в окне спецификации фильтра отображения в верхней части главного окна Wireshark. Затем выберите «Применить» (справа от того места, где вы ввели «http»). Это приведет к тому, что в списке пакетов будет отображаться только сообщение HTTP.

8. Найдите сообщение HTTP GET, которое было отправлено с вашего компьютера на HTTP-сервер gaia.cs.umass.edu. (Найдите сообщение HTTP GET в разделе «Список перехваченных пакетов» окна Wireshark, в котором отображается «GET», за которым следует введенный вами URL-адрес gaia.cs.umass.edu. Когда вы выбираете HTTP Сообщение GET, кадр Ethernet, дейтаграмма IP, сегмент TCP, и информация заголовка сообщения HTTP будет отображаться в окне заголовка пакета. Нажав на «+» и «-» стрелки, указывающие вправо и вниз, в левой части окна сведений о пакете, уменьшите количество отображаемой информации о кадрах, Ethernet, Интернет-протоколе и протоколе управления передачей. Максимально увеличьте объем отображаемой информации о протоколе HTTP.

Теперь ваш дисплей Wireshark должен выглядеть примерно так, как показано на рисунке. (Обратите внимание, в частности, на минимизированный объем информации о протоколе для всех протоколов, кроме HTTP, и максимальный объем информации о протоколе для HTTP в окне заголовка пакета).

Graphical user interface, application

Description automatically generated

10. Закройте Wireshark.

**ЧАСТЬ 2.**

ЗАДАЧА

1. Установите Wireshark (лабораторная работа 1, часть 1) - у вас уже есть вся информация.

2. Используйте nslookup для анализа сообщений DNS.

3. Используйте ipconfig для анализа сообщений DNS.

4. Используйте Wireshark для анализа сообщений DNS.

1. nslookup

В первой части лабораторной работы мы будем использовать инструмент nslookup. Этот инструмент сегодня доступен на большинстве платформ Linux / Unix и Microsoft. Если у вас есть MAC и \ или нет этого инструмента на вашем ПК - попробуйте поискать в Интернете, как вы можете это исправить. Если проблемы не исчезнут - напишите, пожалуйста, на почту преподавателю.

Чтобы запустить nslookup в Linux / Unix:

Вы должны ввести команду nslookup в командной строке.

𝑛𝑠𝑙𝑜𝑜𝑘𝑢𝑝

• Чтобы запустить его в Windows:

Откройте командную строку и запустите nslookup в командной строке.

Text

Description automatically generated

В этой самой базовой операции инструмент nslookup позволяет хосту, на котором запущено средство, запрашивать запись DNS на любом указанном DNS-сервере. Запрашиваемый DNS-сервер может быть корневым DNS-сервером, DNS-сервером домена верхнего уровня, авторитетным DNS-сервером или промежуточным DNS-сервером. Для выполнения этой задачи nslookup отправляет DNS-запрос на указанный DNS-сервер, получает DNS-ответ от того же DNS-сервера и отображает результат.

Чтобы закрыть nslookup, напишите «exit» в командной строке.

• Рассмотрим первую команду:

𝑛𝑠𝑙𝑜𝑜𝑘𝑢𝑝 𝑤𝑤𝑤. 𝑖𝑡𝑚𝑜. 𝑟𝑢

Как показано на снимке экрана, ответ этой команды предоставляет две части информации: (1) имя и IP-адрес DNS-сервера, который предоставляет ответ; и (2) сам ответ - имя хоста и IP-адрес www.itmo.ru.

Вы увидите следующее:

A screenshot of a computer

Description automatically generated

Это означает, что сервер, к которому обращается утилита nslookup, не является авторитетным, то есть может вызвать сомнения, например, с точки зрения безопасности. Однако, если мы знаем, что это доменное имя является безопасным, мы можем использовать следующую опцию:

𝑛𝑠𝑙𝑜𝑜𝑘𝑢𝑝 - 𝑡𝑦𝑝𝑒 = 𝑁𝑆 𝑤𝑤𝑤. 𝑖𝑡𝑚𝑜. 𝑟𝑢

𝑛𝑠𝑙𝑜𝑜𝑘𝑢𝑝 - 𝑡𝑦𝑝𝑒 = 𝑁𝑆 𝑖𝑡𝑚𝑜. 𝑟𝑢

В этом примере мы предоставили параметр «-type = NS» и домены «itmo.ru» и «www.itmo.ru». Это заставляет nslookup отправлять запрос о записи типа NS на локальный DNS-сервер по умолчанию.

Text

Description automatically generated

На словах запрос гласит: «пришлите мне, пожалуйста, имена хостов авторитетного DNS для mit.edu». (Если параметр - 𝑡𝑦𝑝𝑒 не используется, nslookup использует значение по умолчанию, которое заключается в запросе записей типа A.)

Ответ, показанный на приведенном выше снимке экрана, сначала указывает DNS-сервер, который предоставляет ответ (который является локальным DNS-сервером по умолчанию), а также два сервера имен ИТМО.

Однако nslookup также указывает, что ответ «неавторизованный», то есть этот ответ пришел из кэша какого-то сервера, а не от авторитетного DNS-сервера ИТМО. Наконец, ответ также включает IP-адрес авторитетного DNS-сервера в ИТМО.

Теперь, наконец, рассмотрим третью команду:

𝑛𝑠𝑙𝑜𝑜𝑘𝑢𝑝 𝑤𝑤𝑤. ℎ𝑑𝑢.𝑒𝑑𝑢. 𝑐𝑛 𝑟𝑜𝑢𝑡𝑒𝑟. 𝑎𝑠𝑢𝑠. 𝑐𝑜𝑚

Text

Description automatically generated

В этом примере мы указываем, что хотим отправить запрос на DNS-сервер router.asus.com.

Таким образом, транзакция запроса и ответа происходит непосредственно между нашим запрашивающим хостом и router.asus.com. В этом примере DNS-сервер router.asus.com предоставляет IP-адрес хоста 𝑤𝑤𝑤. ℎ𝑑𝑢.𝑒𝑑𝑢. 𝑐𝑛, который является веб-сервером Университета HDU.

Теперь, когда мы рассмотрели несколько наглядных примеров, вы, возможно, задаетесь вопросом об общем синтаксисе команд nslookup. Синтаксис:

𝑛𝑠𝑙𝑜𝑜𝑘𝑢𝑝 - 𝑜𝑝𝑡𝑖𝑜𝑛1 - 𝑜𝑝𝑡𝑖𝑜𝑛2 ℎ𝑜𝑠𝑡 - 𝑡𝑜 - 𝑓𝑖𝑛𝑑 𝑑𝑛𝑠 - 𝑠𝑒𝑟𝑣𝑒𝑟

Как правило, nslookup можно запускать с нулевым, одним, двумя или более параметрами. И, как мы видели в приведенных выше примерах, dns-сервер также не является обязательным; если он не указан, запрос отправляется на локальный DNS-сервер по умолчанию.

Теперь, когда мы представили обзор nslookup, пришло время протестировать его самостоятельно. Сделайте следующее (выберите серверы и университеты и запишите результаты):

1. Запустите nslookup, чтобы получить IP-адрес веб-сервера университета (любого) в России. Какой IP-адрес у этого сервера?

2. Запустите nslookup, чтобы определить авторитетные DNS-серверы для университета в Европе.

3. Запустите nslookup, чтобы один из DNS-серверов, полученных в вопросе 2, запросил почтовые серверы для почты Яндекса (или любого другого). Какой у него IP-адрес?

4. Сделайте скриншоты вашей командной строки и поместите их в отчет, поместите их в отчет вместе с ответами на вопросы.

2. Ipconfig

ipconfig (для Windows) и ifconfig (для Linux / Unix) - одни из самых полезных небольших утилит на вашем хосте, особенно для отладки сетевых проблем. Здесь мы опишем только ipconfig, хотя ifconfig Linux / Unix очень похож. Если у вас есть MAC и \ или нет этого инструмента на вашем ПК - попробуйте поискать в Интернете.

ipconfig можно использовать для отображения вашей текущей информации TCP / IP, включая ваш адрес, адреса DNS-серверов, тип адаптера и так далее. Например, если вы получите всю эту информацию о своем хосте, просто введя 𝑖𝑝𝑐𝑜𝑛𝑓𝑖𝑔 \ 𝑎𝑙𝑙 в командную строку, как показано на следующем снимке экрана.

Text

Description automatically generated

Введите следующую команду:

𝑖𝑝𝑐𝑜𝑛𝑓𝑖𝑔 / 𝑑𝑖𝑠𝑝𝑙𝑎𝑦𝑑𝑛𝑠

Каждая запись показывает оставшееся время жизни (TTL) в секундах. Чтобы очистить кеш, введите

𝑖𝑝𝑐𝑜𝑛𝑓𝑖𝑔 / 𝑓𝑙𝑢𝑠ℎ𝑑𝑛𝑠

Очистка кеша DNS очищает все записи и перезагружает записи из файла hosts.

Сделайте скриншоты своей работы и добавьте их в отчет

3. Отслеживание DNS с помощью Wireshark

Давайте сначала перехватим DNS-пакеты, которые генерируются обычным веб-серфингом.

• Используйте ipconfig, чтобы очистить кэш DNS на вашем хосте.

• Откройте браузер и очистите кэш браузера. (В Internet Explorer перейдите в меню «Сервис» и выберите «Свойства обозревателя»; затем на вкладке «Общие» выберите «Удалить файлы».)

• Откройте Wireshark и введите «ip.addr == your\_IP\_address» в фильтр, где вы получите your\_IP\_address с помощью ipconfig. Этот фильтр удаляет все пакеты, которые не исходят и не предназначены для вашего хоста.

• Запустите захват пакетов в Wireshark.

• В браузере посетите некоторую веб-страницу

• Остановить захват пакетов.

Вы увидите что-то подобное.

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, table

Description automatically generated

Ответьте на следующие вопросы. По возможности, отвечая на вопрос ниже, вы должны

вручите распечатку пакета (ов) с трассировкой, которую вы использовали для ответа на заданный вопрос.

Добавьте аннотации к распечатке, чтобы объяснить свой ответ. Чтобы распечатать пакет, используйте File-> Print, выберите Selected

только пакет, выберите Строку сводки пакета и выберите минимальное количество деталей пакета, которое вы

нужно ответить на вопрос.

Вопросы (сделайте скриншот результатов):

1. Найдите сообщения DNS-запроса и ответа. Они отправляются по UDP или TCP?

2. Каков порт назначения для сообщения DNS-запроса? Каков порт источника ответа DNS?

3. На какой IP-адрес отправляется сообщение с запросом DNS? Используйте ipconfig, чтобы определить IP-адрес вашего локального DNS-сервера. Эти два IP-адреса одинаковы?

4. Изучите сообщение DNS-запроса. Что это за «тип» DNS-запроса? Содержит ли запросное сообщение какие-либо «ответы»?

5. Изучите ответное сообщение DNS. Сколько «ответов» дается? Что содержит каждый из этих ответов?

6. Есть ли на этой веб-странице изображения? Перед получением каждого изображения ваш хост выдает новые DNS-запросы?

Теперь - nslookup.

• Начать захват пакета.

• Сделайте 𝑛𝑠𝑙𝑜𝑜𝑘𝑢𝑝 𝑤𝑤𝑤. ℎ𝑑𝑢.𝑒𝑑𝑢. 𝑐𝑛

• Остановить захват пакетов. У вас должен получиться след, который выглядит примерно так (на последних фотографиях).

Из приведенного выше снимка экрана видно, что nslookup действительно отправлял DNS-запросы и получал DNS-ответы.

1. Какой порт назначения для сообщения DNS-запроса? Каков порт источника ответного сообщения DNS?

2. На какой IP-адрес отправляется сообщение с запросом DNS? Это IP-адрес вашего локального DNS-сервера по умолчанию?

3. Изучите сообщение DNS-запроса. Что это за «тип» DNS-запроса? Содержит ли запросное сообщение какие-либо «ответы»?

4. Изучите ответное сообщение DNS. Сколько «ответов» дается? Что содержит каждый из этих ответов?

5. Предоставьте скриншот.

Теперь повторите предыдущий эксперимент, но вместо этого введите команду:

𝑛𝑠𝑙𝑜𝑜𝑘𝑢𝑝 - 𝑡𝑦𝑝𝑒 = 𝑁𝑆 𝑎𝑑𝑑𝑟𝑒𝑠𝑠\_𝑤ℎ𝑎𝑡\_𝑦𝑜𝑢\_𝑤𝑎𝑛𝑡

Ответьте на следующие вопросы:

1. На какой IP-адрес отправляется сообщение с запросом DNS? Это IP-адрес вашего локального DNS-сервера по умолчанию?

2. Изучите сообщение с запросом DNS. Что это за «тип» DNS-запроса? Содержит ли запросное сообщение какие-либо «ответы»?

3. Изучите ответное сообщение DNS. Какие серверы имен предоставляет ответное сообщение?

4. Предоставьте скриншот.

Теперь повторите предыдущий эксперимент, но вместо этого введите команду:

𝑛𝑠𝑙𝑜𝑜𝑘𝑢𝑝 𝑎𝑑𝑑𝑟𝑒𝑠𝑠\_𝑤ℎ𝑎𝑡\_𝑦𝑜𝑢\_𝑤𝑎𝑛𝑡 𝑦𝑜𝑢𝑟\_𝐷𝑁𝑆

Ответьте на следующие вопросы:

1. На какой IP-адрес отправляется сообщение с запросом DNS? Это IP-адрес вашего локального DNS-сервера по умолчанию? Если нет, то чему соответствует IP-адрес?

2. Изучите сообщение с запросом DNS. Что это за «тип» DNS-запроса? Содержит ли запросное сообщение какие-либо «ответы»?

3. Изучите ответное сообщение DNS. Сколько «ответов» дается? Что содержит каждый из этих ответов?

4. Предоставьте скриншот.

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

# СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Протоколы, технологии, технологии. 3-е издание. СПб.: Изд-во Питер, 2003. – 960 с.

2. Мулюха В.А., Новопашенный А.Г., Подгурский Ю.Е., Заборовский В.С. Методы и средства защиты компьютерной информации. Межсетевое экранирование: учеб. Пособие. СПб.: Изд-во Политехн. университета, 2010. – 92 с.

3. [Электронный ресурс] // Олифер В.Г., Олифер Н.А. Введение в IP-сети. 2003.

4. Ицыксон В.М. Курс лекций «Технологии компьютерных сетей» 2012.

5. [Электронный ресурс] // Network Working Group. RFC 2821. Simple Mail Transfer Protocol. 2001

6. Фролов А.И. Сети ЭВМ и телекоммуникации. Орел: 2006. – 71 с.

7. [Электронный ресурс] // Network Working Group. RFC 1939. Post Office Protocol – Version 3. 1996.

8. [Электронный ресурс] // Храмцов П.Б. Электронная почта и DNS.

9. [Электронный ресурс] https://habr.com/ru/post/350720/

# ПРИЛОЖЕНИЕ 1

Варианты индивидуальных заданий к лабораторной работе №2 (таблица 1):

Таблица 1

|  |  |  |
| --- | --- | --- |
| Вариант | Источник | Приемник |
| 1 | 192.168.3.3  192.168.3.4 | 192.168.3.4  192.168.3.6 |
| 2 | 192.168.3.4  192.168.3.5 | 192.168.3.7  192.168.5.3 |
| 3 | 192.168.3.5  192.168.3.6 | 192.168.3.6  192.168.3.7 |
| 4 | 192.168.3.6  192.168.3.7 | 192.168.5.4  192.168.3.4 |
| 5 | 192.168.3.3  192.168.3.7 | 192.168.3.7  192.168.5.5 |
| 6 | 192.168.5.3  192.168.3.6 | 192.168.5.4  192.168.3.4 |
| 7 | 192.168.3.3  192.168.3.5 | 192.168.5.3  192.168.3.7 |
| 8 | 192.168.3.3  192.168.3.4 | 192.168.5.4  192.168.3.5 |
| 9 | 192.168.3.4  192.168.3.5 | 192.168.5.3  192.168.3.4 |
| 10 | 192.168.5.4  192.168.3.6 | 192.168.5.5  192.168.3.3 |
| 11 | 192.168.3.4  192.168.3.7 | 192.168.5.3  192.168.5.4 |
| 12 | 192.168.3.5  192.168.3.6 | 192.168.5.5  192.168.3.7 |
| 13 | 192.168.3.5  192.168.3.7 | 192.168.5.4  192.168.3.3 |
| 14 | 192.168.3.6  192.168.3.7 | 192.168.5.3  192.168.5.5 |

# ПРИЛОЖЕНИЕ 2

Варианты индивидуальных заданий к лабораторной работе №3 (таблица 1):

Таблица 1

|  |  |  |  |
| --- | --- | --- | --- |
| Вариант 1 | | | |
| Конечные узлы | IP-адрес | Маска сети | IP-адрес DNS-сервера |
| PC0 | 172.16.1.90 | 255.255.0.0 | 172.16.1.20 |
| PC1 | 172.16.1.100 | 255.255.0.0 | 172.16.1.20 |
| Серверы | | | |
| Server0 | 172.16.1.20 | 255.255.0.0 | 172.16.1.20 |
| Server1 | 172.16.1.60 | 255.255.0.0 | 172.16.1.20 |
| Вариант 2 | | | |
| Конечные узлы | IP-адрес | Маска сети | IP-адрес DNS-сервера |
| PC0 | 172.16.0.12 | 255.255.0.0 | 172.16.0.50 |
| PC1 | 172.16.0.13 | 255.255.0.0 | 172.16.0.50 |
| Серверы | | | |
| Server0 | 172.16.0.50 | 255.255.0.0 | 172.16.0.50 |
| Server1 | 172.16.0.10 | 255.255.0.0 | 172.16.0.50 |
| Вариант 3 | | | |
| Конечные узлы | IP-адрес | Маска сети | IP-адрес DNS-сервера |
| PC0 | 192.168.3.1 | 255.255.255.0 | 192.168.3.8 |
| PC1 | 192.168.3.3 | 255.255.255.0 | 192.168.3.8 |
| Серверы | | | |
| Server0 | 192.168.3.8 | 255.255.255.0 | 192.168.3.8 |
| Server1 | 192.168.3.5 | 255.255.255.0 | 192.168.3.8 |
| Вариант 4 | | | |
| Конечные узлы | IP-адрес | Маска сети | IP-адрес DNS-сервера |
| PC0 | 172.16.2.90 | 255.255.0.0 | 172.16.2.25 |
| PC1 | 172.16.2.10 | 255.255.0.0 | 172.16.2.25 |
| Серверы | | | |
| Server0 | 172.16.2.25 | 255.255.0.0 | 172.16.2.25 |
| Server1 | 172.16.2.40 | 255.255.0.0 | 172.16.2.25 |
| Вариант 5 | | | |
| Конечные узлы | IP-адрес | Маска сети | IP-адрес DNS-сервера |
| PC0 | 192.168.5.1 | 255.255.255.0 | 192.168.5.7 |
| PC1 | 192.168.5.3 | 255.255.255.0 | 192.168.5.7 |
| Серверы | | | |
| Server0 | 192.168.5.7 | 255.255.255.0 | 192.168.5.7 |
| Server1 | 192.168.5.5 | 255.255.255.0 | 192.168.5.7 |
| Вариант 6 | | | |
| Конечные узлы | IP-адрес | Маска сети | IP-адрес DNS-сервера |
| PC0 | 192.168.4.1 | 255.255.255.0 | 192.168.4.9 |
| PC1 | 192.168.4.3 | 255.255.255.0 | 192.168.4.9 |
| Сервер | | | |
| Server0 | 192.168.4.9 | 255.255.255.0 | 192.168.4.9 |
| Server1 | 192.168.4.6 | 255.255.255.0 | 192.168.4.9 |
| Вариант 7 | | | |
| Конечные узлы | IP-адрес | Маска сети | IP-адрес DNS-сервера |
| PC0 | 172.16.3.15 | 255.255.0.0 | 172.16.3.70 |
| PC1 | 172.16.3.25 | 255.255.0.0 | 172.16.3.70 |
| Серверы | | | |
| Server0 | 172.16.3.70 | 255.255.0.0 | 172.16.3.70 |
| Server1 | 172.16.3.40 | 255.255.0.0 | 172.16.3.70 |
| Вариант 8 | | | |
| Конечные узлы | IP-адрес | Маска сети | IP-адрес DNS-сервера |
| PC0 | 172.16.4.90 | 255.255.0.0 | 172.16.4.30 |
| PC1 | 172.16.4.10 | 255.255.0.0 | 172.16.4.30 |
| Серверы | | | |
| Server0 | 172.16.4.30 | 255.255.0.0 | 172.16.4.30 |
| Server1 | 172.16.4.100 | 255.255.0.0 | 172.16.4.30 |
| Вариант 9 | | | |
| Конечные узлы | IP-адрес | Маска сети | IP-адрес DNS-сервера |
| PC0 | 172.16.5.20 | 255.255.0.0 | 172.16.5.10 |
| PC1 | 172.16.5.40 | 255.255.0.0 | 172.16.5.10 |
| Серверы | | | |
| Server0 | 172.16.5.10 | 255.255.0.0 | 172.16.5.10 |
| Server1 | 172.16.5.80 | 255.255.0.0 | 172.16.5.10 |
| Вариант 10 | | | |
| Конечные узлы | IP-адрес | Маска сети | IP-адрес DNS-сервера |
| PC0 | 172.16.6.20 | 255.255.0.0 | 172.16.6.40 |
| PC1 | 172.16.6.10 | 255.255.0.0 | 172.16.6.40 |
| Серверы | | | |
| Server0 | 172.16.6.40 | 255.255.0.0 | 172.16.6.40 |
| Server1 | 172.16.6.30 | 255.255.0.0 | 172.16.6.40 |
| Вариант 11 | | | |
| Конечные узлы | IP-адрес | Маска сети | IP-адрес DNS-сервера |
| PC0 | 192.168.6.2 | 255.255.255.0 | 192.168.6.7 |
| PC1 | 192.168.6.3 | 255.255.255.0 | 192.168.6.7 |
| Серверы | | | |
| Server0 | 192.168.6.7 | 255.255.255.0 | 192.168.6.7 |
| Server1 | 192.168.6.5 | 255.255.255.0 | 192.168.6.7 |
| Вариант 12 | | | |
| Конечные узлы | IP-адрес | Маска сети | IP-адрес DNS-сервера |
| PC0 | 192.168.7.2 | 255.255.255.0 | 192.168.7.5 |
| PC1 | 192.168.7.4 | 255.255.255.0 | 192.168.7.5 |
| Серверы | | | |
| Server0 | 192.168.7.5 | 255.255.255.0 | 192.168.7.5 |
| Server1 | 192.168.7.8 | 255.255.255.0 | 192.168.7.5 |
| Вариант 13 | | | |
| Конечные узлы | IP-адрес | Маска сети | IP-адрес DNS-сервера |
| PC0 | 192.168.8.4 | 255.255.255.0 | 192.168.8.2 |
| PC1 | 192.168.8.3 | 255.255.255.0 | 192.168.8.2 |
| Серверы | | | |
| Server0 | 192.168.8.2 | 255.255.255.0 | 192.168.8.2 |
| Server1 | 192.168.8.8 | 255.255.255.0 | 192.168.8.2 |
| Вариант 14 | | | |
| Конечные узлы | IP-адрес | Маска сети | IP-адрес DNS-сервера |
| PC0 | 192.168.9.3 | 255.255.255.0 | 192.168.9.6 |
| PC1 | 192.168.9.4 | 255.255.255.0 | 192.168.9.6 |
| Серверы | | | |
| Server0 | 192.168.9.6 | 255.255.255.0 | 192.168.9.6 |
| Server1 | 192.168.9.7 | 255.255.255.0 | 192.168.9.6 |

Размещено на Allbest.ru