Министерство науки и высшего образования РФ

Томский государственный университет
систем управления и радиоэлектроники

**А.К. Новохрестов, А.Ю. Якимук**

# ТЕХНОЛОГИИ ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ КАНАЛОВ ПЕРЕДАЧИ ДАННЫХ

Учебно-методическое пособие
для студентов направлений подготовки
10.00.00 Информационная безопасность

Томск
2022

**УДК** 004.056
**ББК** 32.973.26-018.2
Н 64

**Новохрестов Алексей Константинович**
Н 64 Технологии построения защищенных каналов передачи данных: учебно-методическое пособие/ А.К. Новохрестов, А.Ю. Якимук. – Томск: Томск. гос. ун-т систем упр. и радиоэлектроники, 2022. – 166 с.

Настоящее учебно-методическое пособие содержит описания лабораторных и самостоятельных работ по дисциплине «Технологии построения защищенных каналов передачи данных» для направлений подготовки, входящих в укрупненную группу специальностей и направлений 10.00.00 Информационная безопасность.

УДК 004.056
ББК 32.973.26-018.2

© Новохрестов А.К., Якимук А.Ю. 2022
© Томск. гос. ун-т систем упр. и радиоэлектроники, 2022

**СОДЕРЖАНИЕ**

## Введение

Целью преподавания дисциплины является подготовка студента к деятельности, связанной с выработкой предложений по вопросам построения защищенных каналов передачи данных, разработке предложений по совершенствованию и повышению эффективности комплекса мер защиты каналов передачи данных.

Задачи изучения дисциплины:

– Изучить принципы построения защищенных каналов передачи данных и управления ими;

– Обучить студентов использованию программных и аппаратных средств защиты каналов передачи данных;

– Познакомить студентов с методами проектирования, развертывания и сопровождения защищенных каналов передачи данных;

– Познакомить студентов с методами обследования и анализа защищенности каналов передачи данных.

## ЛАБОРАТОРНАЯ РАБОТА №1
## Сетевые диагностические утилиты

### 1 Краткая теоретическая справка

Интерфейс командной строки активно используется сетевыми администраторами и разработчиками оборудования для оперативного администрирования сети – конфигурирования и управления коммутаторами и маршрутизаторами. Доступ к командной строке зависит от типа операционной системы. В системе Windows для доступа к командной строке необходимо выполнить последовательность действий: Пуск→Выполнить и в открывшемся окне набрать cmd (cmd.exe) , рис. 1.1.

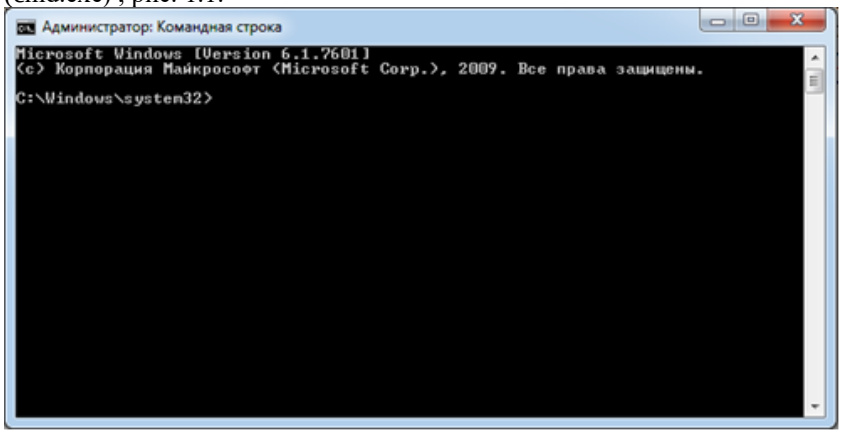



Рисунок 1.1 – Интерфейс командной строки в Windows

В среде операционных систем Windows Vista/Windows 7 интерпретатор cmd.exe должен быть запущен для выполнения с использованием пункта контекстного меню

«Запустить от имени администратора». Командные файлы, в которых используются сетевые утилиты, также должны выполняться в контексте учетной записи с привилегиями администратора. В списке представлены сетевые утилиты командной строки для получения информации о сетевых настройках, выполнения операций по конфигурированию и диагностике сети.

Далее в данном разделе рассматриваются следующие диагностические утилиты, предназначенные для проверки конфигурации и тестирования сетевых соединений (табл. 1.1).

Таблица 1.1 – Сетевые утилиты

| **Утилита** | **Назначение** |
|---|---|
| hostname | Выводит имя локального хоста, используется без параметров |
| ipconfig | Выводит значения для текущей конфигурации: IP-адрес, маску подсети, адрес шлюза по умолчанию, адреса WINS (Windows Internet Naming Service) и DNS (Domain Name System) |
| ping | Осуществляет проверку связи с удаленным хостом путем отправки эхо-пакетов ICMP (Internet Control Message Protocol) |
| tracert | Осуществляет проверку маршрута к удаленному компьютеру путем отправки эхо-пакетов протокола ICMP и выводит маршрут прохождения пакетов на удаленный компьютер |
| arp | Выводит для просмотра и изменения таблицу трансляции адресов, используемую протоколом разрешения адресов ARP (Address Resolution Protocol – определяет локальный адрес по IP-адресу) |
| route | Модифицирует таблицы маршрутизации IP (отображает содержимое таблицы, добавляет и удаляет маршруты IP) |
| netstat | Выводит статистику и текущую информацию по соединениям |
| nslookup | Осуществляет проверку записей и доменных псевдонимов хостов, доменных сервисов хостов путем запросов к серверам DNS |
| telnet | Осуществляет соединение с другим хостом по протоколу эмуляции терминалаTELNET и используется для проверки работоспособности сетевых служб, использующих TCP-порты (например, возможности соединения с почтовым сервером по протоколам POP3 и SMTP) |

В описании команд используется:

<текст> – текст в угловых скобках, обязательный параметр. [текст] – текст в квадратных скобках, необязательный параметр.

(текст) – текст в круглых скобках, необходимо выбрать один из параметров.

Вертикальная черта | – разделитель для взаимоисключающих параметров, нужно выбрать один из них.

Многоточие ... – возможно повторение параметров.

## 1.2 Последовательность выполнения работы

Необходимо ознакомиться с синтаксисом использования утилит и освоить особенности их использования.

**Утилита ipconfig**. При устранении неисправностей и проблем в сети следует сначала проверить правильность конфигурации. Для этого используется утилита ipconfig, рис. 1.2. Она полезна на компьютерах, работающих с DHCP (Dynamic Host Configuration Protocol), так как дает пользователям возможность определить, какая конфигурация сети и какие величины были установлены с помощью DHCP.

**Синтаксис:** ipconfig [/all | /renew[adapter] | /release[adapter]]

**Параметры:**

/all – вывод подробных сведений (выдает весь список параметров, без этого ключа происходит вывод сведений (отображается только IP-адрес, маска и шлюз по умолчанию));

/renew [adapter] – обновление IP-адреса для указанного сетевого адаптера;

/release [adapter] – освобождение IP-адресов для указанного сетевого адаптера;adapter – имя сетевого адаптера;

/displaydns – выводит информацию о содержимом локального кэша клиента DNS, используемого для разрешения доменных имен.

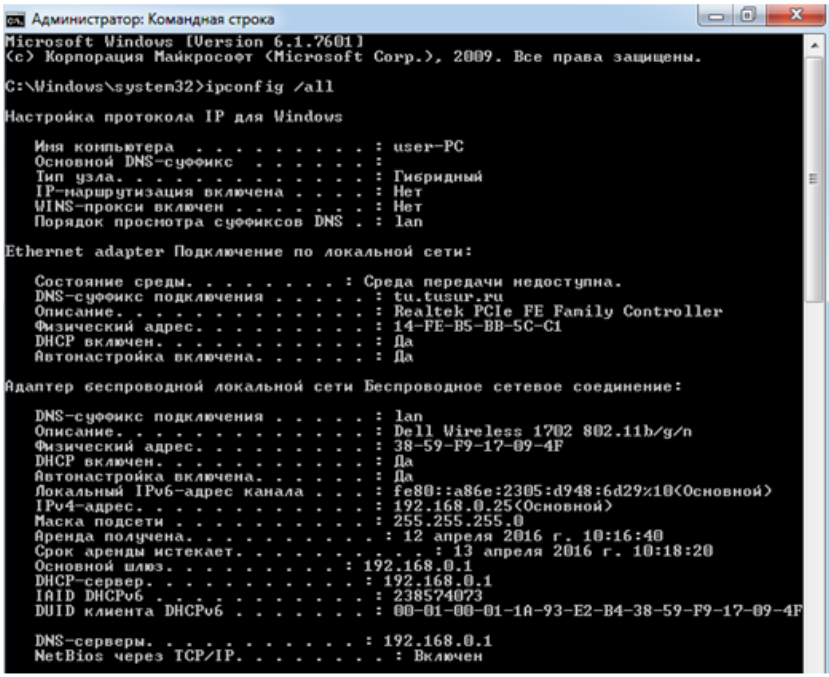



Рисунок 1.2 – пример использования утилиты ipconfig

Таким образом, утилита ipconfig позволяетвыяснить, инициализирована ли конфигурация и не дублируются ли IP-адреса:

• если конфигурация инициализирована, то появляется IP-адрес, маска, шлюз;

• если IP-адреса дублируются, то маска сети будет 0.0.0.0;

• если при использовании DHCP компьютер не смог получить IP-адрес, то он будет равен 0.0.0.0 .

Пример поочередного использования ключей /release (после этого становятся недоступны ранее созданные соединения) и /renew, приведен на рис. 1.3.

Утилита ping (Packet Internet Grouper) используется для проверки конфигурирования и диагностики ошибок соединения. Она определяет доступность и функционирование конкретного узла или хоста. Использование ping лучший способ проверки того, что между компьютерами существует маршрут. Утилита проверяет соединение путем посылки эхо-пакетов ICMP и прослушивания эхо-ответов. Ping ожидает каждый посланный пакет и печатает количество переданных и

принятых пакетов. Каждый принятый пакет проверяется в соответствии с переданным сообщением. Поэтому из сообщений ping становится ясно, сколько пакетов потеряно и по этим данным можно судить о качестве связи.

По умолчанию (в Windows) передается 4 эхо-пакета длиной 32 байта (возможны и другие варианты значения по умолчанию) – периодическая последовательность символов алфавита в верхнем регистре. Ping позволяет изменить размер и количество пакетов, указать, следует ли записывать маршрут, который она использует, какую величину времени жизни (TTL) устанавливать, можно ли фрагментировать пакет и т.д. При получении ответа в поле Time указывается, за какое время (в миллисекундах) посланный пакет доходит до удаленного хоста и возвращается назад. Так как значение по умолчанию для ожидания отклика равно 1 секунде, то все значения данного поля будут меньше 1000 миллисекунд. Если в окне отображается сообщение «Request time out» (Превышен интервал ожидания), то, возможно, если увеличить время ожидания отклика, пакет дойдет до удаленного хоста. Это можно сделать с помощью ключа –w.


Рисунок 1.3 – Пример использования ключей /release и /renew

Ping можно использовать для тестирования как имени хоста (DNS или NetBIOS), так и его IP-адреса. Если ping с IP-адресом выполнилась успешно, а с именем – неудачно, это значит, что проблема заключается в распознавании соответствия адреса и имени, а не в сетевом соединении.

Утилита ping используется следующими способами:

Для проверки того, что TCP/IP установлен и правильно сконфигурирован на локальном компьютере, в команде ping задается адрес петли обратной связи (loopback address), рис. 1.4.

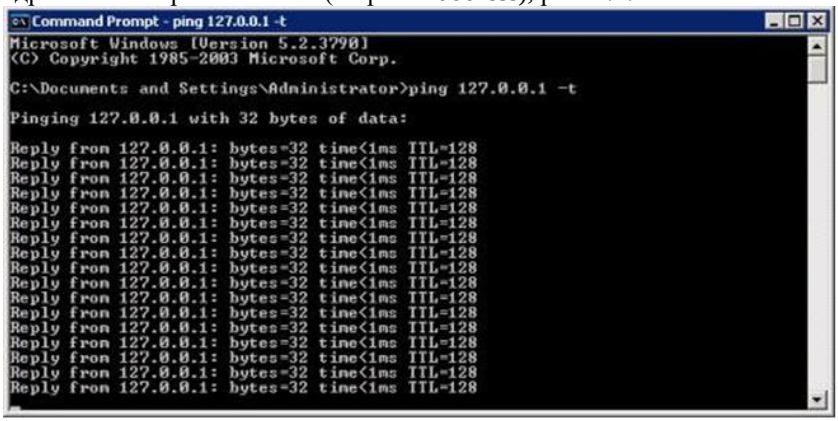



Рисунок 1.4 – Использование петли обратной связи для проверки работы TCP/IP

Чтобы убедиться в том, что компьютер правильно добавлен в сеть и IP-адрес не

дублируется, используется IP-адрес локального компьютера: ping IP-адрес_локального_хоста

Чтобы проверить, что шлюз по умолчанию функционирует и что можно установить соединение с любым локальным хостом в локальной сети, задается IP-адрес шлюза по умолчанию:

ping IP-адрес_шлюза

Для проверки возможности установления соединения через маршрутизатор в команде ping задается IP-адрес удаленного хоста:

ping IP-адрес_удаленного хоста Синтаксис:

ping [-t] [-a] [-n count] [-l length] [-f] [-i ttl] [-v tos] [-r count] [-s count] [ [-j host-list] | [-k host- list] ] [-w timeout] destination-list

Параметры:

-t –выполняет команду ping до прерывания (Ctrl-C – прервать выполнение команды);

-a – позволяет определить доменное имя удаленного компьютера по его IP-адресу;

-n count – посылает количество пакетов ECHO, указанное параметром count;

-l length – посылает пакеты длиной length байт (максимальная длина 8192 байта);

-f – посылает пакет с установленным флагом «не фрагментировать». Этот пакет не будет фрагментироваться на маршрутизаторах по пути своего следования;

-i ttl – устанавливает время жизни пакета в величину ttl (каждый маршрутизатор уменьшает ttl на единицу);

-v tos – устанавливает тип поля «сервис» в величину tos;

-r count – записывает путь выходящего пакета и возвращающегося пакета в поле записи пути. Count – от 1 до 9 хостов;

-s count – позволяет ограничить количество переходов из одной подсети в другую (хопов). Count задает максимально возможное количество хопов;

-j host-list – направляет пакеты с помощью списка хостов, определенного параметром host-list. Последовательные хосты могут быть отделены промежуточными маршрутизаторами (гибкая статическая маршрутизация). Максимальное количество хостов в списке, позволенное IP, равно 9;

-k host-list – направляет пакеты через список хостов, определенный в host-list. Последовательные хосты не могут быть разделены промежуточными маршрутизаторами (жесткая статическая маршрутизация). Максимальное количество хостов – 9;

-w timeout – указывает время ожидания (timeout) ответа от удаленного хоста в миллисекундах (по умолчанию – 1сек);

-destination-list – указывает удаленный хост, к которому надо направить пакеты ping. Пример использования утилиты ping: C:\WINDOWS>ping –n 6 www.netscape.com Обмен пакетами с www.netscape.com [205.188.247.65] по 32 байт:

Ответ от 205.188.247.65: число байт=32 время=194мс TTL=48 Ответ от 205.188.247.65: число байт=32 время=240мс TTL=48 Ответ от 205.188.247.65: число байт=32 время=173мс TTL=48 Ответ от 205.188.247.65: число байт=32 время=250мс TTL=48 Ответ от 205.188.247.65: число байт=32 время=187мс TTL=48 Ответ от 205.188.247.65: число байт=32 время=239мс TTL=48 Статистика Ping для 205.188.247.65:

Пакетов: послано = 6, получено = 6, потеряно = 0 (0% потерь) Приблизительное время передачи и приема:

Наименьшее = 173мс, наибольшее = 406мс, среднее =236мс

В случае невозможности проверить доступность хоста утилита выводит информацию об ошибке. Ниже приведен пример ответа утилиты ping при попытке послать запрос на несуществующий хост.

Обмен пакетами с 172.16.6.21 по 32 байт:

Превышен интервал ожидания для запроса. Превышен интервал ожидания для запроса. Превышен интервал ожидания для запроса. Превышен интервал ожидания для запроса. Статистика Ping для 172.16.6.21:

Пакетов: отправлено = 4, получено = 0, потеряно = 4 (100% потерь), Приблизительное время передачи и приема:

наименьшее = 0мс, наибольшее = 0мс, среднее = 0мс

Утилита сообщает не об отсутствии хоста, а о том, что за отведенное время не был получен ответ на посланный запрос. Причиной этого не обязательно является отсутствие хоста в сети. Проблема может крыться в сбоях связи, перегрузке или неправильной настройке маршрутизаторов и т. п. Ошибка «сеть недоступна» (network unreachable) прямо указывает на проблемы маршрутизации.

Утилита tracert предназначена для трассировки маршрута. Она использует поле TTL (time-to-live, время жизни) пакета IP и сообщения об ошибках ICMP для определения маршрута от одного хоста до другого. Утилита может быть более содержательной и удобной, чем ping, особенно в тех случаях, когда удаленный хост недостижим. С помощью нее можно определить район проблем со связью (у Internet-провайдера, в опорной сети, в сети удаленного хоста) по тому, насколько далеко будет отслежен маршрут. Если возникли проблемы, то утилита выводит на экран звездочки (*), либо сообщения типа «Destination net unreachable», «Destination host unreachable», «Request time out», «Time Exeeded».

Утилита tracert работает следующим образом: посылается по 3 пробных эхо-пакета на каждый хост, через который проходит маршрут до удаленного хоста. На экран при этом выводится время ожидания ответа на каждый пакет (его можно изменить с помощью параметра -w). Пакеты посылаются с различными величинами времени жизни. Каждый маршрутизатор, встречающийся по пути, перед перенаправлением пакета уменьшает

величину TTL на единицу. Таким образом, время жизни является счетчиком точек промежуточной доставки (хопов). Когда время жизни пакета достигнет нуля, предполагается, что маршрутизатор пошлет в компьютер-источник сообщение ICMP “Time Exeeded” (Время истекло).

Маршрут определяется путем посылки первого эхо- пакета с TTL=1. Затем TTL увеличивается на 1 в каждом последующем пакете до тех пор, пока пакет не достигнет удаленного хоста, либо будет достигнута максимально возможная величина TTL (по умолчанию 30, задается с помощью параметра -h).

Маршрут определяется путем изучения сообщений ICMP, которые присылаются обратно промежуточными маршрутизаторами ( некоторые маршрутизаторы просто молча уничтожают пакеты с истекшим TTL и не будут видны утилите tracert).

Синтаксис:

tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] имя_целевого_хоста.

Параметры:

-d – указывает, что не нужно распознавать адреса для имен хостов;

-h maximum_hops – указывает максимальное число хопов для того, чтобы искать

цель;

-j host-list – указывает нежесткую статическую маршрутизацию в соответствии с

host-list;

-w timeout – указывает, что нужно ожидать ответ на каждый эхо-пакет заданное число мсек.

В качестве примера можно просмотреть трассировку до goooogle.com или ya.ru. Пример использования утилиты tracert: C:\WINDOWS>tracert yandex.ru

Утилита arp. Основная задача протокола ARP – трансляция IP-адресов в соответствующие локальные адреса. Для этого ARP-протокол использует информацию из ARP-таблицы (ARP-кэша). Если необходимая запись в таблице не найдена, то протокол ARP отправляет широковещательный запрос ко всем компьютерам локальной подсети, пытаясь найти владельца данного IP-адреса. В кэше могут содержаться два типа записей: статические и динамические. Статические записи вводятся вручную и хранятся в кэше постоянно. Динамические записи помещаются в кэш в результате выполнения широковещательных запросов. Для них существует понятие времени жизни. Если в течение определенного времени (по умолчанию 2 мин.) запись не была востребована, то она удаляется из кэша.

Синтаксис:

arp [-s inet_addr eth_addr] | [-d inet_addr] | [-a].

Параметры:

-s –занесение в кэш статических записей;

-d – удаление из кэша записи для определенного IP-адреса;

-a – просмотр содержимого кэша для всех сетевых адаптеров локального компьютера;

inet_addr – IP-адрес; eth_addr – MAC-адрес.

Пример использования утилиты arp: arp –a, рис. 1.5.

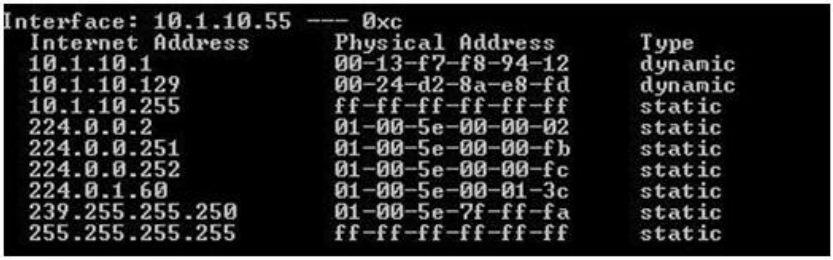



Рисунок 1.5 – Пример использования утилиты arp

Утилита route предназначена для работы с локальной таблицей маршрутизации.

Она имеет следующий Синтаксис:

route [-f] [-p] [команда [узел] [MASK маска] [шлюз] [METRIC метрика] [IF интерфейс]].

Параметры:

-f – Очистка таблицы маршрутизации.

-p – При указании совместно с командой ADD создает постоянную запись, которая сохраняется после перезагрузки компьютера. По умолчанию записи таблицы маршрутов не сохраняются при перезагрузке.

команда одна из четырех команд:

PRINT - вывод информации о маршруте; ADD - добавление маршрута;

DELETE - удаление маршрута; CHANGE - изменение маршрута.

узел адресуемый узел;

маска маска подсети; по умолчанию используется маска 255.255.255.255;

шлюз адрес шлюза;

метрика метрика маршрута;

интерфейс идентификатор интерфейса, который будет использован для пересылки пакета.

Для команд PRINT и DELETE возможно использование символов подстановки при указании адресуемого узла или шлюза. Параметр шлюза для этих команд может быть опущен.

При добавлении и изменении маршрутов утилита route осуществляет проверку введенной информации на соответствие условию (УЗЕЛ & МАСКА) = УЗЕЛ. Если это условие не выполняется, то утилита выдает сообщение об ошибке и не добавляет или не изменяет маршрут.

Утилита осуществляет поиск имен сетей в файле networks. Поиск имен шлюзов осуществляется в файле hosts. Оба файла расположены в папке \system32\drivers\etc. Наличие и заполнение этих файлов не обязательно для нормального функционирования утилиты route и работы маршрутизации.

Хотя в большинстве случаев на рабочей станции это не требуется, можно вручную редактировать таблицы маршрутизации.

Пример использования утилиты route (добавление статического маршрута): route add 172.16.6.0 MASK 255.255.255.0 172.16.11.1 METRIC 1 IF 0x1000003.

Утилита netstat позволяет получить статическую информацию по некоторым из протоколов стека (TCP, UDP, IP, ICMP), а также выводит сведения о текущих сетевых соединениях. Особенно она полезна на брандмауэрах. Так, с ее помощью можно обнаружить нарушения безопасности периметра сети.

Синтаксис:

netstat [-a] [-e] [-n] [-s] [-p protocol] [-r].

Параметры:

-a – выводит перечень всех сетевых соединений и прослушивающихся портов локального компьютера;

-e – выводит статистику для Ethernet-интерфейсов (например, количество полученных и отправленных байт);

-n – выводит информацию по всем текущим соединениям (например, TCP) для всех сетевых интерфейсов локального компьютера. Для каждого соединения выводится информация об IP-адресах локального и удаленного интерфейсов вместе с номерами используемых портов;

-s – выводит статистическую информацию для протоколов UDP, TCP, ICMP, IP.

-r – выводит содержимое таблицы маршрутизации. Пример использования утилиты приведен на рис. 1.6.

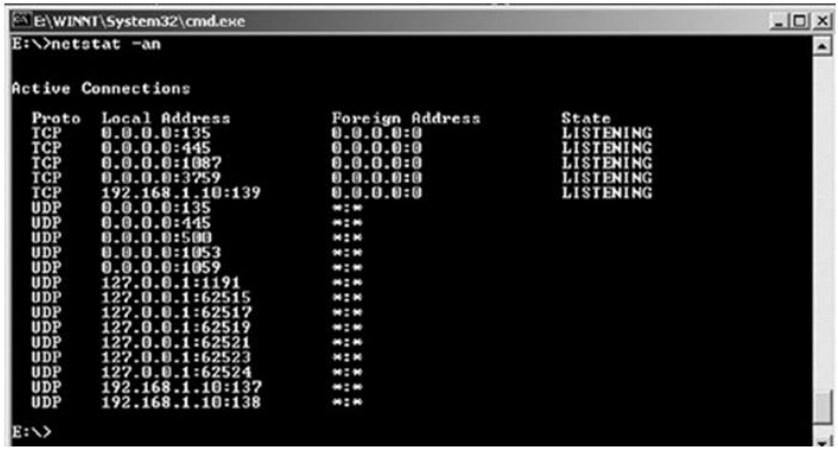



Рисунок 1.6 – Пример использования утилиты netstat

Утилита nslookup предназначена для диагностики службы DNS, в простейшем случае – для выполнения запросов к DNS-серверам на разрешение имен в IP-адреса. В общем случае утилита позволяет просмотреть любые записи DNS-сервера:

A – каноническое имя узла, устанавливает соответствие доменного имени ip-адресу.

SOA – начало полномочий, начальная запись, единственная для зоны;

MX – почтовые серверы (хосты, принимающие почту для заданного домена);

NS – серверы имен (содержит авторитетные DNS-серверы для зоны);

PTR – указатель (служит для обратного преобразования ip-адреса в символьное имя хоста) и т. д.

Утилита nslookup достаточно сложна и содержит свой собственный командный интерпретатор. В простейшем случае (без входа в командный режим) утилита nslookup имеет следующий

Синтаксис: nslookup хост [сервер].

Параметры:

Хост – DNS-имя хоста, которое должно быть преобразовано в IP-адрес.

Сервер – Адрес DNS-сервера, который будет использоваться для разрешения имени. Если этот параметр опущен, то будут

последовательно использованы адреса DNS- серверов из параметров настройки протокола TCP/IP.

Примеры использования утилиты nslookup:

1. Получение списка серверов имен для домена ya.ru без входа в командный режим (с использованием ключей), рис. 1.7.

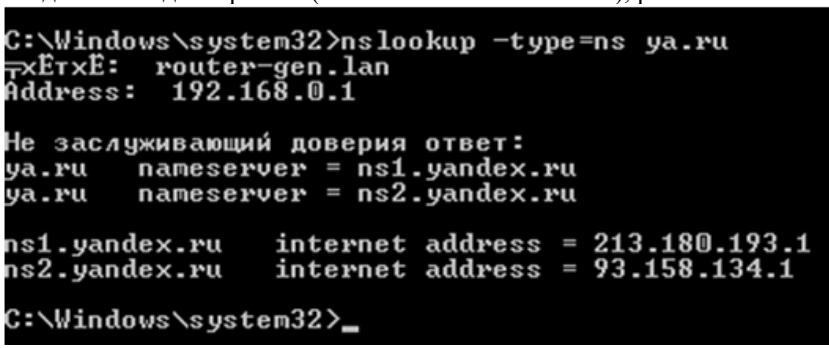



Рисунок 1.7 – Пример использования утилиты nslookup

2. Получение записи SOA домена ya.ru с авторитетного сервера с использование командного интерпретатора nslookup.

C:\>nslookup
Default Server: dns04.catv.ext.ru Address: 217.10.39.4
> set type=SOA
> server ns2.yandex.ru Default Server: ns2.yandex.ru Address: 213.180.199.34
> yandex.ru
Server: ns1.yandex.ru Address: 213.180.193.1
>yandex.ru
primary name server = ns1.yandex.ru responsible mail addr = sysadmin.yandex-team.r serial = 2009022707
refresh = 1800 (30 mins)
retry = 900 (15 mins)
expire = 2592000 (30 days)
default TTL = 900 (15 mins) yandex.ru nameserver = ns5.yandex.ru yandex.ru nameserver = ns1.yandex.ru yandex.ru
nameserver = ns4.yandex.ru yandex.ru nameserver = ns2.yandex.ru

ns1.yandex.ru internet address = 213.180.193.1 ns2.yandex.ru internet address = 213.180.199.34 ns4.yandex.ru internet address = 77.88.19.60 ns5.yandex.ru internet address = 213.180.204.1

> exit

3. Получение адреса почтового сервера для домена yandex.ru. C:\ >nslookup

Default Server: dns01.catv.ext.ru Address: 217.10.44.35

> set q=mx

> yandex.ru

Server: dns01.catv.ext.ru Address: 217.10.44.35 Non-authoritative answer:

yandex.ru MX preference = 10, mail exchanger = mx2.yandex.ru yandex.ru MX preference = 10, mail exchanger = mx3.yandex.ru yandex.ru MX preference = 10, mail exchanger = mx1.yandex.ru yandex.ru nameserver = ns2.yandex.ru

yandex.ru nameserver = ns1.yandex.ru yandex.ru nameserver = ns4.yandex.ru yandex.ru nameserver = ns5.yandex.ru mx1.yandex.ru internet address = 77.88.21.89 mx2.yandex.ru internet address = 93.158.134.89 mx3.yandex.ru internet address = 213.180.204.89 ns2.yandex.ru internet address = 213.180.199.34 ns4.yandex.ru internet address = 77.88.19.60 ns5.yandex.ru internet address = 213.180.204.1

Указав ключ type=any, можно получить все записи об узле или домене. Ключи querytype, t, q эквивалентны type.

Утилита telnet1 (TELecommunication NETwork) реализует клиентскую часть сетевого протокола telnet, организующего текстовый интерфейс по сети (при помощи транспортного протокола TCP).

Исторически Telnet служил для удалённого доступа к интерфейсу командной строки операционных систем. Впоследствии его стали использовать для прочих текстовых интерфейсов. Теоретически, даже обе стороны протокола могут являться программами, а не человеком. Иногда клиенты telnet используются для доступа к другим протоколам на основе транспорта TCP.

Протокол telnet используется в управляющем соединении FTP, т.е. заходить на сервер командой telnet ftp.example.net для выполнения отладки и экспериментов не только возможно, но и правильно (в отличие от применения клиентов telnet для доступа к HTTP, IRC и большинству других протоколов). В протоколе не предусмотрело ни шифрования, ни проверки подлинности данных. Поэтому он уязвим для любого вида атак на TCP. Для функциональности удалённого доступа к системе в настоящее время применяется сетевой протокол SSH

(особенно его версия 2), при создании которого упор делался именно на вопросы безопасности. Следует иметь в виду, что сессия telnet обладает крайне низкой защищенностью, если только не осуществляется в полностью контролируемой сети или с применением защиты на сетевом уровне (различные реализации виртуальных частных сетей). По причине ненадёжности от telnet как средства управления операционными системами давно отказались.

Тем не менее, клиент telnet пригоден для осуществления ручного доступа (например, в целях отладки) к таким протоколам прикладного уровня как HTTP, IRC, SMTP, POP3 и прочим текст-ориентированным протоколам на основе транспорта TCP. По умолчанию (если порт не задан), telnet использует порт 23.

Синтаксис:

telnet имя_узла номер_порта.

1.3 Задание для самостоятельной работы

Выведите на экран справочную информацию по всем рассмотренным утилитам (см. таблицу). Для этого в командной строке введите имя утилиты без параметров или с /?. Для получения справочной информации. По nslookup необходимо войти в командный режим, набрав nslookup без параметров, и ввести команду help.

Необходимо изучите ключи, используемые при запуске утилит. Далее вывести на экран имя локального хоста с помощью команды hostname, проверить конфигурацию TCP/IP с помощью утилиты ipconfig и заполнить таблицу.

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

С помощью утилит необходимо:

4. Проверить правильность установки и конфигурирования TCP/IP на локальном компьютере.

5. Проверить, правильно ли добавлен в сеть локальный компьютер и не дублируется ли IP-адрес.

6. Проверить функционирование шлюза по умолчанию, послав 5 эхо-пакетов длиной 64 байта.

7. Проверить возможность установления соединения с удаленным хостом.

8. С помощью утилиты ping проверить перечисленные ниже адреса и для каждого из них отметьте время отклика. Далее необходимо попробовать изменить параметры команды ping таким образом, чтобы увеличилось время отклика.

- yandex.ru;
- google.com;
- feko.info;
- любой узел из локальной сети.

9. Изучить синтаксис утилиты getmac.

10. С помощью команды tracert проверить для перечисленных ниже адресов, через какие промежуточные узлы идет передача (время жизни установить равным 10):

- tusur.ru;
- yandex.ru;
- google.com;
- feko.info.

11. Используя утилиту arp просмотреть ARP-таблицу локального компьютера. Внести в кэш локального компьютера любую статическую запись.

12. С помощью утилиты route просмотреть локальную таблицу маршрутизации.

13. С помощью утилиты netstat выведите перечень сетевых соединений и статистическую информацию для протоколов UDP, TCP, ICMP, IP.

14. Используя nslookup определить ip-адреса следующих узлов:

- ru.wikipedia.org;
- mail.ru;
- vk.com.

15. Результаты показать преподавателю.

# ЛАБОРАТОРНАЯ РАБОТА №2
# Симулятор Cisco Packet Tracer

## 1 Краткая теоретическая справка

В данном разделе приведено вводное описание функциональных возможностей симулятора CISCO Packet Tracer.

В процессе проектирования компьютерных важным этапом является исследование технических решений на предмет выполнения ими заданных функций. Такое исследование может быть проведено двумя способами: натурным экспериментом и компьютерным имитационным моделированием. В первом случае проектировщики, используя реальное оборудование, собирают требуемую компьютерную сеть и проводят необходимые эксперименты. Очевидно, что стоимость таких экспериментов достаточно высока и определяется в большей степени стоимостью используемого оборудования. С целью сокращения стоимости экспериментов используется компьютерное имитационное моделирование, в котором вместо реального оборудования используется их программные аналоги.

На рынке программного обеспечения существует множество различных сред имитационного моделирования компьютерных сетей. Наибольшую популярность получили две среды имитационного моделирования компьютерных сетей: GNS3 и CISCO Packet Tracer. Первая среда является свободно распространяемой и реализует имитационное моделирование путем виртуализации реального оборудования. Вторая среда распространяется свободно, но в рамках сетевых академий компании Cisco systems, Inc, и моделирует только оборудование этого производителя. Далее будет использоваться среда CISCO Packet Tracer (CPT).

### 1.1 Последовательность выполнения работы

Запустив программу, пользователь видит главное окно (рис. 1.1).

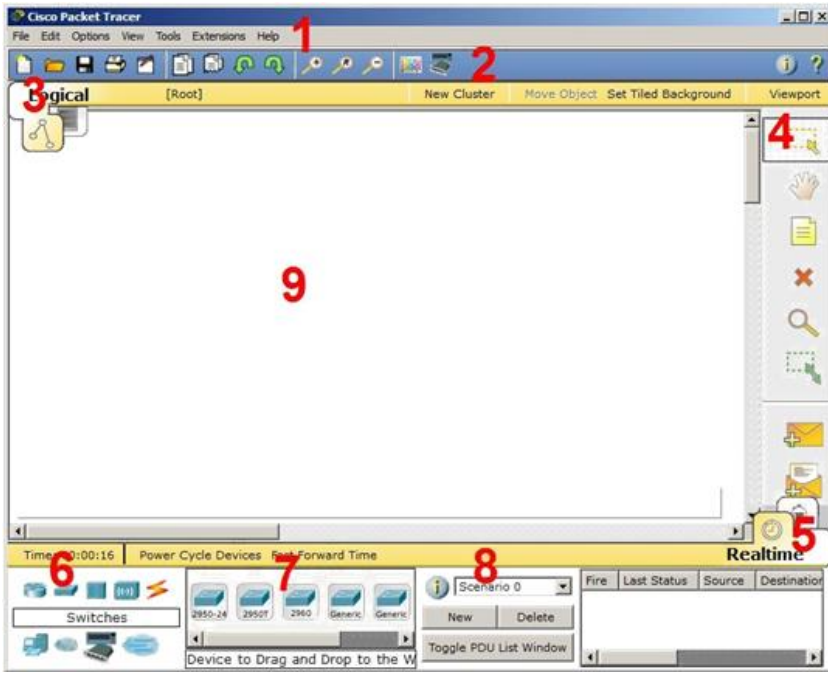



Рисунок 1.1 - Главное окно программы Cisco Packet Tracer

1. Главное меню содержит стандартные пункты: Файл (File), Правка (Edit), Настройки (Options), Вид (View), Инструменты (Tools), Расширения (Extensions), Помощь (Help). Особого внимания заслуживает пункт Расширения, содержащий мастер проектов, многопользовательский режим и ряд других дополнительных возможностей, которые с помощью CPT могут сформировать целую лабораторию.

2. Панель инструментов, часть которых просто дублирует пункты главного меню.

3. Переключатель логической и физической организации рабочего пространства. В режиме «логическая сеть» располагаются сетевые объекты и указываются связи между ними. В режиме «физическая сеть» указывается расположение сетевых объектов и каналов связей в помещениях (как они расположены, в каких стойках и т.п.). В этой же строке располагаются кнопки управления отображением: <Root> - уровень детализации, «New Cluster» - создать объединенное устройство, «Set Tiled Background» - установить фон

рабочей области, «NAVIGATION» - навигация между уровнями отображения физической сети (Район, Город, этаж).

4. Вертикальная панель инструментов, содержащая средства выделения, удаления, перемещения, масштабирования объектов, а также формирования и передачи пакетов данных (PDU) между устройствами.

| | |
|---|---|
|  | Инструмент **Select**. Позволяет выделить один или несколько объектов моделируемой компьютерной сети (логической или физической топологии) |
|  | Инструмент **Move Layout**. Используется для прокрутки схемы модулируемой сети в основном окне рабочего пространства. Для выполнения этого действия могут также использоваться полосы прокрутки. |
|  | Инструмент **Place Note**. Позволяет добавить в текущую моделируемую схему текстовую надпись. |
|  | Инструмент **Delete**. Переключает в режим удаления выделяемых объектов схемы сети. |
|  | Инструмент **Inspect**. Позволяет просматривать таблицы состояния (таблица маршрутизации и т.п.) объектов моделируемой сети. |
|  | Инструмент **Resize Shape**. Используется для изменения размеров графических объектов, размещаемых на схеме с использованием панели «Графические объекты». |
|  | Инструмент **Add Simple PDU**. Позволяет создать эмуляцию простой передачи пакета данных (ICMP, ping) от одного устройства сети к другому. |
|  | Инструмент **Add Complex PDU**. Создает эмуляцию передачи пакета данных от одного устройства к другому. Позволяет задать параметры пакета (тип протокола, исходящий порт и т.п.). |

5. Переключатель режима реального времени (Realtime) и режима симуляции (Simulation Mode). В режиме симуляции пользователю предоставляется возможность посмотреть, как передается информация между сетевыми устройствами в заданных им ситуациях. В режиме реального времени указывается лишь состояние сетевых устройств, результаты передачи отображаются «по факту».

6. Панель выбора группы сетевых устройств, оконечных станций линий связи.

7. Панель, содержащая конкретные типы сетевых устройств (маршрутизаторов, коммутаторов, концентраторов), оконечных устройств и линий связи. Содержимое этой панели зависит

от выбранной группы устройств в пункте выше. Выбрав необходимое устройство его можно «перетащить» в рабочую область или щелчком мышки указать место в рабочей области, куда следует его поместить. Для соединения сетевых устройств необходимо выбрать требуемый тип кабеля (или выбрать «автоматическое определение»), указать начальное устройство, выбрать один из его сетевых портов. В случае выбора

«автоматическое определение», порт и тип кабеля будут выбираться автоматически (номер порта будет выбираться в порядке возрастания).

8. Панель создания пользовательских сценариев.
9. Рабочее пространство.

Конфигурация сетевого устройства производится по двойному щелчку на нем (см. рис. 1.2). В открывшемся окне пользователь может включить/отключить устройство (соответствующим тумблером на его изображении в области «Physical Device View»), изменить аппаратурную конфигурацию добавив или удалив модули, используя область MODULES, изменить картинку для отображения этого устройства в режиме логической сети и в режиме физической сети. Выбрав вкладку «Config» пользователь может задать некоторые конфигурационные параметры (например, настроить сетевой интерфейс, определить имя устройства и т.п.). На вкладке «CLI» предоставляется доступ к командному интерфейсу устройства (если он предусмотрен).

Для оконечных устройств реализованы дополнительные вкладки (рис. 1.2). На вкладке «Desktop» расположены эмуляторы работы некоторых утилит рабочего стола (командная строка, интернет-браузер и т.п.). «Software/Services» – конфигурирование программного обеспечения, которое должно быть установлено на реально действующем оконечном устройстве.

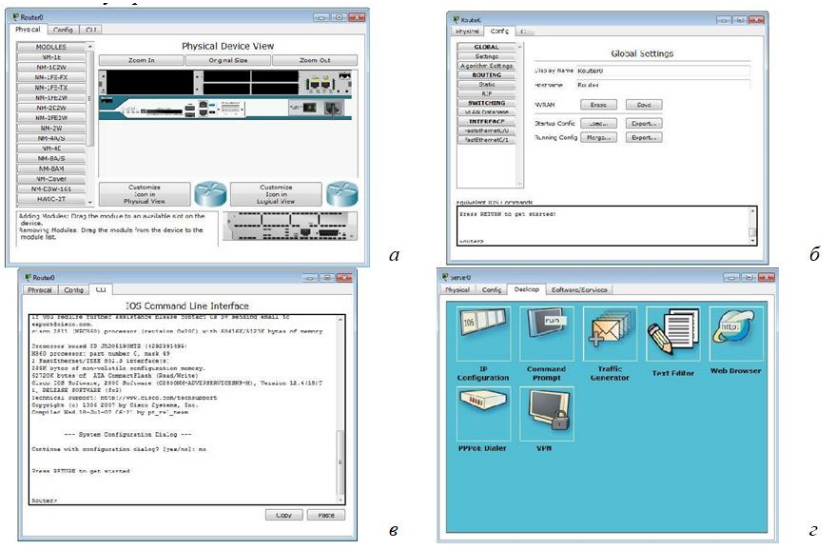



Рисунок 1.2 – Окна конфигурирования сетевого

Наведя курсор мышки на объект и подождав несколько секунд пользователь получит краткую информацию о состоянии объекта. Более подробную информацию пользователь

может получить воспользовавшись инструментом «Inspect». Следует отметить, что всплывающая подсказка при наведении мыши соответствует пункту меню «Port Status Summary Table» инструмента «Inspect» (рис. 1.3).

| Port | Link | VLAN | IP Address | MAC Address |
|---|---|---|---|---|
| FastEthernet0/1 | Up | 1 | -- | 0005.5E8C.8E01 |
| FastEthernet0/2 | Up | 1 | -- | 0005.5E8C.8E02 |
| FastEthernet0/3 | Up | 1 | -- | 0005.5E8C.8E03 |
| FastEthernet0/4 | Up | 1 | -- | 0005.5E8C.8E04 |
| FastEthernet0/5 | Down | 1 | -- | 0005.5E8C.8E05 |
| FastEthernet0/6 | Down | 1 | -- | 0005.5E8C.8E06 |
| FastEthernet0/7 | Down | 1 | -- | 0005.5E8C.8E07 |
| FastEthernet0/8 | Down | 1 | -- | 0005.5E8C.8E08 |
| FastEthernet0/9 | Down | 1 | -- | 0005.5E8C.8E09 |
| FastEthernet0/10 | Down | 1 | -- | 0005.5E8C.8E0A |
| FastEthernet0/11 | Down | 1 | -- | 0005.5E8C.8E0B |
| FastEthernet0/12 | Down | 1 | -- | 0005.5E8C.8E0C |
| FastEthernet0/13 | Down | 1 | -- | 0005.5E8C.8E0D |
| FastEthernet0/14 | Down | 1 | -- | 0005.5E8C.8E0E |
| FastEthernet0/15 | Down | 1 | -- | 0005.5E8C.8E0F |
| FastEthernet0/16 | Down | 1 | -- | 0005.5E8C.8E10 |
| FastEthernet0/17 | Down | 1 | -- | 0005.5E8C.8E11 |
| FastEthernet0/18 | Down | 1 | -- | 0005.5E8C.8E12 |
| FastEthernet0/19 | Down | 1 | -- | 0005.5E8C.8E13 |
| FastEthernet0/20 | Down | 1 | -- | 0005.5E8C.8E14 |
| FastEthernet0/21 | Down | 1 | -- | 0005.5E8C.8E15 |
| FastEthernet0/22 | Down | 1 | -- | 0005.5E8C.8E16 |
| FastEthernet0/23 | Down | 1 | -- | 0005.5E8C.8E17 |
| FastEthernet0/24 | Down | 1 | -- | 0005.5E8C.8E18 |
| GigabitEthernet0/1 | Down | 1 | -- | 0005.5E8C.8E19 |
| GigabitEthernet0/2 | Down | 1 | -- | 0005.5E8C.8E1A |
| Vlan1 | Down | 1 | <not set> | 0003.E4E4.ADE6 |

Hostname: Switch

Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet

Рисунок 1.3 – Всплывающая «подсказка»

Отладка исследуемой сети может производиться двумя способами: имитируя деятельность пользователя с реальным оборудованием и с применением средств моделирования. В первом случае пользователь среды может выполнять необходимые действия над сетевыми объектами и принимать решения о функциональности собранной им сети. Во втором случае используются встроенные средства среды имитационного моделирования, которые позволяют пошагового наглядно продемонстрировать этапы передачи информации по сети. Анализируемые задания по передачи данных по сети объединяются в сценарий. В среде допускает создавать несколько сценариев и переключаться между ними для анализа работы сети.

Для создания задания по передаче данных по протоколу ICPM (ping) используется кнопка «Add Simple PDU». Пользователь задает начальный сетевой узел (который будет генерировать данные) и конечный сетевой узел. В результате автоматически создается одно задание в текущем сценарии. Для формирования передач данных по сети с указанием параметров передаваемой информации (протокол, порт

и т.п.) используется кнопка «Add Complex PDU». Нажав на соответствующую кнопку в вертикальной панели пользователь должен указать протокол передачи, источник передаваемой информации и задать параметры: сетевой порт через который данные будут передаваться, адрес источника и получателя, порт получателя и отправителя, время жизни и обслуживания, номер пакета в последовательности, размер пакета, а также определить будет ли эта передача носить разовый характер или повторяться в течение некоторого периода времени (рис. 1.4).

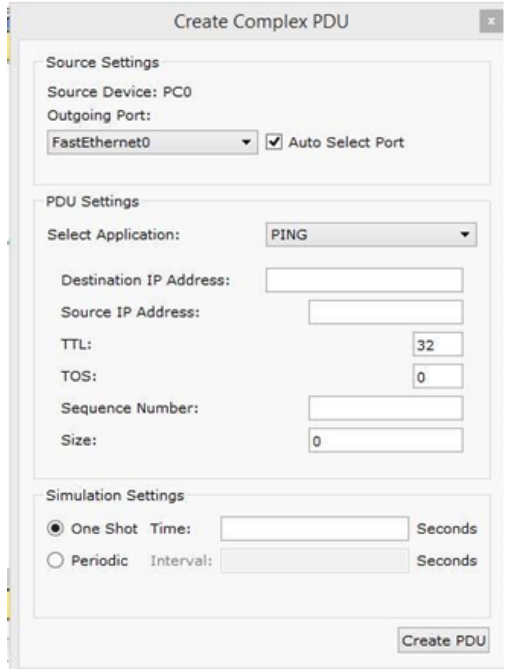



Рисунок 1.4 – Окно настроек параметров передачи информации по сети

Результаты выполнения заданий по передаче данных отображаются в области сценариев. В режиме реального времени результаты выполнения заданий выводятся сразу же по окончании симуляции. В случае, если пользователь попытается указать устройство (источник или приемник), не имеющего настроенного сетевого интерфейса, то сразу будет выдано сообщение об ошибке (рис. 1.5).

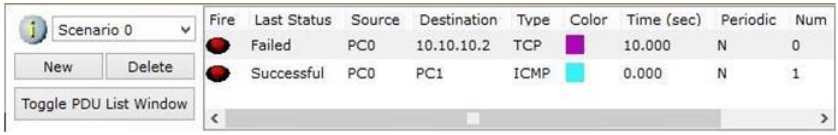



Рисунок 2.5 – Пример результатов выполнения сценария передачи данных (в реальном времени)

Переключившись в режим симуляции пользователь получает возможность наглядно посмотреть каким образом передаются данные по сети. Переход к следующему шагу производится нажатием на кнопку «Capture / Forward». Перейти к предыдущему шагу можно нажав на клавишу «Back». Нажав на кнопку «Auto Capture / Play» запускается автоматический переход к следующему шагу (время перехода указывается в области настроек (рис. 1.6). Кнопка «Reset Simulation» – сбрасывает исследуемую сеть в исходное состояние. Также в панели настроек можно указать дополнительные фильтры на вывод информации о передаче данных по сети (указать интересующие протоколы).

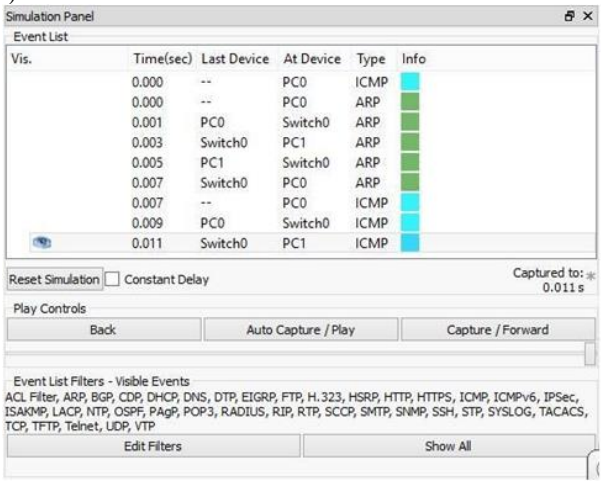



Рисунок 1.6 – Панель настроек пошагового моделирования

Большинство сетевых устройств компании CISCO допускают конфигурирование. Для этого пользователь сети должен подключиться к устройству используя: прямое кабельное (консольное) подключение, удалённое терминальное подключение или Web- интерфейс. Задавая параметры устройства, пользователь сети определяет его поведение и настраивает порядок его работы.

Подключившись к устройству напрямую или через удалённый терминал пользователю предлагается командная строка (Command Line Interface – CLI), в которой он может приступить к его конфигурированию (рис. 1.7). Интерфейс командной строки для устройств доступен в окне настроек параметров сетевого устройства на вкладке

«CLI». Оно имитирует прямое кабельное (консольное) подключение к сетевому устройству. Создав новое устройство в этом окне можно наблюдать процесс его загрузки (сервисные сообщения).

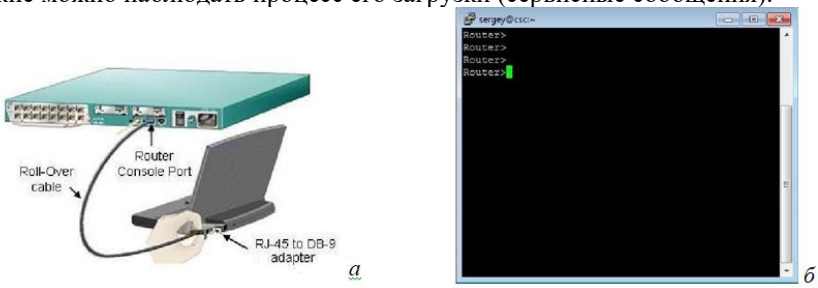



Рисунок 1.7 – Пример подключения к сетевому устройству

Командная строка представляет собой место, куда пользователь вводит символы, формирующие управляющее воздействие. Это место обозначается: приглашением и следующим за ним курсором (который может мигать). Приглашение командной строки обычно содержит имя сетевого узла и один (или несколько) специальных символов, отвечающих за подсказку пользователю, в каком режиме сейчас находится командная строка или в какой части конфигурационных параметров сейчас будут производиться действия. Ввод команд завершается нажатием клавиши <ENTER>. Команда начинает интерпретироваться (исполняться) после нажатия клавиши <ENTER>. Если команда написана правильно, то будет выполнено соответствующее действие. Иначе появится сообщение об ошибке, указывающее на некорректное место в командной строке.

Пользователь может набрать несколько букв в командной строке и нажать клавишу <TAB>. В этом случае команда или её параметр будет продолжен (если набранная последовательность однозначно определяет их) или не произойдет никаких действий. Проверить почему команда или параметр не были продолжены можно с помощью контекстной помощи. Набрав ?, пользователю будут показаны возможные альтернативы. Для отмены действия, выполненного какой-либо

командой, необходимо выполнить её ещё раз указав перед ней команду no.

В случае, если в результате выполнения команды выводится информация, не помещающаяся в одном окне, то в нижней строке выводится фраза –More–. Построчная прокрутка текста осуществляется клавишей <Enter>. Постраничная прокрутка – клавише <Пробел>.

Работа с командной строкой осуществляется в нескольких режимах (табл. 2.1). Едиными для всех устройств режимами являются: пользовательский, привилегированный и глобальной конфигурации. Остальные режимы зависят от типа устройства и его внутренней организации.

Таблица 2.1 – Режимы командного интерфейса

| **Режим** | **Переход в режим** | **Вид командной строки** | **Выход из режима** |
|---|---|---|---|
| Пользовательский (User EXEC) | Подключение | Router> | logout |
| Привилегированный (Privileged EXEC) | enable | Router# | disable |
| Глобальная конфигурация | configure terminal | Router(config)# | exit, end или Ctrl-Z |
| Настройка интерфейсов | Interface | Router(config-if) | exit |

Подключившись к устройству командная строка, находится в пользовательском режиме. В этом режиме доступны команды, позволяющие посмотреть некоторую (открытую) часть текущей конфигурации сетевого устройства, запустить процесс проверки работоспособности сети (команды ping и traceroute), открыть терминальную сессию для подключения к другому сетевому устройству и т.п.

В привилегированном режиме пользователю доступно больше информации обо всей конфигурации сетевого устройства, а также предоставляется доступ к команде перехода в режим конфигурирования (изменения конфигурационной информации).

Внутри командной строки имеется встроенная контекстная документация (подсказка или помощь), выводимая командной help или ?. Если пользователь знает начальные символы команды, но не помнит её продолжение, или не уверен какие параметры следует указать команде, то следует указать в нужном месте командной строки знак ? и

тогда выведется информация о соответствующих командах или параметрах.

В качестве примеров настройки устройства приведем команды изменения имени устройства и определения сообщения, выдаваемого пользователю при подключении (вход в пользовательский режим).

Для этого необходимо подключиться к устройству, перейти в привилегированный режим, затем в режим глобальной конфигурации. Команда для изменения имени – hostname, для определения приветственного сообщения – banner. Далее приведен пример настройки имени устройства и приветственного сообщения.

```
Router>enable
Router#configure terminal
Router(config)#hostname MAIN
MAIN(config)#banner motd /
Enter TEXT message. End with the character '/'.
TUSUR /MAIN (config)#no hostname
Router (config)#
```

Все сетевые устройства имеют одно или несколько подключений к

телекоммуникационной сети – сетевых интерфейса. Каждый сетевой интерфейс (или кратко – интерфейс) имеет свои тип, определяющий способ подключения к нему (например, Ethernet, FastEthernet, Serial и т.п.) и уникальный номер. Номер интерфейса, обычно, имеет вид: номер контроллера/номер интерфейса внутри контроллера. Например, запись Ethernet 0/1 означает интерфейс с типом подключения Ethernet, расположенные на контроллере с номером 0 и имеющий на нем порядковый номер 1.

Для конфигурирования сетевого интерфейса необходимо в режиме глобальной конфигурации ввести команду interface с указанием его типа и номера. Вернуться в режим глобальной конфигурации можно командой exit. Каждый интерфейс в зависимости от своего типа имеет ряд настроек. Для всех интерфейсов присутствует две настройки: описание и состояние (включен или нет). Первая настройка задается командой description, вторая – shutdown. Далее приведен пример задания описания и включения интерфейса fastEthernet 0/1.

```
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#description Connect to main office
Switch(config-if)#no shutdown
Swtich(config-if)#exit
Switch(config)#
```

Если пользователю необходимо произвести одинаковую настройку для нескольких однотипных интерфейсов, то он может, указав в команде interface диапазон конфигурируемых интерфейсов (параметр range). Диапазон задается следующим образом. Указывается тип интерфейсов, а в номере указывается диапазон. Например, запись range fastEthernet 0/1-4 означает, что будут задаваться параметры для интерфейсов 0/1, 0/2, 0/3 и 0/4 с типом fastEthernet.

```
Switch(config)#interface range fastEthernet 0/1-4
Switch(config-if-range)#description Connect to main office
Switch(config-if-range)#no shutdown
Swtich(config-if-range)#exit
Switch(config)#
```

Посмотреть текущие настройки сетевого интерфейса можно в привилегированном

режиме с помощью команды show interfaces и указав его тип и номер. Чтобы посмотреть настройки сразу всех интерфейсов используется команда show interfaces.

Подключившись к устройству пользователь по умолчанию получает полный доступ не вводя никаких авторотационных данных. Очевидно, что такой режим в действующих сетях не приемлем. Задать параметры авторизации можно в режиме глобальной конфигурации с помощью команды line. В качестве параметров команды указывается способ подключения (консоль или удалённый терминал) и номер линии для подключения. Пример настройки пароля для доступа к устройству приведен далее.

```
Switch(config)#line console 0
Switch(config-line)#password qwerty
Switch(config-line)#login
Switch(config-line)#exit
Switch(config)#line vty 0 3
Switch(config-line)#password qwerty
Switch(config-line)#login
Switch(config-line)#transport input telnet
Switch(config-line)#exit
Switch(config)#
```

Конфигурацию оборудования можно стереть, сохранить в отдельный файл и затем

восстановить её из него. Сделать это можно с помощью окна настроек оборудования (вкладка Config). Следует отметить, что конфигурация оборудования изменяется в режиме реального времени.

Перезагрузка устройства приведет к тому, что изменения не будут сохранены. Чтобы изменения сохранились и остались неизменными при перезагрузке устройства, то их надо сохранить в энергонезависимой памяти. Для этого в привилегированном режиме следует выполнить команду copy running-config startup- config или выбрать соответствующие кнопки в окне свойств сетевого объекта.

Посмотреть содержимое текущей конфигурации или конфигурации, сохранённой на диске, можно в привилегированном режиме с помощью команды show running-conf.

При работе с помощью командной строки, все вводимые команды можно сокращать. Главное, чтобы сокращение однозначно указывало на команду. Например, show running-config сокращается до sh run, configure terminal можно сократить до conf t, enable до en, exit до ex и тд. По нажатию Tab сокращенная команда дописывается до полной (данное действие не обязательно, но приветствуется), а знак вопроса, следующий за командой, выводит список дальнейших возможностей и небольшую справку по ним.

Можно использовать горячие клавиши:

- Ctrl+A – Передвинуть курсор на начало строки.
- Ctrl+E – Передвинуть курсор на конец строки.
- Ctrl+W – Стереть предыдущее слово.
- Ctrl+U – Стереть всю линию.
- Ctrl+C – Выход из режима конфигурирования.
- Ctrl+Z – Применить текущую команду и выйти из режима конфигурирования.
- Ctrl+Shift+6 – Остановка длительных процессов.
- Курсорные Up, Down – Перемещение по истории команд.

### 1.2 Задание для самостоятельной работы

Для выполнения задания необходимо:

1. Сформировать топологию сети, представленную на рис. 2.8.
2. Используя командную строку задать сетевым узлам:

- Уникальные сетевые имена.
- Приветственные приглашения, в которых должна указываться краткая информация о сетевом устройстве.
- Пароли для прямого подключения к устройствам и режим их проверки.

• Для устройств, соединяющих главный и дополнительный офисы, задать описания для соответствующих сетевых интерфейсов.

3. Сохранить настройки сетевых устройств в их энергонезависимой память. Для маршрутизаторов, соединяющих главный и дополнительный офисы, сохранить конфигурацию в отдельные файлы.

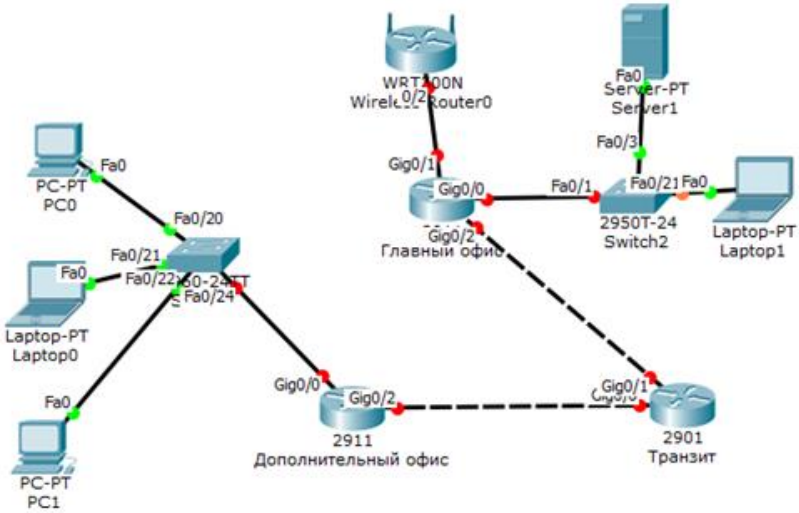



Рисунок 1.8 – Топология сети

## ЛАБОРАТОРНАЯ РАБОТА №3
## Cisco Packet Tracer. Виртуальные локальные сети

### 1. Цель работы

Целью данной работы является изучение работы с VLAN в пакете «Tracer» от Cisco, создание и тестирование собственной VLAN. Будет рассмотрена настройка оборудования CISCO при помощи CLI (англ. Command Line Interface).

### 2. Краткие теоретические сведения

Сетевые технологии лучше всего изучать на практике, посредством подключения устройств к сетям и наблюдения соответствующих процессы. Инновационное средство визуализации и моделирования сетей Cisco Packet Tracer поможет надежно закрепить навыки конфигурирования – результаты вашей работы отображаются непосредственно на экране настольного или мобильного устройства. Packet Tracer поможет вам:

1) закрепить свои навыки при подготовке к собеседованию;

2) подготовиться к сертификационному экзамену;

3) опробовать на практике знания, полученные в ходе учебных курсов;

4) овладев необходимыми навыками, вы сможете приступить к построению карьеры в сфере Интернета вещей.

VLAN (аббр. от англ. Virtual Local Area Network) – логическая («виртуальная») локальная компьютерная сеть, представляет собой группу хостов с общим набором требований, которые взаимодействуют так, как если бы они были подключены к широковещательному домену, независимо от их физического местонахождения. VLAN имеет те же свойства, что и физическая локальная сеть, но позволяет конечным станциям группироваться вместе, даже если они не находятся в одной физической сети. Такая реорганизация может быть сделана на основе программного обеспечения вместо физического перемещения устройств Широковещательный домен – область сети, в которой происходит обмен широковещательными сообщениями и устройства могут отправлять друг другу сообщения непосредственно, без участия маршрутизатора.

### 3. Ход работы

### 3.1. Создание сети

Для выполнения работы необходимо создать два маршрутизатора 1941, два коммутатора 2960 и шесть компьютеров или ноутбуков. Для более удобной настройки переименуйте их как на рис. 1.

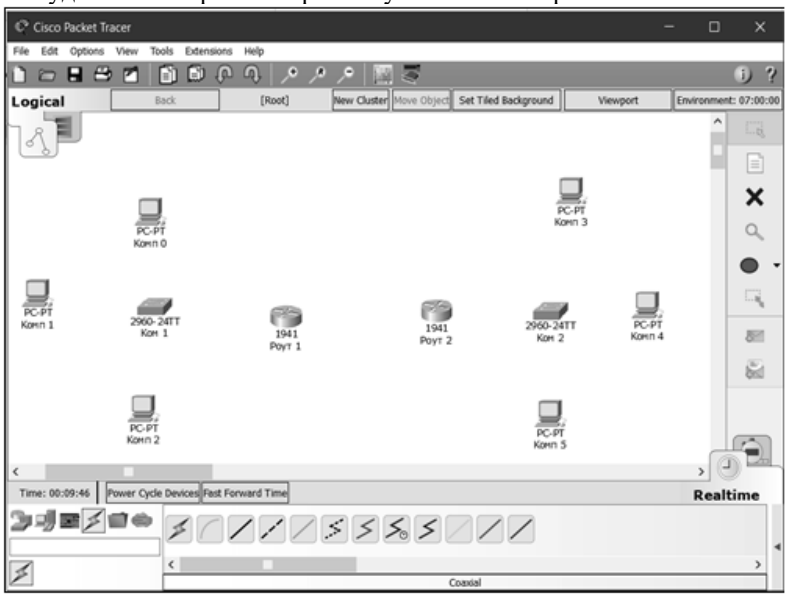



Рисунок 1 – Создание оборудования

Соедините устройства согласно данным табл. 1.

Таблица 1 – Соединение устройств

| Устр.1 | Устр.2 | Тип кабеля | Интерфейс устр.1 | Интерфейс устр. 2 |
|---|---|---|---|---|
| Комп 0 | Ком 1 | Copper Straight-Through | Fa0 | Fa0/1 |
| Комп 1 | Ком 1 | | | Fa0/2 |
| Комп 2 | Ком 1 | | | Fa0/3 |
| Комп 3 | Ком 2 | | | Fa0/1 |
| Комп 4 | Ком 2 | | | Fa0/2 |
| Комп 5 | Ком 2 | | | Fa0/3 |
| Ком 1 | Роут 1 | Copper Cross-Over | Gig0/1 | Gig0/1 |
| Ком 2 | Роут 2 | | | |
| Роут 1 | Роут 2 | Serial DTE | Se0/0/0 | |

Не забывайте, что для соединения роутеров, в них должен быть установлен модуль HWIC-2T. В итоге получится сеть, как на рис. 2.

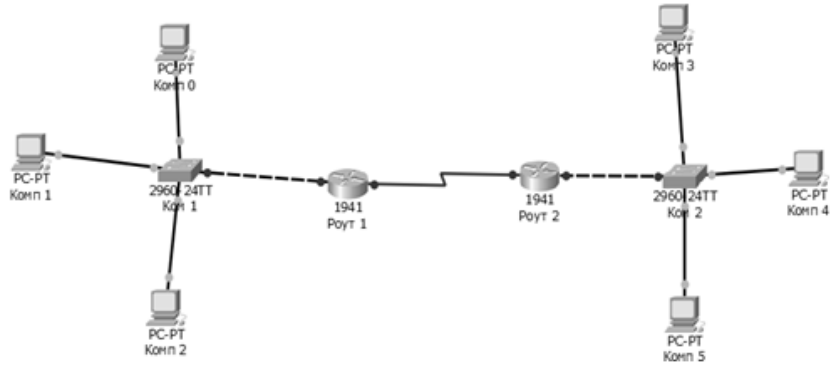



Рис. 2. Соединенные устройства

### 3.2 Настройка устройств

Нужно создать внутри одной сети три виртуальные (VLAN). Виртуальные сети позволяют разделять на группы устройства, подключенные к одному коммутатору, уменьшить широковещательный трафик в сети, увеличить безопасность сети или уменьшить количество сетевого оборудования и так далее. Так как реальное оборудование Cisco настраивается в основном с помощью интерфейса командной строки, то большую часть настройки будем выполнять с её помощью.

Используемые команды:

ena – включить устройство;

conf t – войти в режим настройки устройства; vlan * – создать виртуальную сеть *;

exit – выйти из текущего режима настройки; int * – режим настройки интерфейса *;

switchport mode access – переключить режим порта на статичный доступ;

switchport mode trunk – переключить режим порта на магистральный; switchport access vlan * – переключить порт на виртуальную сеть *; ip address * # – задать текущему интерфейсу адрес * с маской #; no shut – включить интерфейс;

encapsulation dot1Q * – включение инкапсуляции dot1Q для виртуальной сети *.

Настройте коммутатор Ком 1 для работы с виртуальными сетями.

Перейдите во вкладку CLI и введите команды, приведенные на рис. 3.

Таким образом в коммутаторе будут созданы три виртуальные сети. Далее нужно указать, какой интерфейс должен работать с каждой сетью, для этого выполните команды, представленные на рис. 4.

```
Switch>ena
Switch#conf t
Enter configuration commands, one per line.  End with
CNTL/Z.
Switch(config)#vlan 2
Switch(config-vlan)#vlan 3
Switch(config-vlan)#vlan 4
Switch(config-vlan)#exit
Switch(config)#
```

Рис. 3. Создание виртуальных сетей

```
Switch(config)#int Fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
Switch(config)#int Fa0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 3
Switch(config-if)#exit
Switch(config)#int Fa0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 4
Switch(config-if)#exit
Switch(config)#
```

Рис. 4. Настройка интерфейсов

Теперь, когда настроены порты, идущие к ПК, нужно разрешить трафик виртуальных сетей между коммутатором и маршрутизатором (рис. 5).

```
Switch(config)#int Gig0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch(config)#
```

Рис. 5. Переключение режима порта

Если навести мышку на коммутатор, отобразится состояние портов. Состояние портов после проделанных действий представлено на рис. 6.

Настроим маршрутизатор. Для настройки IP-адреса виртуальных интерфейсов для сетей выполните команды, показанные на рис. 7.

Порт для обмена данными с коммутатором настроен, также нужно, чтобы роутер мог обмениваться данными со вторым роутером. Для этого введите команды с рис. 8.


Рис. 6. Состояние портов

```
Router>ena
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int gig0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.248
Router(config-if)#no shut

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up

Router(config-if)#exit
Router(config)#int gig0/0.2
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.2, changed state to
up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0.2, changed state to up

Router(config-subif)#encapsulation dot1Q 2
Router(config-subif)#ip address 192.168.1.9 255.255.255.248
Router(config-subif)#exit
Router(config)#int gig0/0.3
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.3, changed state to
up
```

Рис. 7 (начало)

```
Router(config)#int gig0/0.3
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.3, changed state to
up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0.3, changed state to up

Router(config-subif)#encapsulation dot1Q 3
Router(config-subif)#ip address 192.168.1.17 255.255.255.248
Router(config-subif)#exit
Router(config)#int gig0/0.4
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.4, changed state to
up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0.4, changed state to up

Router(config-subif)#encapsulation dot1Q 4
Router(config-subif)#ip address 192.168.1.25 255.255.255.248
Router(config-subif)#exit
Router(config)#
```

Рис. 7 (окончание). Настройка маршрутизатора

```
Router#conf t
Enter configuration commands, one per line.  End with
CNTL/Z.
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 10.10.10.0
Router(config-router)#network 192.168.1.0
Router(config-router)#exit
Router(config)#int se0/0/0
Router(config-if)#ip address 10.10.10.1 255.0.0.0
Router(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to
down
Router(config-if)#exit
```

Рис. 8. Настройка обмена данными между роутерами

Задайте IP-адреса компьютерам Комп 0, Комп 1, Комп2 в соответствии с табл. 2.

Таблица 2 – Адреса компьютеров

| Компьютер | IP адрес | Mask | Gateway IP |
|---|---|---|---|
| Комп 0 | 192.168.1.10 | 255.255.255.248 | 192.168.1.9 |
| Комп 1 | 192.168.1.18 | | 192.168.1.17 |
| Комп 2 | 192.168.1.26 | | 192.168.1.25 |

Получится сеть как на рис. 9.

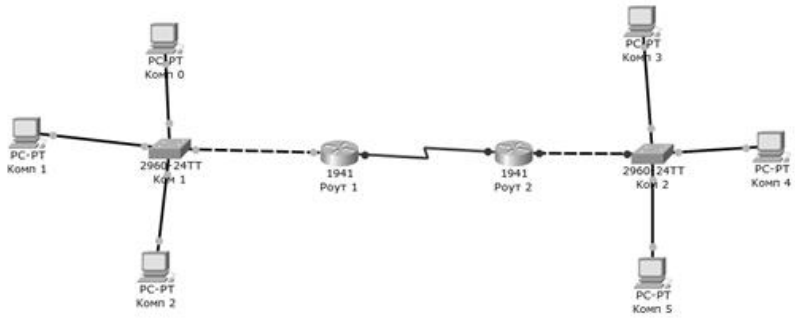



Рис. 9. Рабочая левая часть сети

Чтобы убедиться, что виртуальные сети работают, попробуйте отправить UDP-пакет с Комп 0 на Комп 1 в режиме симуляции. Вы должны увидеть, что пакет идет не напрямую через коммутатор к Комп 1, а через маршрутизатор, т.е. через маршрутизатор идет пересылка дан-

ных в другую сеть. Если бы компьютеры были в одной виртуальной сети, то пакет прошел бы через коммутатор напрямую к цели.

## 4. Задание на лабораторную работу

1. Ознакомиться с теорией.
2. Настроить правую часть сети самостоятельно, чтобы обе части могли через маршрутизаторы обмениваться данными, например, Комп 0 мог успешно отправить данные Комп 5.
3. После настройки подтвердить успешную отправку PDU пакета по сети.

## 5. Контрольные вопросы

1. Что такое VLAN?
2. Зачем используются VLAN?
3. Может ли компьютер, подключенный к VLAN 1, увидеть ком- пьютер, подключенный к VLAN 2, без маршрутизатора?
4. Что такое CLI?
5. Как с помощью CLI можно задать адрес интерфейсу?
6. Зачем настраивают протокол RIP на маршрутизаторе?
7. Для чего используют режим интерфейса «access»?
8. Для чего используют режим интерфейса «trunk»?
9. За счет чего реализуется VLAN в Packet «Tracer»?
10. Как с помощью CLI сделать виртуальный интерфейс?

## ЛАБОРАТОРНАЯ РАБОТА №4
## Сетевые службы

### 1 Краткая теоретическая справка

DNS (Domain Name System – система доменных имен) – компьютерная распределённая система для получения информации о доменах. Чаще всего используется для получения IP-адреса по имени хоста (компьютера или устройства), получения информации о маршрутизации почты, обслуживающих узлах для протоколов в домене.

Распределённая база данных DNS поддерживается с помощью иерархии DNS- серверов, взаимодействующих по определенному протоколу. Основой DNS является представление об иерархической структуре доменного имени и зонах. Каждый сервер, отвечающий за имя, может делегировать ответственность за дальнейшую часть домена другому серверу (с административной точки зрения – другой организации или человеку), что позволяет возложить ответственность за актуальность информации на серверы различных организаций (людей), отвечающих только за «свою» часть доменного имени.

DNS важна для работы Интернета, так как для соединения с узлом необходима информация о его IP-адресе, а для людей проще запоминать буквенные (обычно осмысленные) адреса, чем последовательность цифр IP-адреса. В некоторых случаях это позволяет использовать виртуальные серверы, например HTTP-серверы, различая их по имени запроса. Первоначально преобразование между доменными и IP-адресами производилось с использованием специального текстового файла hosts, который составлялся централизованно и автоматически рассылался на каждую из машин в своей локальной сети. С ростом Сети возникла необходимость в эффективном, автоматизированном механизме, которым и стала DNS.

Ключевыми понятиями DNS являются:

• Домен (domain, область) – узел в дереве имён, вместе со всеми подчинёнными ему узлами (если таковые имеются), то есть именованная ветвь или поддерево в дереве имен. Структура доменного имени отражает порядок следования узлов в иерархии; доменное имя читается слева направо от младших доменов к доменам высшего уровня (в порядке повышения значимости): вверху находится корневой домен (не имеющий идентификатора), ниже идут домены первого уровня (доменные зоны), затем – домены второго уровня, третьего и т. д. (например, для адреса ru.wikipedia.org. домен первого уровня – org, второго wikipedia, третьего ru). На практике точку перед корневым

доменом часто опускают («ru.wikipedia.org»вместо «ru.wikipedia.org.»), но она бывает важна в случаях разделения между относительными доменами и FQDN (англ. Fully Qualifed Domain Name, полностью определённое имя домена).

• Поддомен (subdomain) – подчинённый домен (например, wikipedia.org – поддомен домена org, а ru.wikipedia.org – домена wikipedia.org). Теоретически такое деление может достигать глубины 127 уровней, а каждая метка может содержать до 63 символов, пока общая длина вместе с точками не достигнет 254 символов. Но на практике регистраторы доменных имён используют более строгие ограничения. Например, если у вас есть домен вида mydomain.ru, вы можете создать для него различные поддомены вида mysite1.mydomain.ru,mysite2.mydomain.ru и т. д.

• Ресурсная запись – единица хранения и передачи информации в DNS. Каждая ресурсная запись имеет имя (то есть привязана к определенному Доменному имени, узлу в дереве имен),тип и поле данных, формат и содержание которого зависит от типа.

• Зона – часть дерева доменных имен (включая ресурсные записи), размещаемая как единое целое на некотором сервере доменных имен (DNS-сервере), а чаще – одновременно на нескольких серверах. Целью выделения части дерева в отдельную зону является передача ответственности за соответствующий домен другому лицу или организации. Это называется делегированием. Как связная часть дерева, зона внутри тоже представляет собой дерево. Если рассматривать пространство имен DNS как структуру из зон, а не отдельных узлов/имен, тоже получается дерево; оправданно говорить о родительских и дочерних зонах, о старших и подчиненных. На практике большинство зон 0-го и 1-го уровня ('.', ru, com, …) состоят из единственного узла, которому непосредственно подчиняются дочерние зоны. В больших корпоративных доменах (2-го и более уровней) иногда встречается образование дополнительных подчиненных уровней без выделения их в дочерние зоны.

• DNS-сервер – специализированное ПО для обслуживания DNS, а также компьютер, на котором это ПО выполняется. DNS-сервер может быть ответственным за некоторые зоны и/или может перенаправлять запросы вышестоящим серверам.

• DNS-клиент – специализированная библиотека (или программа) для работы с DNS. В ряде случаев DNS-сервер выступает в роли DNS-клиента.

POP3 (Post Office Protocol Version 3) – почтовый протокол) – стандартный Интернет- протокол прикладного уровня, используемый клиентами электронной почты для извлечения электронного сообщения с удаленного сервера по TCP/IP-соединению. POP и IMAP (Internet Message Access Protocol) – наиболее распространенные Интернет-протоколы для извлечения почты. Практически все современные клиенты и сервера электронной почты поддерживают оба стандарта. Протокол POP был разработан в нескольких версиях, нынешним стандартом является третья версия (POP3). Большинство поставщиков услуг электронной почты также поддерживают IMAP и POP3.

DHCP (Dynamic Host Configuration Protocol – протокол динамической настройки узла) – сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. Данный протокол работает по модели «клиент-сервер». Для автоматической конфигурации компьютер-клиент на этапе конфигурации сетевого устройства обращается к так называемому серверу DHCP и получает от него нужные параметры. Сетевой администратор может задать диапазон адресов, распределяемых сервером среди компьютеров. Это позволяет избежать ручной настройки компьютеров сети и уменьшает количество ошибок. Протокол DHCP используется в большинстве сетей TCP/IP.

Протокол DHCP предоставляет три способа распределения IP-адресов:

• Ручное распределение. При этом способе сетевой администратор сопоставляет аппаратному адресу (для Ethernet сетей это MAC-адрес) каждого клиентского компьютера определённый IP-адрес. Фактически, данный способ распределения адресов отличается от ручной настройки каждого компьютера лишь тем, что сведения об адресах хранятся централизованно (на сервере DHCP), и потому их проще изменять при необходимости.

• Автоматическое распределение. При данном способе каждому компьютеру на постоянное использование выделяется произвольный свободный IP-адрес из определённого администратором диапазона.

• Динамическое распределение. Этот способ аналогичен автоматическому распределению, за исключением того, что адрес выдаётся компьютеру не на постоянное пользование, а на определённый срок. Это называется арендой адреса. По истечении срока аренды IP-адрес вновь считается свободным, и клиент обязан запросить новый (он, впрочем, может оказаться тем же самым). Кроме того, клиент сам может отказаться от полученного адреса.

HTTP (HyperText Transfer Protocol, протокол передачи гипертекста) –протокол прикладного уровня передачи данных (изначально – в виде гипертекстовых документов в формате HTML, в настоящий момент используется для передачи произвольных данных). Основой HTTP является технология «клиент-сервер», то есть предполагается существование потребителей (клиентов), которые инициируют соединение и посылают запрос, и поставщиков (серверов), которые ожидают соединения для получения запроса, производят необходимые действия и возвращают обратно сообщение с результатом.

HTTP в настоящее время повсеместно используется в Интернете для получения информации с веб-сайтов. Основным объектом манипуляции в HTTP является ресурс, на который указывает URI (Uniform Resource Identifier) в запросе клиента. Обычно такими ресурсами являются хранящиеся на сервере файлы, но ими могут быть логические объекты или что-то абстрактное. Особенностью протокола HTTP является возможность указать в запросе и ответе способ представления одного и того же ресурса по различным параметрам: формату, кодировке, языку и т.д. (В частности для этого используется HTTP- заголовок.) Именно благодаря возможности указания способа кодирования сообщения клиент и сервер могут обмениваться двоичными данными, хотя данный протокол является текстовым.

Обмен сообщениями при использовании HTTP идёт по обыкновенной схеме

«запрос-ответ». Для идентификации ресурсов HTTP использует глобальные URI. В отличие от многих других протоколов, HTTP не сохраняет своего состояния. Это означает отсутствие сохранения промежуточного состояния между парами «запрос-ответ». Компоненты, использующие HTTP, могут самостоятельно осуществлять сохранение информации о состоянии, связанной с последними запросами и ответами (например, «куки» на стороне клиента, «сессии» на стороне сервера). Браузер, посылающий запросы, может отслеживать задержки ответов. Сервер может хранить IP-адреса и заголовки запросов последних клиентов. Однако сам протокол не осведомлён о предыдущих запросах и ответах, в нём не предусмотрена внутренняя поддержка состояния, к нему не предъявляются такие требования.

FTP (File Transfer Protocol – протокол передачи файлов) – стандартный протокол, предназначенный для передачи файлов по TCP-сетям (например, Интернет). FTP часто используется для загрузки сетевых страниц. FTP является одним из старейших прикладных протоколов, появившимся задолго до HTTP, в 1971 году. Он и сегодня

широко используется для распространения ПО и доступа к удалённым хостам. Протокол построен на архитектуре «клиент-сервер» и использует разные сетевые соединения для передачи команд и данных между клиентом и сервером. Пользователи FTP могут пройти аутентификацию, передавая логин и пароль открытым текстом, или же, если это разрешено на сервере, они могут подключиться анонимно. Можно использовать протокол SSH для безопасной передачи, скрывающей (шифрующей) логин и пароль, а также шифрующей содержимое.

Симулятор CPT позволяет проводить настройку таких сетевых сервисов, как: HTTP, DHCP, DNS, POP3, FTP и др. в составе сервера сети. Данная работа посвящена изучению некоторых из них.

## 2 Последовательность выполнения работы

Создайте следующую схему сети, представленную на рис. 2.1.

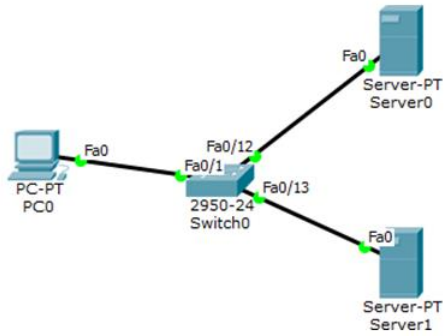



Рисунок 2.1 – Топология сети

Необходимо настроить сеть следующим образом:

1. Server0 – DNS- и Web-сервер;
2. Server1 – DHCP сервер;
3. Компьютер PC0 получает параметры протокола TCP/IP с DHCP сервера и открывает сайт www.emc.ru на Server0.

Первоначально необходимо задать параметры протокола TCP/IP на PC0 и серверах. Для этого нужно настроить интерфейс PC0, установив режим получения IP-адреса через DHCP сервер (рис. 5.2). Затем в конфигурации серверов указать следующие настройки IP:

- Server0: IP адрес – 10.10.10.1, маска подсети – 255.255.255.0.
- Server1: IP адрес – 10.10.10.2, маска подсети – 255.255.255.0.

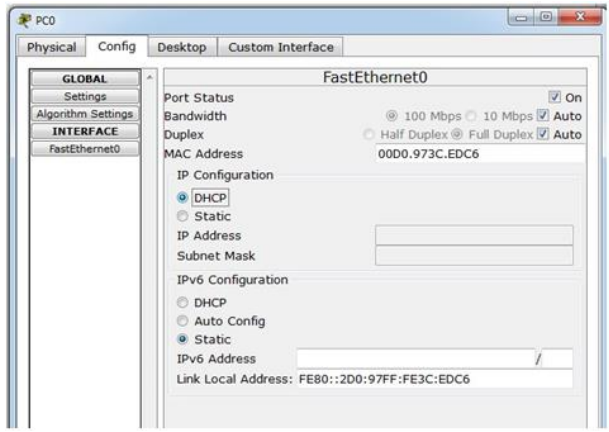



Рисунок 2.2 – Настройка режима получения IP-адреса на интерфейсе PC0

Далее необходимо настроить службу DNS на Server0. Для этого в конфигурации Server0 необходимо перейти на вкладку Services, выбрать DNS и создать запить типа A Record, тем самым связав доменное имя с IP-адресом рис. 5.3 (для добавления записи нажать кнопку ADD);

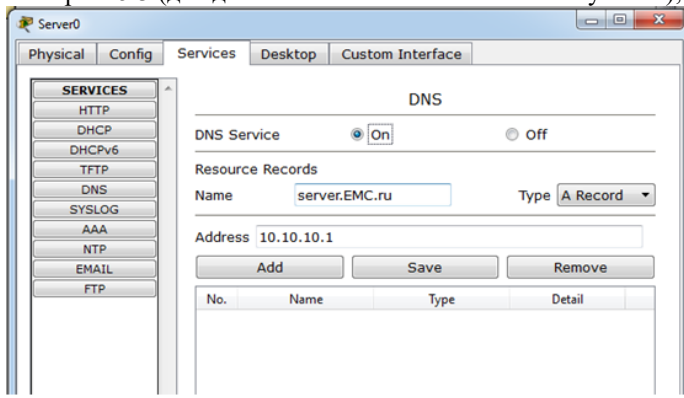



Рисунок 2.3 – Ввод ресурсной записи типа A Record

• в ресурсной записи типа CNAME (позволяет присваивать хосту мнемонические имена или псевдонимы, используемые для связывания с хостом какой-либо функции, либо просто для сокращения имени) связать псевдоним сайта с компьютером (рис. 2.4)

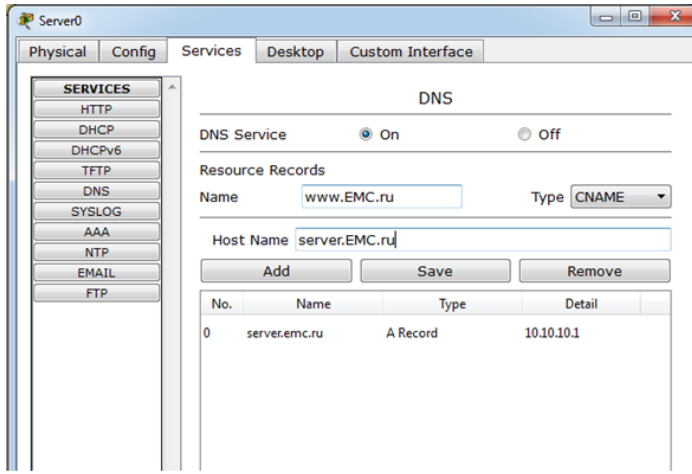



Рисунок 2.4 – Ввод ресурсной записи типа CNAME.

Далее в конфигурации Server0 необходимо перейти на вкладку HTTP и задать настройки стартовой страницы сайта www.EMC.ru (рис. 2.5):

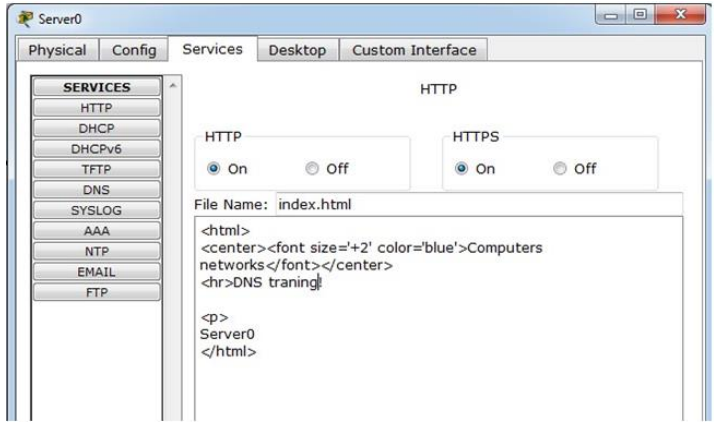



Рисунок 2.5 – Стартовая страница сайта www.emc.ru

Далее необходимо настроить DHCP службу на Server1. Для этого перейдя на вкладку Services выбрать раздел DHCP и сделать соответствующие настройки (рис. 2.6).

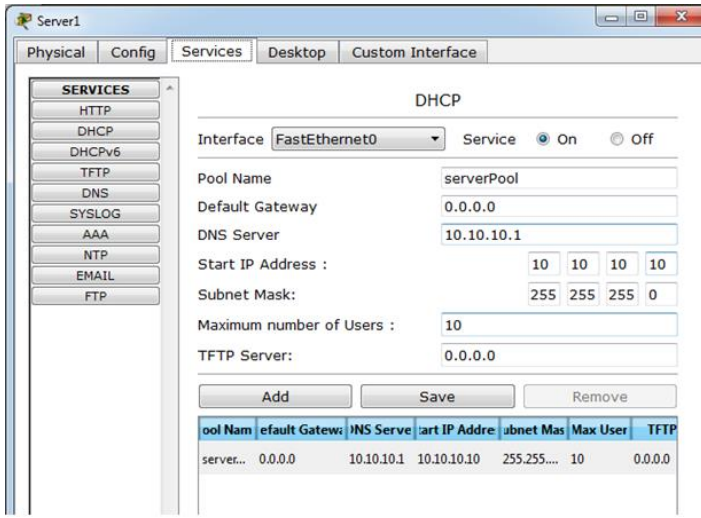



Рисунок 2.6 – Настройка DHCP сервера

После этого необходимо проверить работу клиента. Для этого необходимо войти в конфигурацию хоста PC0 и с помощью командной строки сконфигурировать работу стека протоколов TCP/IP. Так, командой PC>ipconfig /release сбросить старые параметры IP- адреса, и затем командой: PC>ipconfig /renew получить новые параметры настройки с DHCP сервера (рис. 2.7):

```
Packet Tracer PC Command Line 1.0
PC>ipconfig /release

   IP Address......................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: 0.0.0.0
   DNS Server......................: 0.0.0.0

PC>ipconfig /renew

   IP Address......................: 10.10.10.11
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: 0.0.0.0
   DNS Server......................: 10.10.10.1

PC>
```

Рисунок 2.7 – Конфигурация протокол TCP/IP клиента хоста PC0

Далее выбрав Web Browser проверить доступность сайта www.emc.ru (рис. 2.8).

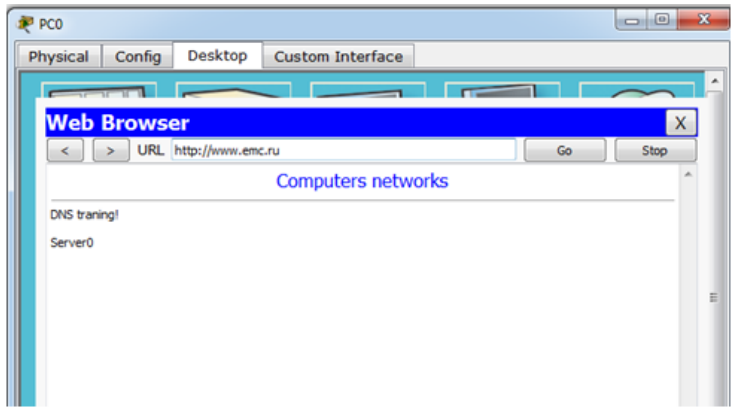



Рисунок 2.8 – Проверка доступности сайта www.emc.ru

Далее рассмотрим особенности настройки почтовых служб, для этого добавив еще один хост– ноутбук. На Server0 к службам DNS и Web добавится еще и почтовая EMAIL служба (рис. 2.9).

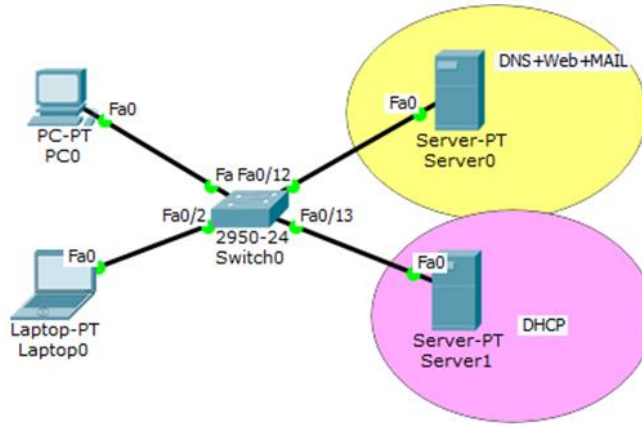



Рисунок 2.9 – Топология сети с двумя серверами и двумя хостами

Первоначально предпочтительнее настроить сервер, указав доменное имя и создав требуемое количество пользователей, в данном случае, двоих, PC и Laptop (рис. 2.10).

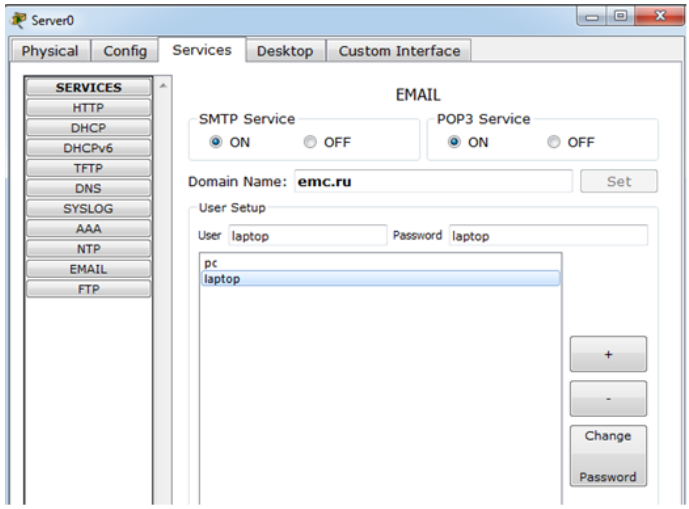
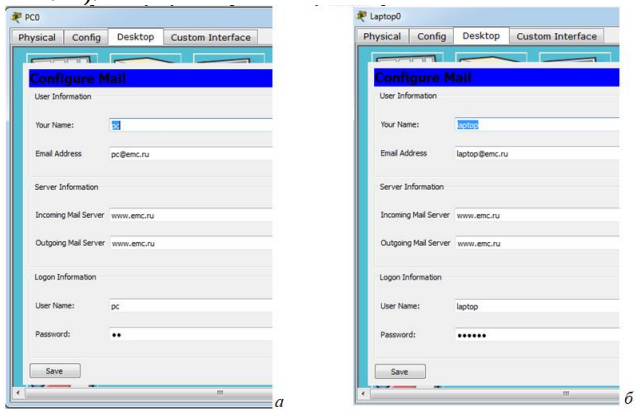



Рисунок 2.10 – Настройки почтовой службы на сервере

Поскольку сеть функционирует, на хостах необходимо только настроить почтовый ящик компьютера и ноутбука, открыв вкладку Email (рис. 2.11).




*а* *б*

Рисунок 2.11 – Настройка почтового ящика компьютера (а) и ноутбука (б)

Правильность настроек можно проверить следующим образом: необходимо в Mail Browser нажать Receive и проконтролировать

появление записи об успешном получении (Receive Mail Success), в нижней части окна. Далее можно создавать, отвечать и получать письма с использованием соответствующих кнопок (рис. 2.12).

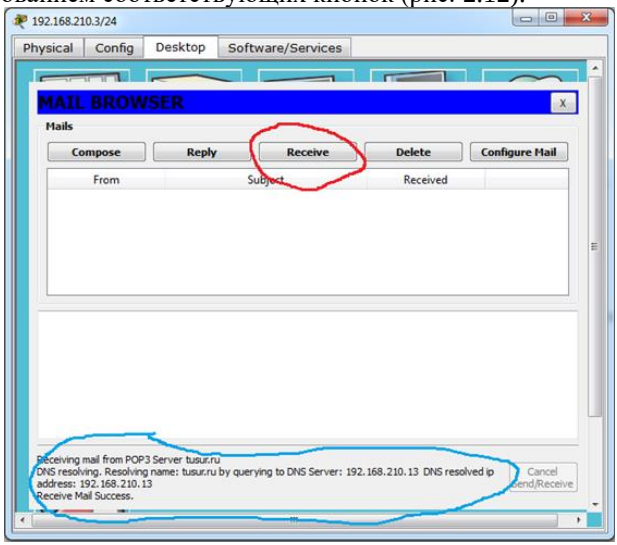



Рисунок 2.12 – Проверка корректности настроек

Когда не совпадают пароли, т.е. в настройках пользователя на PC задан один, а на сервере другой, то при попытке получить ответ от сервера будет получено сообщение об ошибке (рис. 2.13).

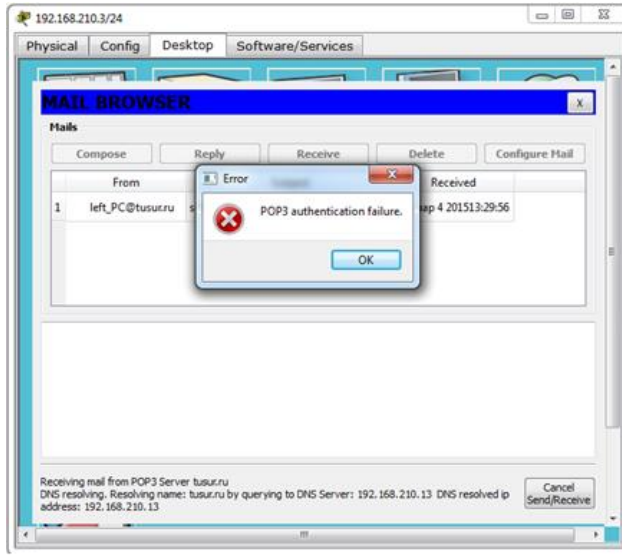



Рисунок 2.13 – Ошибка, возникающая при несовпадении паролей пользователя

### 2.3 Задание для самостоятельной работы

В качестве задания для самостоятельного работы сформировать и настроить сеть (с двумя серверами: DNS и почтовый), представленную на рис. 2.14.

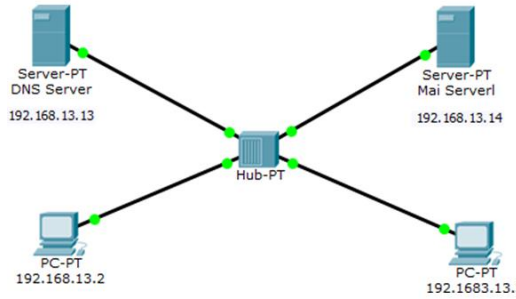



Рисунок 2.14 – Топология сети

Требуется помимо настройки сетевых устройств и служб изменить заглавную страницу «созданного» в ходе работы сайта,

применив знания HTML кодов (в случае возникновения трудностей можно воспользоваться текстом).

```
[1] <HTML>
<head>
<style>
p { text-indent:30px; }
</style>
</head>
<BODY>
<H2 align=center><I> Electromagnetic compatibility (EMC), </I></H2>
<br>
<font face="Academy" color="Red">
is the branch of electrical sciences which studies the unintentional generation, propagation and reception of electromagnetic
energy with reference to the unwanted effects that such energy may induce.
</font>
<p> In order to achieve this, EMC pursues two different kinds of issues. Emission issues are related to the unwanted generation
of electromagnetic energy by some source, and to the countermeasures which should be taken in order to reduce such generation
and to avoid the escape of any remaining energies into the external environment.</p>
<p>
<FONT SIZE=-1 COLOR=FF00FF>
Interference mitigation and hence electromagnetic compatibility is achieved by addressing both emission and susceptibility
issues, i.e., quieting the sources of interference and hardening the potential victims.
</FONT>
</p>
</HTML>
</BODY>
```

## ЛАБОРАТОРНАЯ РАБОТА №5
## Принцип работы коммутатора

### 1 Краткая теоретическая справка

Сетевой коммутатор или свитч (switch) – устройство, предназначенное для соединения нескольких узлов компьютерной сети в пределах одного сегмента. В отличие от концентратора, который распространяет трафик от одного подключенного устройства ко всем остальным, коммутатор передает данные только непосредственно получателю. Это повышает производительность и безопасность сети, избавляя остальные сегменты сети от необходимости (и возможности) обрабатывать данные, которые им не предназначались. Коммутатор работает на канальном уровне модели OSI (именно поэтому их иногда называют коммутаторами L2 уровня), и потому в общем случае может только объединять узлы одной сети по их MAC-адресам. Для соединения нескольких сетей на основе сетевого уровня служат маршрутизаторы.

Коммутатор хранит в памяти специальную таблицу (таблицу коммутации или MAC- таблицу), в которой указывается соответствие MAC-адреса узла порту коммутатора. При его включении эта таблица пуста, и он работает в режиме обучения. При этом поступающие на его порты данные передаются на все остальные порты коммутатора, кроме того порта через который они получены. В тоже время коммутатор анализирует данных, определяя MAC-адрес отправителя, и помещает его в таблицу коммутации. Далее, если на один из его портов поступят пакеты, предназначенные для этого узла, они будут отправлены только через соответствующий порт. Если MAC-адрес получателя еще не известен, то пакет будет продублирован на все интерфейсы с помощью ARP-запросов. Со временем коммутатор сформирует «итоговую» таблицу, и в результате трафик локализуется.

Коммутаторы подразделяются на управляемые и неуправляемые. Более сложные коммутаторы позволяют управлять коммутацией на канальном (втором) и сетевом (третьем) уровне модели OSI (поэтому иногда их называют коммутаторами L3 уровня). Многие управляемые коммутаторы реализуют дополнительные функции: VLAN, QoS, агрегирование, и пр. Сложные коммутаторы можно объединять в одно логическое устройство – стек, с целью увеличения числа портов (например, можно объединить 2 коммутатора с 48 портами каждый и получить логический коммутатор с 96 портами).

### 6.2 Последовательность выполнения работы

Сформируем небольшую сеть, состоящею из стационарного компьютера, ноутбука и коммутатора (2950-24), рис. 2.1. Первоначально ARP-таблицы пусты (также пуста и таблица коммутации коммутатора (MAC Table)). На хостах это можно проверить командой arp -a.

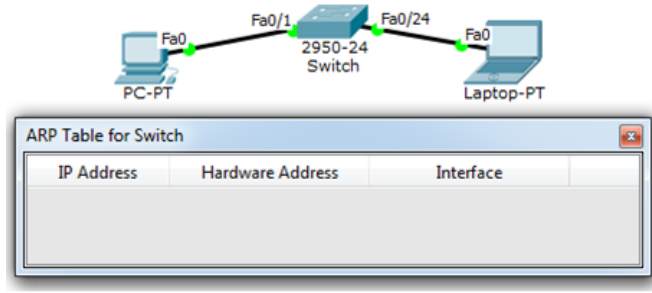



Рисунок 2.1 – Схема сети

Определим MAC-адреса хостов, с помощью команд ipconfig /all. Для стационарного компьютера (PC-PT) в рассматриваемом примере результат приведен на рис. 2.2.

```
PC>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address.....: 0090.0C1E.ECBD
   Link-local IPv6 Address.....: FE80::290:CFF:FE1E:ECBD
   IP Address.....: 10.10.10.2
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: 0.0.0.0
   DNS Servers.....: 0.0.0.0
   DHCP Servers.....: 0.0.0.0
   DHCPv6 Client DUID.....: 00-01-00-01-19-74-7A-53-00-90-0C-1E-EC-BD
```

Рисунок 2.2 – Результат выполнения команды ipconfig /all

Для наглядности дальнейшего изложения нанести на схему дополнительную информацию, рис. 2.3.

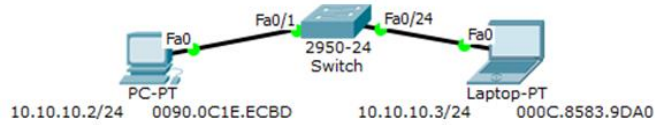



Рисунок 2.3 – MAC-адресация

Далее необходимо проверить связь между стационарным ПК и ноутбуком с помощью утилиты ping. Тогда в IP-заголовке в поле протокола указывается значение 0x1 соответствующее ICMP (согласно RFC790), рис. 2.4.

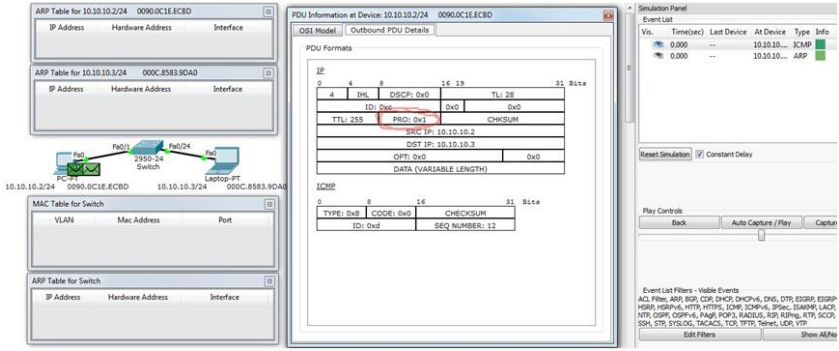


Рисунок 2.4 – IP-заголовок

Поскольку утилита ping использует эхо-запросы протокола ICMP, то после генерации трафика происходит сопоставление IP-адреса назначения (10.10.10.3) с данными таблицы коммутации. Т.к. таблица пуста, генерируется ARP пакет (запрос), в заголовке которого поле Target MAC содержит адрес 0000.0000.0000.0000. В тоже время, в поле адреса назначения Ethernet-кадра заносится широковещательный MAC-адрес FFFF.FFFF.FFFF (рис. 2.5).

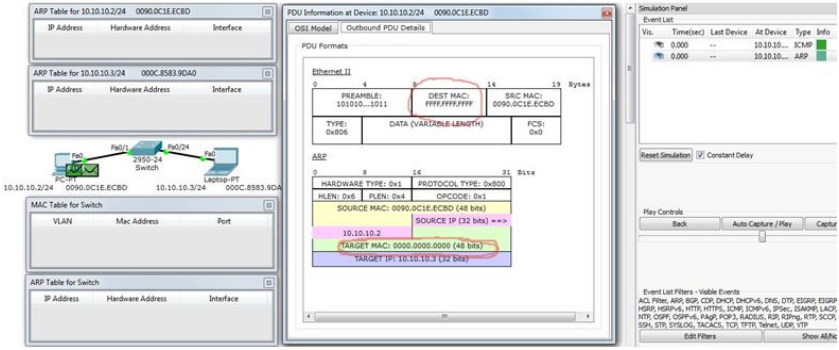


Рисунок 2.5 – Ethernet-кадр

Получив кадр с адресом FFFF.FFFF.FFFF в поле адреса назначения, коммутатор переправляет его на все активные порты, кроме того порта через который получен кадр, после чего в таблицу коммутации добавляется строка соответствия номера порта коммутатора MAC-адресу стационарного ПК (рис. 2.6).

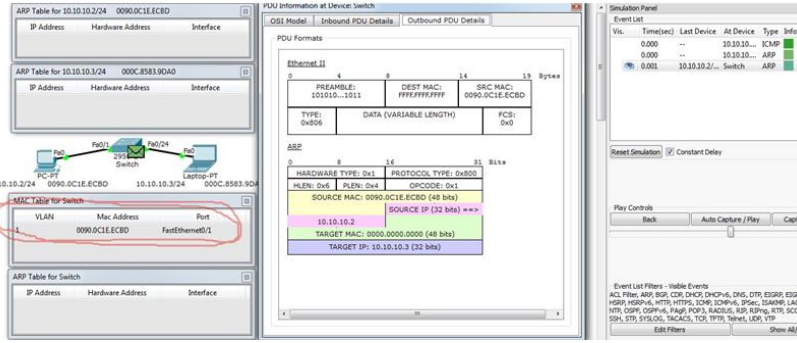


Рисунок 2.6 – Таблица коммутации

После того как ноутбук получит кадр, он выполнит анализ заголовка ARP пакета (рис. 2.7).

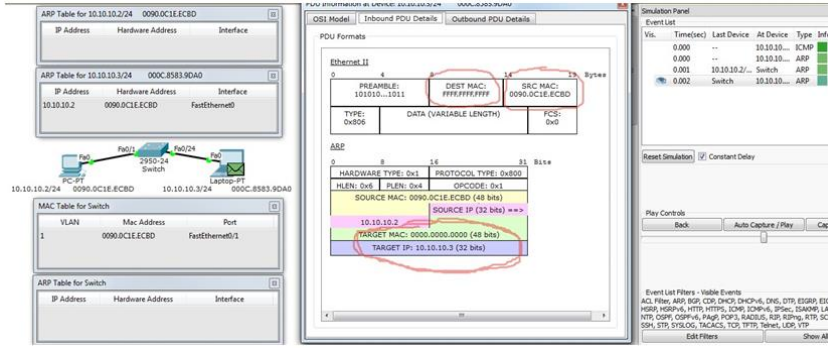


Рисунок 2.7 – Заголовок ARP пакета

Сравнением IP-адреса назначения (поле Target IP) из заголовка и своим собственным, ноутбук «понимает», что запрос предназначен ему и подготовит ARP пакет (ответ). В результате в поле адреса источника Ethernet-кадра будет помещен MAC-адрес его сетевого адаптера, а в поле адреса назначения будет помещен адрес стационарного ПК.

(Аналогично будут заполнены соответствующие поля ARP пакета.) После чего кадр будет отправлен на коммутатор (рис. 2.8).

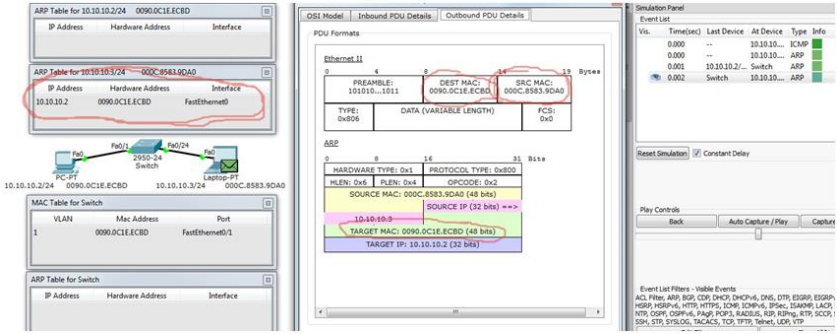



Рисунок 2.8 – Заполнение таблицы коммутации

Получив кадр, коммутатор проанализирует поле адреса назначения (адрес стационарного ПК) в заголовке и сопоставит его со своей таблицей коммутации и, найдя соответствие, переправит кадр через соответствующий порт, а также скорректирует свою таблицу коммутации, добавив в нее информацию о MAC-адресе ноутбука (рис. 2.9).

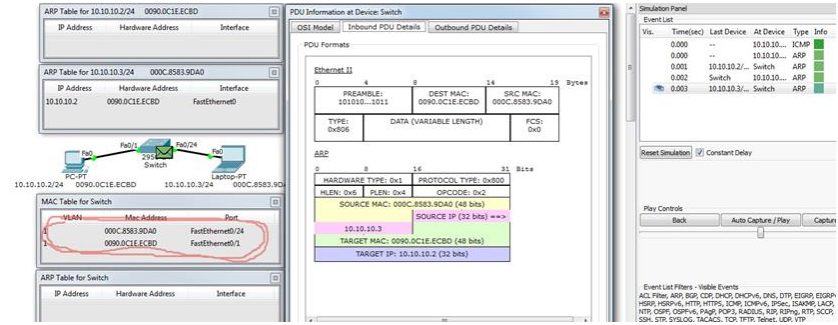



Рисунок 2.9 – Корректировка таблицы коммутации

Получив кадр, стационарный компьютер скорректирует свою ARP-таблицу (рис. 2.10).

В результате следующие ICMP-запросы будет продвигаться по «проложенному пути» без необходимости использования ARP-запросов и «ненужной» широковещательной рассылки кадров по сети.


Рисунок 2.10 – Корректировка ARP-таблицы

### 3.1 Задание для самостоятельной работы

Первоначально необходимо проанализировать работу сети, оценить как будут заполнены таблицы коммутации, а затем проверить с помощью Cisco Packet Tracer. Необходимо рассмотреть две сети (рис. 3.1 и 3.2).

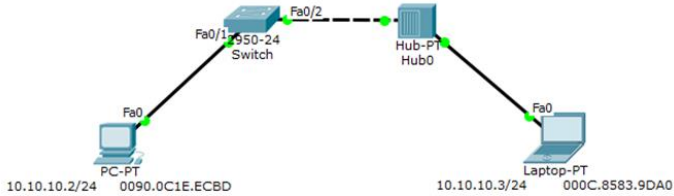



Рисунок 3.1 – Топология первой сети

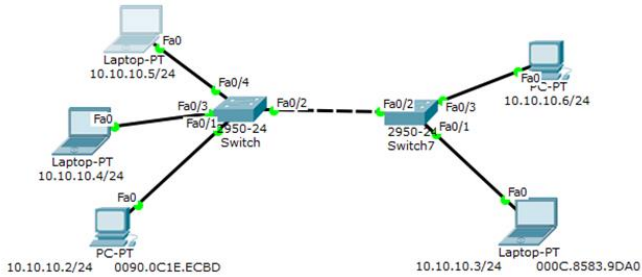



Рисунок 3.2 – Топология второй сети

## ЛАБОРАТОРНАЯ РАБОТА №6
## Функция коммутатора: port-security

### 1 Краткая теоретическая справка

Port security – функция коммутатора, позволяющая указать MAC-адреса хостов, которым разрешено передавать данные через порт. После этого порт не передает пакеты, если MAC-адрес отправителя не указан как разрешенный. Кроме того, можно указывать не конкретные MAC-адреса, разрешенные на порту коммутатора, а ограничить количество MAC-адресов, которым разрешено передавать трафик через порт.

Используется для предотвращения:

• несанкционированной смены MAC-адреса сетевого устройства или подключения к сети,

• атак направленных на переполнение таблицы коммутации. Коммутатор поддерживает такие типы безопасных MAC-адресов:

• Статические MAC-адреса:

o задаются статически командой switchport port-security mac-address mac- address в режиме настройки интерфейса,

o хранятся в таблице адресов,

o добавляются в текущую конфигурацию коммутатора;

• Динамические MAC-адреса:

o динамически выучиваются,

o хранятся только в таблице адресов,

o удаляются при перезагрузке коммутатора;

• Sticky MAC-адреса:

o могут быть статически настроены или динамически выучены,

o хранятся в таблице адресов,

o добавляются в текущую конфигурацию коммутатора. Если эти адреса сохранены в конфигурационном файле, после перезагрузки коммутатора, их не надо заново перенастраивать.

Нарушением безопасности для port security считаются ситуации:

• максимальное количество безопасных MAC-адресов было добавлено в таблицу адресов и хост, чей MAC-адрес не записан в таблице адресов пытается получить доступ через интерфейс,

• адрес, выученный или настроенный как безопасный на одном интерфейсе, появился на другом безопасном интерфейсе в том же VLAN'e.

На интерфейсе могут быть настроены такие режимы реагирования на нарушения безопасности:

• protect – когда количество безопасных MAC-адресов достигает максимального ограничения настроенного на порту, пакеты с неизвестным MAC-адресом отправителя отбрасываются до тех пор, пока не будет удалено достаточное количество безопасных MAC-адресов, чтобы их количество было меньше максимального значения, или увеличено максимальное количество разрешенных адресов. Оповещения о нарушении безопасности нет.

• restrict – когда количество безопасных MAC-адресов достигает максимального ограничения настроенного на порту, пакеты с неизвестным MAC-адресом отправителя отбрасываются до тех пор, пока не будет удалено достаточное количество безопасных MAC-адресов, чтобы их количество было меньше максимального значения, или увеличено максимальное количество разрешенных адресов. В этом режиме при нарушении безопасности

отправляется оповещение – отправляется SNMP trap, сообщение syslog и увеличивается счетчик нарушений (violation counter).

• shutdown – нарушение безопасности приводит к тому, что интерфейс переводится в состояние error-disabled и выключается немедленно, и выключается LED порта. Отправляется SNMP trap, сообщение syslog и увеличивается счетчик нарушений (violation counter). Когда порт в состоянии error-disabled, вывести из этого состояния его можно введя команду errdisable recovery cause psecure-violation или вручную включить интерфейс введя в режиме настройки интерфейса shutdown и no shutdown. Это режим по умолчанию.

На коммутаторах Cisco такие настройки по умолчанию для функции port security:

• Port security – выключен.

• Запоминание sticky-адресов – выключено.

• Максимальное количество безопасных MAC-адресов на порту-1.

• Режим реагирования на нарушения – shutdown.

• Время хранения адресов:

o отключено. Значение aging time – 0,

o для статических адресов – отключено,

o тип времени – абсолютное.

Цель работы – изучение специфики функцию коммутатора port-security.

## 2 Последовательность выполнения работы

Для изучения особенностей настройки функции port-security рассматривается схема, представленная на рис. 2.1.

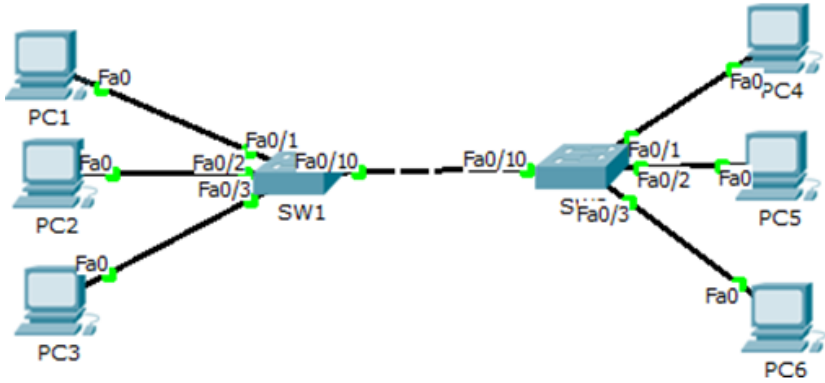



Рисунок 2.1 – Топология сети для изучения port-security

Таблица 1 – Таблица адресации

| Устройство | IP адрес | Маска подсети | Интерфейс | Режимы реагирования |
|---|---|---|---|---|
| PC1 | 16.4.0.1 | 255.0.0.0 | Fa0 | n/a |
| PC2 | 16.4.0.2 | 255.0.0.0 | Fa0 | n/a |
| PC3 | 16.4.0.3 | 255.0.0.0 | Fa0 | n/a |
| PC4 | 16.4.0.4 | 255.0.0.0 | Fa0 | n/a |
| PC5 | 16.4.0.5 | 255.0.0.0 | Fa0 | n/a |
| PC6 | 16.4.0.6 | 255.0.0.0 | Fa0 | n/a |
| SW1 | N/A | N/A | Fa0/1 | Shutdown |
| SW1 | N/A | N/A | Fa0/2 | Restrict |
| SW1 | N/A | N/A | Fa0/3 | Protect |
| SW2 | N/A | N/A | Fa0/1 | Shutdown |
| SW2 | N/A | N/A | Fa0/2 | Restrict |
| SW2 | N/A | N/A | Fa0/3 | Protect |

Установить порты в режим access на SW1 и SW2

```
Switch(config)#interface fastethernet0/10
Switch(config-if)#switchport mode access
```

Активировать port-security на портах SW1 и SW2, предназначенные для подключения оконечных устройств.

```
Switch(config-if)#switchport mode access
Switch(config-if)#
Switch(config-if)#switchport port-security
Switch(config-if)#
```

Установить максимальное количество secure-mac на портах SW1и SW2 смотрящие в сторону конечных устройств.

```
Switch(config-if)#switchport port-security maximum 1
```

Установить динамическое определение secure-mac на SW1

```
Switch(config-if)#switchport port-security mac-address sticky
```

Указать действие при нарушении настроенных ограничений на SW1 порт Fa0/1 и на SW2 порт Fa0/1.

```
Switch(config-if)#switchport port-security violation shutdown
```

Указать действие при нарушении настроенных ограничений на SW1 порт Fa0/2 и на SW2 порт Fa0/2

```
Switch(config-if)#switchport port-security violation restrict
```

Указать действие при нарушении настроенных ограничений на SW1 порт Fa0/3 и на SW2 порт Fa0/3

```
Switch(config-if)#switchport port-security violation protect
```

Проверить результат с помощью команды show port-security

Видно в каком состоянии находятся порты: Fa0/1 – shutdown, Fa0/2 – protect, Fa0/3 – restrict. Столбец Security Violation, является счетчиком. Значение в этом столбце равное 2, означает, что он сработал 2 раза, когда была попытка подключиться через небезопасный MAC-адрес.

## 3 Задание для самостоятельной работы

Схема, предназначенная для исследования, приведена на рис. 3.1. Информация, необходимая для конфигурирования оборудования приведена в табл. 2.

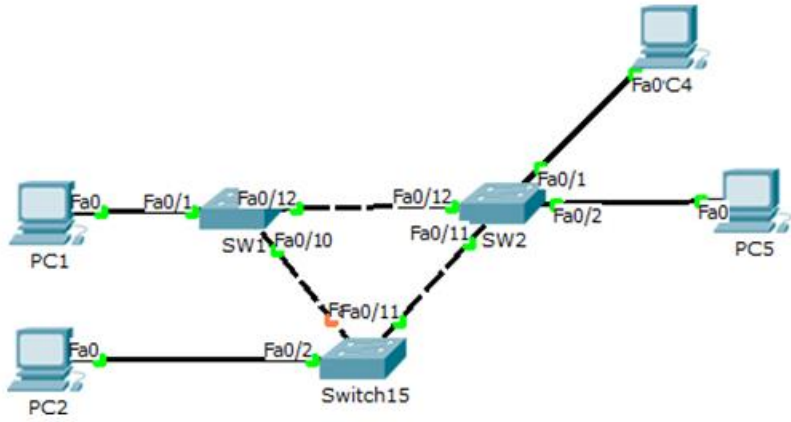



Рисунок 3.1 – Топология сети

Таблица 2 – Адресация

| **Устройство** | **IP адрес** | **Маска подсети** | **Интерфейс** | **Режимы реагирования** |
|---|---|---|---|---|
| PC1 | 192.168.0.66 | 255.255.255.128 | Fa0 | n/a |
| PC2 | 192.168.0.67 | 255.255.255.128 | Fa0 | n/a |
| PC3 | 192.168.0.68 | 255.255.255.128 | Fa0 | n/a |
| PC4 | 192.168.0.69 | 255.255.255.128 | Fa0 | n/a |
| SW1 | N/A | N/A | Fa0/1 | Protect |
| SW2 | N/A | N/A | Fa0/1 | Shutdown |
| SW2 | N/A | N/A | Fa0/2 | Restrict |
| Switch15 | N/A | N/A | Fa0/2 | Shutdown |

Необходимо:

1. Перевести интерфейсы fa0/1 – fa0/2 на всех SW в режим access.
2. Активировать port-security на всех портах SW, к которым подключены оконечные устройства.
3. На портах установить максимальное количество secure-mac равное двум.
4. Установить динамическое определение secure-mac.
5. Указать действие при нарушении настроенных ограничений в соответствии с табл. 2.
6. Проверить результат.

7. Результаты о проделанной работе показать преподавателю и обосновать результаты.

## ЛАБОРАТОРНАЯ РАБОТА №7
## Виртуальные локальные сети: VLAN

### 1 Краткая теоретическая справка

Коммутатор использует таблицу коммутации для пересылки трафика. Когда на один из его портов поступает пакет данных, он извлекает из него информацию о MAC-адресе приемника и ищет этот MAC-адрес в своей таблице коммутации. Если в таблице есть запись, ассоциирующая MAC-адрес приемника с одним из портов коммутатора, за исключением того, на который поступил кадр, то кадр пересылается через этот порт. Если такой ассоциации нет, кадр передается через все порты, за исключением того, на который он поступил. Это называется лавинным распространением (flooding). Широковещательная и многоадресная рассылка выполняется также путем лавинного распространения. С этим связана одна из проблем, ограничивающая применение коммутаторов. Наличие коммутаторов в сети не препятствует распространению широковещательных кадров (broadcast) по всем сегментам сети, сохраняя ее прозрачность. В случае если в результате каких-либо программных или аппаратных сбоев протокол верхнего уровня или сам сетевой адаптер начнет работать не правильно, и будет постоянно генерировать широковещательные кадры, коммутатор в этом случае будет передавать кадры во все сегменты, затапливая сеть ошибочным трафиком. Такая ситуация называется широковещательным штормом (broadcast storm).

Современные коммутаторы, как правило, обладают дополнительными функциями. Одной, из которых является VLAN – построение виртуальных локальных сетей. Построение и поддержка VLAN является одной из основных и часто применяемых функций, используемых в сетях с коммутаторами. Таким образом, применение технологии VLAN преследует следующие цели:

1. Уменьшение количества широковещательного трафика в сети. Это одна из основных задач, решаемая с помощью VLAN. Сеть, построенная на коммутаторах (устройства 2-го уровня модели OSI), даже при значительно разветвленной топологии обязана пропускать широковещательный трафик (MAC-адреса FFFF:FFFF:FFFF) ко всем компьютерам разных сегментов сети. Производительность сети в данные моменты значительно снижается. Создание VLAN на коммутаторе означает разбиение коммутатора на несколько широковещательных доменов. Если один и тот же VLAN есть на разных

коммутаторах, то порты разных коммутаторов будут образовывать один широковещательный домен.

2. Гибкое разделение устройств на группы. Как правило, одному VLAN соответствует одна IP-подсеть. Устройства, находящиеся в разных VLAN, будут находиться в разных IP-подсетях. Но в то же время VLAN не привязан к местоположению устройств и поэтому устройства, находящиеся на расстоянии друг от друга, все равно могут быть в одном VLAN независимо от местоположения.

3. Увеличение безопасности и управляемости сети. Когда сеть разбита на VLAN, упрощается задача применения политик и правил безопасности. С VLAN политики можно применять к целым подсетям, а не к отдельному устройству. Кроме того, переход из одного VLAN в другой предполагает прохождение через устройство 3 уровня, на котором, как правило, применяются политики, разрешающие или запрещающие доступ из VLAN в VLAN.

Другими словами VLAN – группа узлов сети, трафик которой, в том числе широковещательный, на канальном уровне полностью изолирован от трафика других узлов. Для того, чтобы трафик одной VLAN попадал в другую применяются сетевые устройства 3-го уровня OSI, а именно маршрутизаторы.

Таким образом, достоинством технологии виртуальных сетей является то; что она позволяет создавать полностью изолированные сегменты сети, путем логического конфигурирования коммутаторов, не прибегая к изменению физической структуры.

Построение VLAN сетей могут осуществляться различными способами. Самым широко используемым является VLAN на основе меток в дополнительном поле кадра (на основе поля Type кадра Ethernet) – стандарт IEEE 802.1Q (Protocol based). У провайдеров услуг широко используется технология Vlan на основе стандарта IEEE 802.1ad (Q-in- Q VLAN).

Тегированный кадр – помеченный кадр Ethernet, согласно стандарта IEEE 802.1Q, который имеет дополнительное 12 битное поле, помещаемое после поля с MAC-адресом отправителя. Введение стандарта 802.1Q позволило производителям оборудования преодолеть различия в фирменных реализациях VLAN и добиться совместимости при построении виртуальных локальных сетей. Поддерживают технику VLAN как производители коммутаторов, так и сетевых адаптеров для серверов.

Из выше сказанного, следует, что порты коммутатора, поддерживающие VLAN, (с некоторыми допущениями) можно разделить на два множества:

• Тегированные порты (или транковые порты, trunk-порты в терминологии Cisco, Huawei, tagged – в терминологии Alcatel, D-Link, ZyXEL и др.).

• Нетегированные порты (или порты доступа, access-порты в терминологии Cisco, Huawei, untagged – в терминологии Alcatel, D-Link, ZyXEL и др.).

Обычно, по умолчанию все порты коммутатора считаются нетегированными членами VLAN 1. В процессе настройки или работы коммутатора они могут перемещаться в другие VLAN.

***Исходный кадр***

| Адрес получателя | Адрес отправителя | Тип протокола | Данные | Контрольная сумма |
|---|---|---|---|---|

***Тегированный кадр***

| Адрес получателя | Адрес отправителя | Тег | Тип протокола | Данные | Новая контрольная сумма |
|---|---|---|---|---|---|

## 2 Последовательность выполнения работы

Для выполнения данной лабораторной работы необходимо знать IP адресацию IPv4, разбиение сети на подсети и базовые навыки конфигурации коммутаторов.

Цель работы – получение навыков создания и принципов работы VLAN.

Для этого требуется сформировать топологию сети, представленную на рис. 2.1. В таблице указана адресация, которую нужно применять только тогда, когда это будет явно указано в описательной части. В таблице 2.1 приведено назначение портов коммутаторов.

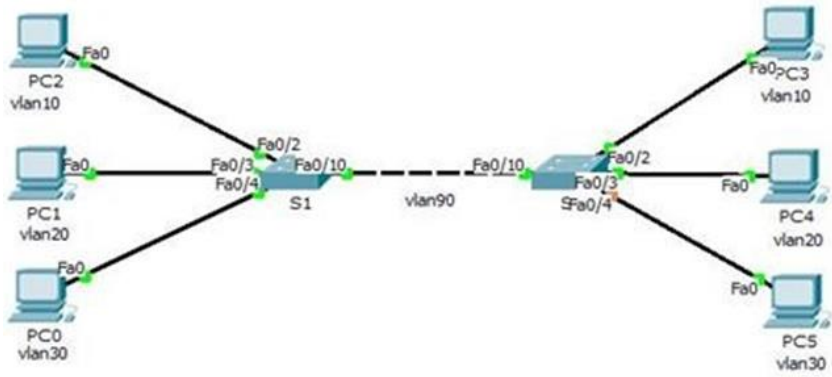



Рисунок 2.1 – Топология сети

Таблиц 1 – Адресация

| Устройство | Интерфейс | IP адрес | Маска подсети |
|---|---|---|---|
| PC0 | NIC | 192.168.30.10 | 255.255.255.0 |
| PC1 | NIC | 192.168.20.10 | 255.255.255.0 |
| PC2 | NIC | 192.168.10.10 | 255.255.255.0 |
| S1 | VLAN90 | 192.168.90.1 | 255.255.255.0 |
| S2 | VLAN90 | 192.168.90.2 | 255.255.255.0 |
| PC3 | NIC | 192.168.10.11 | 255.255.255.0 |
| PC4 | NIC | 192.168.20.11 | 255.255.255.0 |
| PC5 | NIC | 192.168.30.11 | 255.255.255.0 |

Первоначально необходимо активировать пользовательские порты на S2 и S3 и настроить режим access на пользовательские порт согласно таблице 2.2

Таблица 2 – Таблица назначения портов коммутаторов

| Порт | Назначение | Сеть |
|---|---|---|
| FastEthernet 0/10 | Trunks | 192.168.90.0 /24 |
| FastEthernet 0/2 | Access VLAN10 - Red | 192.168.10.0 /24 |
| FastEthernet 0/3 | Access VLAN20 - Blue | 192.168.20.0 /24 |
| FastEthernet 0/4 | Access VLAN30 - Green | 192.168.30.0 /24 |

Настройка интерфейсов коммутатора S1.

```
Switch#enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface range fa0/2, fa0/3, fa0/4
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#no shutdown
Switch(config-if-range)#
```

Аналогично сконфигурировать порты на S2. Далее настроить сетевые интерфейсы PC0, PC1, PC2, PC3, PC4 и PC5 в соответствии с планом адресации. Создать и присвоить имена VLAN на коммутаторах в соответствии с таблицей.

```
Switch(config)#vlan 90
Switch(config-vlan)#name management
Switch(config-vlan)#ex
Switch(config)#vlan 10
Switch(config-vlan)#name red
Switch(config-vlan)#ex
Switch(config)#vlan 20
Switch(config-vlan)#name blue
Switch(config-vlan)#ex
Switch(config)#vlan 30
Switch(config-vlan)#name green
```

Таким же образом настроить VLAN на коммутаторе S2. Далее проверить выполненные действия на каждом из коммутаторов командой show vlan brief.

```
Switch#show vlan brief

VLAN Name                                Status
---- ----------------------------------- ---------
1    default                             active




10   red                                 active
20   blue                                active
30   green                               active
90   management                          active
```

На коммутаторах S1 и S2 назначить порты соответствующим VLAN и установить режим работы.

```
Switch(config)#interface fastEthernet 0/2
Switch(config-if)#switchport access vlan 10
Switch(config-if)#ex
Switch(config)#interface fastEthernet 0/3
Switch(config-if)#switchport access vlan 20
Switch(config-if)#ex
Switch(config)#interface fastEthernet 0/4
Switch(config-if)#switchport access vlan 30
```

Проверить правильность настроек командой show vlan id vlan-number.

```
Switch#show vlan id 20

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
20   blue                             active    Fa0/3

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
20   enet  100020     1500  -      -      -        -    -        0      0
```

Назначить IP-адрес для интерфейса управления коммутатора S1.

```
Switch(config)#interface vlan 90
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan90, changed state to up

Switch(config-if)#ip add
Switch(config-if)#ip address 192.168.90.1 255.255.255.0
```

Аналогично назначить IP-адрес коммутатору S2. Далее на каждом из коммутаторов настроить trunk-порты.

```
Switch#
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface fastEthernet0/10
Switch(config-if)#switchport mode trunk
```

Аналогично перевести интерфейс Fa0/10 коммутатора S2 в режим trunk, после чего проверить правильность настройки с помощью команды show interfaces trunk.

```
Switch#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/10      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/10      1-1005

Port        Vlans allowed and active in management domain
Fa0/10      1,10,20,30,90

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/10      1,10,20,30,90
```

Из консоли коммутатора S1 выполнить команду ping для проверки связи с коммутатором S2.

```
Switch>
Switch>ping 192.168.90.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.90.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

Правильность настроек проверить с помощью команды ping. Так, проверить связь между PC0 и PC5, PC1 и PC4, PC2 и PC3.

### 3.3 Задание для самостоятельной работы

Сформировать следующую топологию сети на рис. 3.1. Необходимая информацию для настройки оборудования находится в табл. 3.2–3.3.

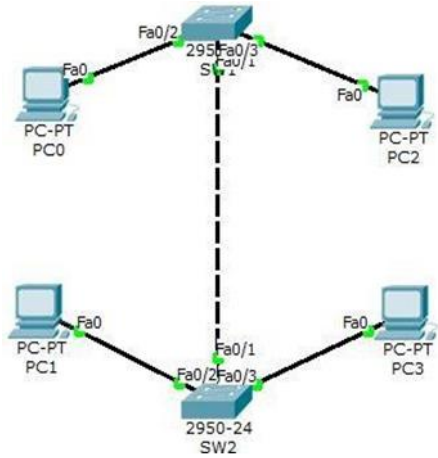


Рисунок 3.2 – Топология сети

Таблица 3 – Адресация

| Устройство | Интерфейс | IP адрес | Маска подсети |
|---|---|---|---|
| PC0 | NIC | 172.16.60.61 | 255.255.255.0 |
| PC1 | NIC | 172.16.60.62 | 255.255.255.0 |
| PC2 | NIC | 172.16.80.81 | 255.255.255.0 |
| PC3 | NIC | 172.16.80.82 | 255.255.255.0 |
| S1 | VLAN99 | 172.16.99.1 | 255.255.255.0 |
| S2 | VLAN99 | 172.16.99.2 | 255.255.255.0 |

Таблица 4 – Назначение портов

| Порт | Назначение | Сеть |
|---|---|---|
| FastEthernet 0/1 на SW1 | Trunks | 172.16.99.0 /24 |
| FastEthernet 0/1 на SW2 | Trunks | 172.16.99.0 /24 |
| FastEthernet 0/3 | VLAN60 – tusurtu | 192.168.60.0 /24 |
| FastEthernet 0/4 | VLAN80 – tusurtor | 192.168.80.0 /24 |

Необходимо:

1. Активировать пользовательские порты на SW1 и SW2. Настроить пользовательские порты в режиме access в соответствии со схемой.

2. Настроить Ethernet интерфейсы персональных компьютеров в соответствии с планом адресации.

3. Настроить VLAN на коммутаторах.

4. Проверить выполненные действия на каждом из коммутаторов командой show vlan brief.

5. На коммутаторах SW1 и SW2 назначить порты соответствующим VLAN согласно таблицы назначения портов.

6. Проверить выполненные настройки командой show vlan id vlan-number.

7. Настроить IP-адреса для интерфейсов управления на SW1 и SW2.

8. На каждом из коммутаторов настроить trunk-порты.

9. Проверить выполненные действия командой show interface trunk.

10. Проверить наличие связей между узла сети.

11. С помощью утилиты ping проверить связь между PC0 и PC1, PC2 и PC3.

12. Результаты о проделанной работе показать преподавателю и обосновать результаты.

## 4 Поиск неисправностей

В ходе данной части работы необходимо восстановить работоспособность двух сетей. Результат продемонстрировать преподавателю. Топология первой сети приведена на рис. Ошибка! Источник ссылки не найден.. Файл выдается преподавателем. Дано 3 VLAN. VLAN20 с именем «Service», VLAN30 – «Marketing», VLAN99 – «Management». Адресные пространства: 192.168.30.0 для VLAN30, 192.168.20.0 – VLAN20, 192.168.99.0 – VLAN99. Требуется восстановить работоспособность сети. Результатом поиска неисправностей должно являться наличие связи между конечными устройствами.

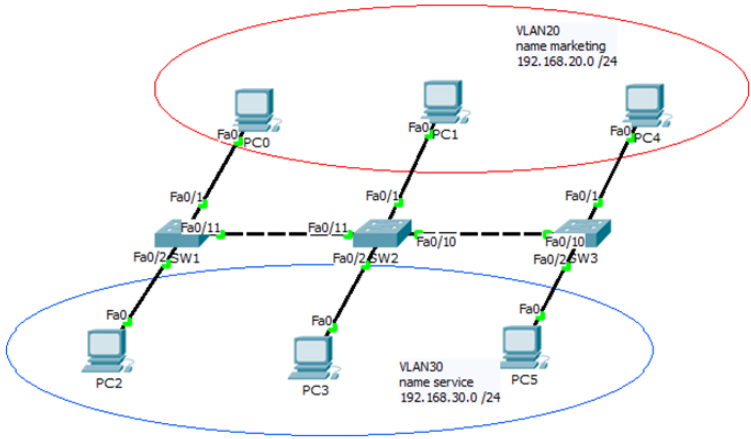



Рисунок 4.1– Топология сети

Второй частью работы посвящена поиску неисправностей в сети, топология которой приведена рис. 4.2 (для наглядности принадлежность хоста определенной VLAN показана с помощью цветовой раскраски).

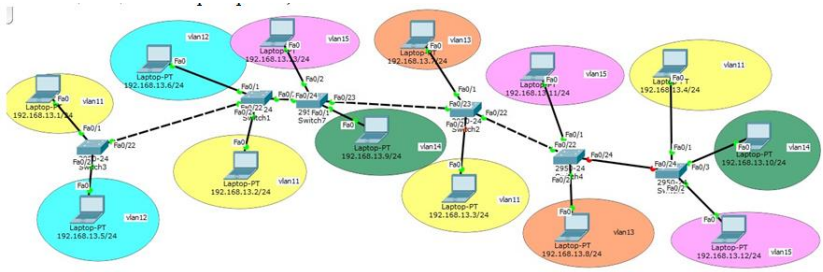



Рисунок 4/2 – Топология сети

## ЛАБОРАТОРНАЯ РАБОТА №8
## Маршрутизация между VLAN: Inter-VLAN, Switch L3 и VTP

### 1 Краткая теоретическая справка

Для взаимодействия устройств, находящихся в разных VLAN, необходим маршрутизатор. Процесс маршрутизации пакетов из одной VLAN в другую называется маршрутизацией между VLAN, или Inter-VLAN маршрутизацией.

Принцип обеспечения маршрутизации между VLAN можно показать на рис. 1. Для передачи трафика из одной сети в другую необходим маршрутизатор. Таким образом, необходимо организовать подключение каждой VLAN к маршрутизатору. Самый простой способ сделать это – подключить порт доступа каждой VLAN к своему интерфейсу маршрутизатора. Интерфейсам присваивается соответствующий данной VLAN IP-адрес. В качестве недостатка такого метода можно отметить высокую стоимость и низкую масштабируемость, поскольку для каждой VLAN требуется выделить по одному интерфейсу коммутатора и маршрутизатора.

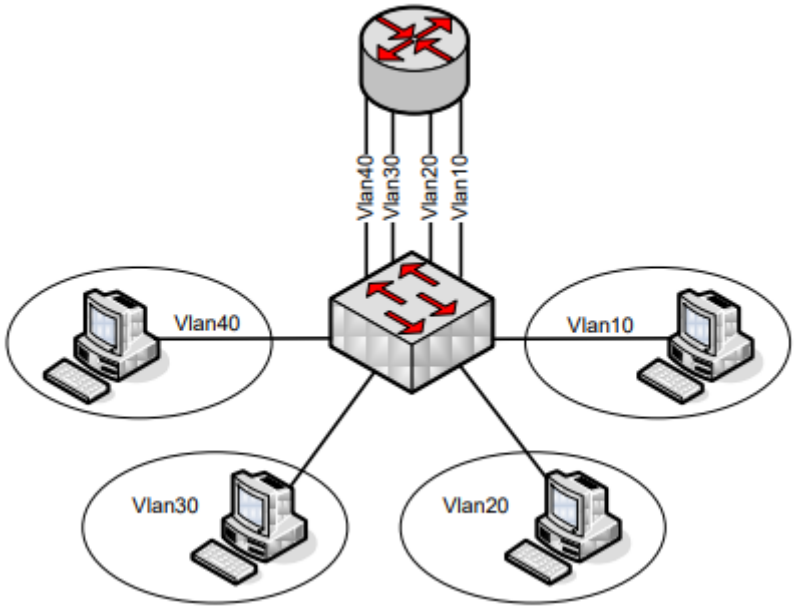



Рисунок 1 – Топология сети с отдельным соединением для каждой Vlan

Более экономичным является решение «маршрутизатор на палочке» («Router on a stick»), использующее преимущество магистральных (trunk) каналов, применяемых в виртуальных локальных сетях. Суть метода заключается в том, что между коммутатором и маршрутизатором формируется магистральный канал, что позволяет передавать информацию от разных VLAN по одному соединению. Затем на маршрутизаторе создаются подынтерфейсы для каждой VLAN, которым присваиваются соответствующие IP-адреса. Это решение позволяет реализовать Inter-VLAN маршрутизацию с гораздо меньшими, чем в предыдущем варианте, затратами. Как правило, номер подынтерфейса соответствует номеру Vlan, для которого он настроен (рис. 2).

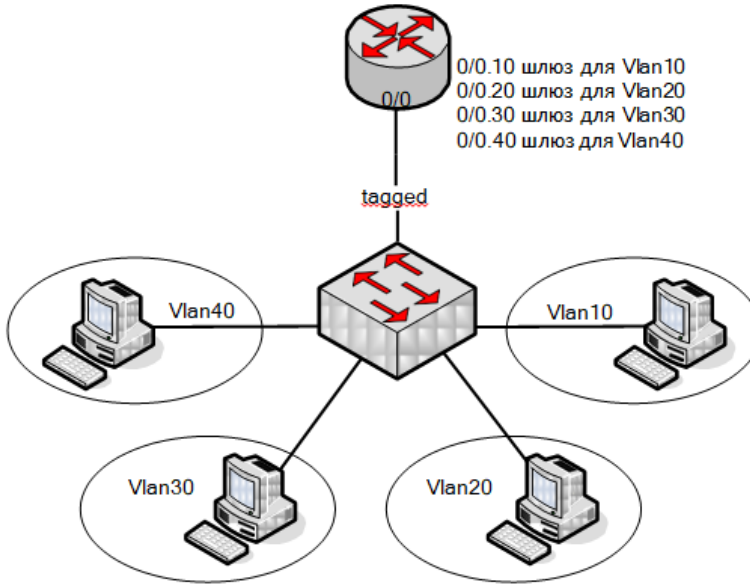



Рисунок 2 – Топология сети с одним соединением для всех Vlan

VLAN Trunking Protocol (VTP) – проприетарный протокол компании Cisco, предназначенный для создания, удаления и переименования VLAN на сетевых устройствах.

На коммутаторе VTP может работать в трёх режимах:

• Server (режим по умолчанию):

- Можно создавать, изменять и удалять VLAN из командной строки коммутатора.
- Генерирует объявления VTP и передает объявления от других коммутаторов.
- Может обновлять свою базу данных VLAN при получении информации не только от других VTP серверов но и от других VTP клиентов в одном домене, с более высоким номером ревизии.

• Client:

- Нельзя создавать, изменять и удалять VLAN из командной строки коммутатора.
- Передает объявления от других коммутаторов.
- Синхронизирует свою базу данных VLAN при получении информации VTP.

• Transparent:

- Можно создавать, изменять и удалять VLAN из командной строки коммутатора, но только для локального коммутатора.
- Не генерирует объявления VTP.
- Передает объявления от других коммутаторов.
- Не обновляет свою базу данных VLAN при получении информации по VTP.
- Всегда использует configuration revision number 0.

## 2 Последовательность выполнения работы

Для выполнения данной работы необходимо знать IP адресацию IPv4 и базовые навыки конфигурации коммутаторов и маршрутизаторов.

Цель – изучение принципов маршрутизации между VLAN.

Необходимо организовать физическую топологию, аналогичную, представленной на рис. 3. Далее выполнять необходимые настройки только тогда, когда это явно указано в описательной части работы. Требуемая адресация приведена в табл. 1.

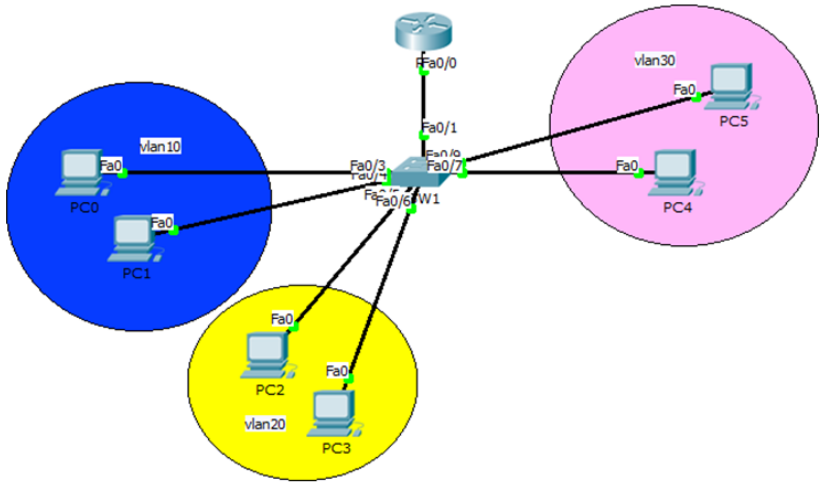



Рисунок 3 – Топология сети

Таблица 1 - Адресация (маска подсети – /24)

| Устройство | Интерфейс | IP адрес | Шлюз по умолчанию | VLan |
|---|---|---|---|---|
| PC0 | Fa0/3 | 192.168.10.10 | 192.168.10.254 | 10 |
| PC1 | Fa0/4 | 192.168.10.11 | 192.168.10.254 | 10 |
| PC2 | Fa0/5 | 192.168.20.10 | 192.168.20.254 | 20 |
| PC3 | Fa0/6 | 192.168.20.11 | 192.168.20.254 | 20 |
| PC4 | Fa0/7 | 192.168.30.10 | 192.168.30.254 | 30 |
| PC5 | Fa0/8 | 192.168.30.11 | 192.168.30.254 | 30 |
| R1 | Fa0/0.10 | 192.168.10.254 | | 10 |
| R1 | Fa0/0.20 | 192.168.20.254 | | 20 |
| R1 | Fa0/0.30 | 192.168.30.254 | | 30 |
| S1 | Vlan10 | 192.168.10.1 | | 10 |
| S1 | Vlan20 | 192.168.20.1 | | 20 |
| S1 | Vlan30 | 192.168.30.1 | | 30 |

Первоначально необходимо создать VLAN 10 на коммутаторе SW1. Назначить Student в качестве имени сети VLAN.

```
Switch>enable
Switch#conf term
Switch(config)#vlan 10
Switch(config-vlan)#name student
Switch(config-vlan)#exit
Switch(config)#
```

Таким же образом создать оставшиеся VLAN и присвоить им соответствующие имена. Далее настроить интерфейс F0/1 в качестве транкового порта на SW1.

```
Switch#conf term
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport mode trunk
```

Назначить портов Fa0/3 и Fa0/4 сети VLAN 10 и настройка портов в качестве портов доступа.

```
Switch(config)#interface range fastEthernet 0/3-4
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#exit
```

Таким же образом назначить порты Fa0/5 и Fa0/6 сети VLAN 20 и настроить порты в качестве портов доступа. Далее назначить порты Fa0/7 и Fa0/8 сети VLAN 30 и настроить порты в качестве портов доступа. Затем назначить IP-адрес интерфейсу VLAN 10 и активировать его. Свериться с таблицей адресации.

```
Switch(config)#interface vlan 10
Switch(config-if)#ip address 192.168.10.1 255.255.255.0
Switch(config-if)#no shutdown
```

Таким же образом назначить IP-адрес интерфейсу VLAN 20 и активировать его. Свериться с таблицей адресации. Назначить IP-адрес сети VLAN 30 и активировать его. Свериться с таблицей адресации. Включить физический интерфейс, подключенный к коммутатору командой no shutdown.

```
Router#conf term
Router(config)#interface fa0/0
Router(config-if)#no shutdown
```

Настроить подынтерфейсы (сабинтерфейсы) на R1 для VLAN10. Обратите внимание на то что после команды encapsulation dot1Q необходимо указать номер vlan и адрес из той же подсети, что и у оборудования, подключенного к портам коммутатора соответствующего Vlan.

```
Router#conf t
Router(config)#interface fa0/0.10
Router(config-subif)# encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.10.254 255.255.255.0
```

Таким же образом настроить подынтерфейсы на R1 для VLAN20 и VLAN30. Проверить правильности конфигурации путем использования утилиты ping. Необходимо протестировать связь внутри каждой Vlan и затем протестировать связь между Vlan. Результаты теста внутри Vlan10. В случае отсутствия связи проверить правильность настроек.

Для дальнейшего изучения используется топология сети (с указанием адресации) приведена на рис. 4. Она включает 3 коммутатора второго уровня, центральный коммутатор третьего уровня (Switch3), выполняющий роль маршрутизатора, сервер и 3 подсети по два узла в каждой. Требуется организовать доступность компьютеров только в своих VLAN и сервера.

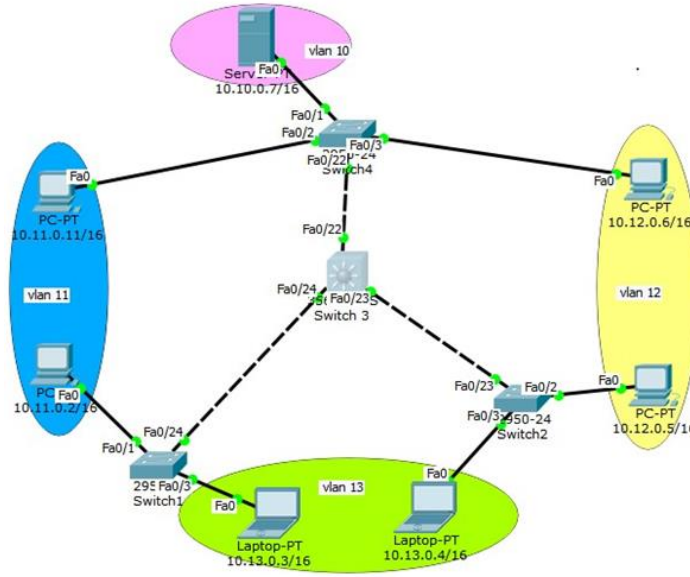



Рисунок 4 – Топология сети

Первоначально настроить адресацию на компьютерах и сервере с указанием соответствующих адресов шлюзов. Далее приступить к настройке центрального коммутатора. Создать VLAN 10.

```
Switch3>en
Switch3#conf t
Switch3(config)#vlan 10
Switch3(config-vlan)#exit
```

Аналогично создать VLAN 11, VLAN 12 и VLAN 13. Далее необходимо настроить протокол VTP в режиме сервера.

```
Switch3(config)#vtp domain HOME
Switch3(config)#vtp password HOME
Switch3(config)#vtp mode server
```

Просмотреть информацию о конфигурации VTP можно с помощью команды Switch#sh vtp status. Затем перевести требуемые интерфейсы (fa0/22–fa0/24) в режим транка. Для настройки первого из них требуется:

```
Switch3(config)#int fa0/1
Switch3(config-if)#switchport mode trunk
Switch3(config-if)#exit
```

Аналогично настроить fa0/23 и fa0/24. После этого приступить к настройке коммутатора Switch4 и перевести его в режим client. Для этого создать vlan 10 и перевести интерфейс fa0/1 в режим access.

```
Switch4>en
Switch4#conf t
Switch4(config)#vlan 10
Switch4(config-vlan)#exit
Switch4(config)#int fa0/1
Switch4(config-if)#switchport access vlan 10
Switch4(config-if)#switchport mode access
Switch4(config-if)#no shut
```

Далее аналогично создать vlan 11 и 12 перевести интерфейсы fa0/2 и fa0/3 в режим access. После чего перевести коммутатор в режим client.

```
Switch4(config)#vtp domain HOME
Switch4(config)#vtp password HOME
Switch4(config)#vtp mode client
```

После этого выполнить аналогичные настройки интерфейсы коммутаторов Switch 1 и Switch 2 и перевести их в режим client. После чего проверить работоспособность сети. После установки всех настроек таблица VLAN будет разослана на все коммутаторы с помощью протокола VTP. В результате компьютеры, расположенные в одном vlan, будут доступны друг для друга, а другие компьютеры недоступны. Если все сделано правильно, то соединение между компьютерами одного vlan будет успешно, если нет – то необходимо проверить следующие настройки:

– режимы транковых портов на коммутаторах;

– наличие всех требуемых vlan на коммутаторах;

– названия и пароли доменов на каждом коммутаторе (команда show vtp status);

– привязку интерфейсов к vlan на коммутаторах (команда show vlan brief).

Только после правильной работе сети приступить к настройке маршрутизации на центральном коммутаторе. Первоначально требуется создать интерфейсы для каждого vlan. Так, настройка интерфейса для

vlan 10 (шлюз по умолчанию) сводится к следующей последовательности действий.

```
Switch3(config)#int vlan 10
Switch3(config-if)#ip address 10.10.0.1 255.255.0.0
Switch3(config-if)#no shut
Switch3(config-if)#exit
```

Далее выполнить аналогичные действия для каждого vlan. После этого проверить совпадение IP-адресов интерфейсов vlan и настроек шлюзов на компьютерах. Далее включить маршрутизацию командой: Switch3(config)#ip routing. После чего проверить работу сети. Так, после включения маршрутизации все компьютеры будут доступны с любого хоста. В случае правильности настроек приступить к выполнению основной задачи работы: для любого vlan могут быть доступны только узлы этого же vlan и сервер. Для этого требуется ввести следующие ограничения на трафик:

1. Разрешить пакеты от любого хоста к серверу.
2. Разрешить пакеты от сервера к любому хосту.
3. Разрешить трафик от компьютеров одной подсети к компьютерам из той же подсети.
4. Правило по умолчанию: запретить всё остальное.

Ограничения на трафик сети задаются с помощью команды фильтрации access-list. Данная команда задает критерии фильтрации в списке опций разрешения и запрета, называемом списком доступа. Списки доступа имеют два правила: permit – разрешить и deny – запретить. Данные правила либо пропускают пакет дальше по сети, либо блокируют его доступ.

Таким образом, требуется провозвести следующие настройки на центральном коммутаторе.

```
Создать расширенный список доступа под номером, например, 100
Switch3(config)#ip access-list extended 100
Разрешается доступ к сети 10.10.0.0/24 из любой подсети
Switch3(config-ext-nacl)#permit ip any 10.10.0.0 0.0.0.255
Разрешается доступ к любым подсетям из сети 10.10.0.0/24
Switch3(config-ext-nacl)#permit ip 10.10.0.0 0.0.0.255 any
Разрешается доступ из сети 10.11.0.0/24 в эту же сеть
Switch3(config-ext-nacl)#permit ip 10.11.0.0 0.0.0.255 10.11.0.0 0.0.0.255
Разрешается доступ из сети 10.12.0.0/24 в эту же сеть
Switch3(config-ext-nacl)#permit ip 10.12.0.0 0.0.0.255 10.12.0.0 0.0.0.255
Разрешается доступ из сети 10.13.0.0/24 в эту же сеть
Switch3(config-ext-nacl)#permit ip 10.13.0.0 0.0.0.255 10.13.0.0 0.0.0.255
```

После этого требуется применить созданный список доступа на конкретный интерфейс vlan и входящий трафик (опция in):

```
Switch3(config)#int vlan 10
Switch3(config-if)#ip access-group 100 in
```

Аналогично применить список к интерфейсам остальных vlan. После чего проверить выполнение требований работы.

## 3 Задание для самостоятельной работы

Топология первой сети приведена на рис. 5. Требуемая адресация приведена в табл. 2.

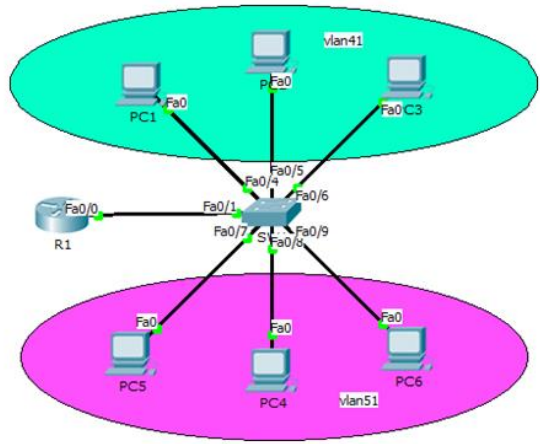



Рисунок 5 – Топология сети

Таблица 2 – Адресация (маска подсети – /24)

| Устройство | Интерфейс | IP адрес | Шлюз по умолчанию | Vlan |
|---|---|---|---|---|
| PC1 | Fa0/4 | 192.168.41.4 | 192.168.41.254 | 41 |
| PC2 | Fa0/5 | 192.168.41.5 | 192.168.41.254 | 41 |
| PC3 | Fa0/6 | 192.168.41.6 | 192.168.41.254 | 41 |
| PC4 | Fa0/7 | 192.168.41.7 | 192.168.41.254 | 51 |
| PC5 | Fa0/8 | 192.168.41.8 | 192.168.41.254 | 51 |
| PC6 | Fa0/9 | 192.168.41.9 | 192.168.41.254 | 51 |
| R1 | Fa0/0.41 | | | 41 |
| R1 | Fa0/0.51 | | | 51 |
| S1 | Vlan41 | 192.168.41.4 | | 41 |
| S1 | Vlan51 | 192.168.41.4 | | 51 |

Необходимо:

1. Создать VLAN 41 на коммутаторе SW1. Назначить emcpost в качестве имени сети VLAN.
2. Создать VLAN 510 на коммутаторе SW1. Назначить dhlpost в качестве имени сети VLAN.
3. Настроить F0/1 в качестве транкового порта на SW1
4. Назначить порты Fa0/4, Fa0/5 и Fa0/6 сети VLAN 41 и настроить порты в качестве портов доступа.
5. Назначить порты Fa0/7, Fa0/8 и Fa0/9 сети VLAN 51 и настроить порты в качестве портов доступа.
6. Назначить IP-адрес сети VLAN 41 и активировать его. Свериться с таблицей адресации
7. Назначить IP-адрес сети VLAN 51 и активировать его. Свериться с таблицей адресации.
8. Включить физический интерфейс, подключенный к коммутатору командой no shutdown.
9. Настроить Саб интерфейс на R1 для VLAN41
10. Настроить Саб интерфейс на R1 для VLAN51
11. Проверить правильности конфигурации путем использования утилиты ping.
12. Результаты о проделанной работе показать преподавателю и обосновать результаты.

Топология второй сети приведена на рис. 6. Так, на предприятии имеется два отдела. Компьютеры отдел 1 подключена к Switch1, компьютеры отдела2 к Switch2. В каждой сети имеется сервер со службами DHCP, DNS и HTTP (на серверах Server1 и Server2 расположены интернет-сайты отделов). Компьютеры ПК0 и ПК3 с DHCP серверов своих сетей получают параметры: IP-адрес и шлюз. Компьютеры ПК1 и ПК2 находятся в отдельной сети в одном VLAN. Требуется дополнить схему сети маршрутизатором или коммутатором третьего уровня, чтобы обеспечить работу корпоративной сети в следующих режимах:

1 – компьютеры ПК0 и ПК3 должны открывать сайты каждого отдела;

2 – компьютеры ПК1 и ПК2 должны быть доступны только друг для друга.

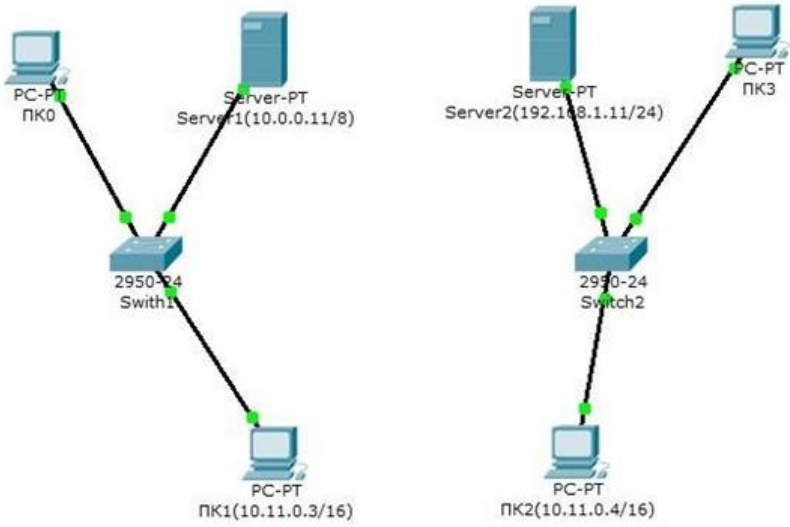



Рисунок 6 – Топология сети

## ЛАБОРАТОРНАЯ РАБОТА №9
## Агрегирование каналов

### 1 Краткая теоретическая справка

Агрегирование каналов (link aggregation) – технологии объединения нескольких параллельных каналов передачи данных в сетях Ethernet в один логический, позволяющие увеличить пропускную способность и повысить надёжность. Стандарт IEEE 802.3ad в составе группы стандартов для локальных вычислительных сетей IEEE 802, принят в 2000 году, полное название – «802.3ad Link aggregation for parallel links».

В общем случае, агрегирование восьми стандартных каналов с помощью 802.3ad оказывается дешевле, чем одно устройство, поддерживающее на порядок большую пропускную способность, и позволяет постепенно увеличивать скорость каналов в системе без необходимости покупать разом дорогостоящие новые платы, на порядок более быстрые. Однако агрегирование имеет ограничения: распределение трафика по каналам может быть неравномерным, вплоть до того, что весь трафик идёт по одному каналу, а другие простаивают (зависит от трафика, возможностей и настроек оборудования), что в крайних случаях означает отсутствие выигрыша в пропускной способности по сравнению с единственным каналом. Кроме того, объединять можно не более восьми каналов, что в случае гигабитных каналов даёт теоретическую суммарную пропускную способность лишь в 8 Гбит/сек в сравнении с одной платой, поддерживающей 10 Гбит/сек.

Как правило, все порты при агрегировании подбираются одного типа, например, все порты с медным покрытием (CAT-5E/CAT-6), все порты оптоволокна одномодового (SM) или многомодового (MM). Также на практике объединяют порты одной скорости, хотя по стандарту 802.3ad смешивать порты с разной скоростью допустимо, на практике такие конфигурации зачастую оказываются неработоспособными.

В терминологии Cisco данная технология называется EtherChannel (вообще говоря, разделяют Fast EtherChannel и Gigabit EtherChannel, но для простоты дальнейшего изложения будет использоваться термин EtherChannel и 100 Мб/с линки для соединений). Существует два протокола, позволяющие автоматически создавать и обслуживать каналы EtherChannel:

- PAgP, проприетарный протокол Cisco.
- LACP, протокол стандарта IEEE 802.3ad.

Поскольку протокол LACP является стандартом IEEE, его можно использовать для создания EtherChannel, при использовании оборудования различных производителей. Поэтому в данном занятии будет рассматриваться именно он и его специфика реализации в оборудовании Cisco.

## 2 Последовательность выполнения работы

Для выполнения данной работы необходимо знать IP адресацию IPv4, принцип агрегирования каналов и базовые навыки конфигурации коммутаторов.

Цель – изучение принципов настройки режима агрегирования каналов.

Для изучения агрегации каналов рассмотрим следующую сеть, состоящую из двух коммутаторов и двух ноутбуков. Первоначально необходимо настроить подключение ноутбуков. Для этого надо задать им IP-адреса (см. рис. 1). Для подключения к коммутатора использовать режим доступа (access, Vlan=10).

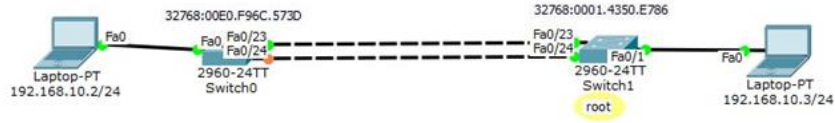



Рисунок 1 – Топология сети

При настройке следуйте следующим рекомендациям и ограничениям при конфигурации интерфейсов EtherChannel:

• Конфигурировать все интерфейсы в EtherChannel необходимо для работы на одной скорости и в одном режиме дуплекса.

• Все интерфейсы в EtherChannel должны принадлежать одной Vlan или быть сконфигурированы как транки.

• EtherChannel поддерживает весь диапазон разрешенных Vlan на всех интерфейсах, когда работает как транковый EtherChannel второго уровня.

Если необходимо изменить эти параметры, необходимо конфигурировать их в режиме конфигурации EtherChannel-интерфейса. После того как, сконфигурирован EtherChannel-интерфейс, любая конфигурация, применяемая к интерфейсу PortChannel, также применяется к индивидуальным интерфейсам. Однако конфигурация, применяемая к индивидуальному интерфейсу, не будет применяться к

интерфейсу PortChannel, что может вызвать несовместимость интерфейсов, принадлежащих EtherChannel.

Далее настроим агрегацию каналов, выполнив следующие команды на обоих коммутаторах:

```
Switch(config)# interface range fa0/23-24[1]
Switch (config-if-range)#channel-group  3 mode active [2]
Switch (config-if-range)#exit
Switch (config)#interface  port-channel 3
Switch (config-if)#  switchport mode trunk
Switch (config-if)#  switchport trunk allowed vlan 1,10
```

После этого необходимо убедиться, что порты объединены в логические каналы с

помощью команды show etherchannel summary. В результате получим:

```
Switch#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+---------------------------

3      Po3(SU)           LACP    Fa0/23(P) Fa0/24(P)
Switch#
```

После чего схема привет вид:

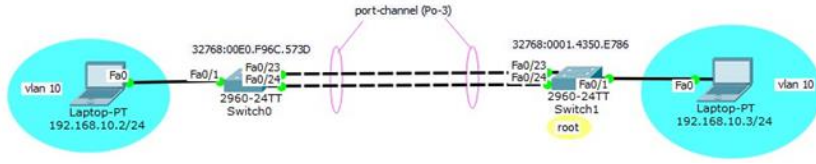



Схема сети после агрегации каналов

Далее следует обратить внимание, на то, как изменилась индикация интерфейсов коммутаторов. Используя команду show etherchannel port-channel можно просмотреть информацию об Port-

channel-интерфейсе. В данном примере, интерфейс Port-channel 2 состоит из двух физических интерфейсов: FastEthernet0/21 и FastEthernet0/22. Он использует LACP в активном режиме и корректно соединен с другим коммутатором с совместимой конфигурацией, поэтому он показывает, что используется (параметр Load не показывает загрузку интерфейса. Он является шестнадцатеричной величиной, которая показывает, какой интерфейс будет выбран для определенного потока трафика).

```
Switch#show etherchannel port-channel
                Channel-group listing:
                ----------------------

Group: 2
----------
                Port-channels in the group:
                ---------------------------

Port-channel: Po2    (Primary Aggregator)
------------

Age of the Port-channel   = 00d:00h:18m:46s
Logical slot/port   = 2/2       Number of ports = 2
GC                  = 0x00000000      HotStandBy port = null
Port state          = Port-channel
Protocol            =   LACP
Port Security       = Disabled

Ports in the Port-channel:

Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
  0     00     Fa0/21   Active             0
  0     00     Fa0/22   Active             0
Time since last port bundled:    00d:00h:14m:12s    Fa0/22
Group: 3
----------
                Port-channels in the group:
                ---------------------------

Port-channel: Po3    (Primary Aggregator)
------------

Age of the Port-channel   = 00d:00h:18m:46s
Logical slot/port   = 2/3       Number of ports = 2
GC                  = 0x00000000      HotStandBy port = null
Port state          = Port-channel
Protocol            =   LACP
Port Security       = Disabled
```

Далее необходимо организовать физическую топологию, аналогичную, представленной на рис. и выполнять необходимые настройки только тогда, когда это явно указано в описательной части работы.

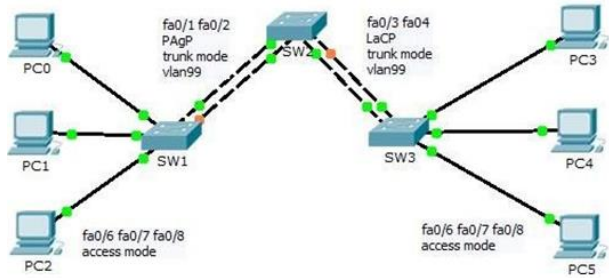



Рисунок 2 – Топология сети

Таблица 1 – Адресация

| Устройство | Интерфейс | IP – адрес | Маска подсети |
|---|---|---|---|
| PC0 | NIC | 192.168.99.10 | 255.255.255.0 |
| PC1 | NIC | 192.168.99.11 | 255.255.255.0 |
| PC2 | NIC | 192.168.99.12 | 255.255.255.0 |
| PC3 | NIC | 192.168.99.20 | 255.255.255.0 |
| PC4 | NIC | 192.168.99.21 | 255.255.255.0 |
| PC5 | NIC | 192.168.99.22 | 255.255.255.0 |
| SW1 | VLAN99 | 192.168.99.31 | 255.255.255.0 |
| SW2 | VLAN99 | 192.168.99.32 | 255.255.255.0 |
| SW3 | VLAN99 | 192.168.99.33 | 255.255.255.0 |

На SW1–SW3 создать VLAN99 и присвоить ему имя management.

```
Switch(config)#vlan 99
Switch(config-vlan)#name management
```

Назначить IP адреса VLAN99 у коммутаторов согласно таблице адресации

```
Switch(config)#interface vlan99
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

Switch(config-if)#ip address 192.168.99.31 255.255.255.0
Switch(config-if)#no shutdown
```

Порты коммутаторов, предназначенные для подключения соседних коммутаторов перевести в режим trunk. Пример.

```
Switch(config)#interface range Fa0/1, Fa0/2
Switch(config-if-range)#switchport mode trunk
```

Порты, предназначенные для подключения оконечных устройства перевести в режим access. Пример.

```
Switch#enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface range fa0/6, fa0/7, fa0/8
Switch(config-if-range)#switchport mode access
```

Назначить IP адреса на всех PC согласно таблице 10.1. Настроить Etherchannel на всех коммутаторах. Для этого транковые порты SW1 (рис. 10.3) и SW2 (рис. 10.4) объединить в канал под номером 1 и включить на них режим PAGP.

```
Switch(config)#interface range fa0/1, fa0/2
Switch(config-if-range)#channel-group 1 mode auto
Switch(config-if-range)#
Creating a port-channel interface Port-channel 1
```

Рисунок 3 – Настройка портов коммутатора SW1

```
Switch(config)#interface range fa0/1, fa0/2
Switch(config-if-range)#channel-group 1 mode desirable
Switch(config-if-range)#
Creating a port-channel interface Port-channel 1
```

Рисунок 4 – Настройка портов коммутатора SW2

При конфигурации агрегирования каналов, необходимо учитывать особенности протокола PAGP (табл. 2).

Таблица 2 – Особенности протокола PAGP

| Режим (mode) | Описание |
|---|---|
| On | Интерфейсы становятся частью логического канала, но не обмениваются PAGP-пакетами |
| PAGP Auto | Коммутатор пассивно ожидает подключения со стороны сосед |
| PAGP Desirable | Коммутатор активно пытается подключиться к соседу |

Порты между SW2 и SW3 необходимо объединить в логический канал под номером 2 и активировать протокол LACP. На первом active (рис. 5), на втором passive (рис. 6). Отличие режимов приведено в табл. 3.

```
Switch(config)#interface range fa0/3, fa0/4
Switch(config-if-range)#channel-group 2 mode active
Switch(config-if-range)#
Creating a port-channel interface Port-channel 2
```

Рисунок 5 –Объединение интерфейсов в канал и активация LACP на SW 2

```
Switch(config)#interface range fa0/3, fa0/4
Switch(config-if-range)#channel-group 2 mode passive
Switch(config-if-range)#
Creating a port-channel interface Port-channel 2
```

Рисунок 6 – Объединение интерфейсов в канал и активация LACP на SW3

Таблица 3 – Особенности протокола LACP

| Режим (mode) | Описание |
|---|---|
| On | Интерфейсы становятся частью логического канала, но не обмениваются LACP-пакетами |
| LACP Active | Коммутатор активно пытается подключиться к соседу. |
| LACP Passive | Коммутатор пассивно ожидает подключения со стороны соседа. |

Для того чтобы убедиться что все порты объединены, необходимо воспользоваться командой show etherchannel summary (рис. 7 для SW2). Видно, что на данном коммутаторе задействованы 2 канала, которые работают по двум разным протоколам, и какие интерфейсы объединены. Так, Po1(SU) – Port-channel 1 связывает SW1 и SW2 по протоколу PAGP, задействовав интерфейсы Fa0/1 и Fa0/2. Po2(SU) – Port-channel 2, связывает SW2 и SW3 по протоколу LACP, задействовав интерфейсы Fa0/3 и Fa0/4.

```
Switch#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------

1      Po1(SU)           PAgP   Fa0/1(P) Fa0/2(P)
2      Po2(SU)           LACP   Fa0/3(P) Fa0/4(P)
```

Рисунок 7 – Общая информация об агрегированных каналах

### 3 Задание для самостоятельной работы

В качестве самостоятельной работы рассматривается сеть, представленная на рис. 8. Информация, необходимая для конфигурирования оборудования приведена в табл. 4.

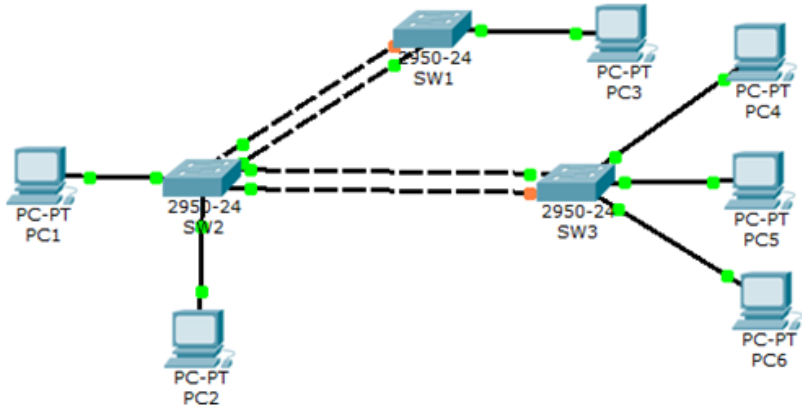



Рисунок 8 – Топология сети

Таблица 4 – Адресация

| Устройство | Интерфейс | IP-адрес | Маска подсети |
|---|---|---|---|
| PC1 | NIC | 192.168.12.1 | 255.255.255.128 |
| PC2 | NIC | 192.168.12.2 | 255.255.255.128 |
| PC3 | NIC | 192.168.12.3 | 255.255.255.128 |
| PC4 | NIC | 192.168.12.4 | 255.255.255.128 |
| PC5 | NIC | 192.168.12.5 | 255.255.255.128 |
| PC6 | NIC | 192.168.12.6 | 255.255.255.128 |
| SW1 | VLAN12 | 192.168.12.11 | 255.255.255.128 |
| SW2 | VLAN12 | 192.168.12.12 | 255.255.255.128 |
| SW3 | VLAN12 | 192.168.12.13 | 255.255.255.128 |

Необходимо:

1. Настроить параметры для каждого коммутатора.
2. Создать VLAN12 и присвоить ему имя “science”.
3. Назначить IP адреса VLAN12 у коммутаторов согласно таблице адресации.
4. Порты на коммутаторах смотрящие в сторону соседнего коммутатора перевести в режим trunk.
5. Порты смотрящие в конечные устройства перевести в режим access.
6. Назначить IP адреса на всех PC согласно адресной таблице.
7. Настроить etherchannel на всех коммутаторах
8. Порты между SW1 и SW2 объединить в канал под номером 6 и включить протокол PAGP.
9. Порты между SW2 и SW3 объединить в канал под номером 7 и включить протокол LACP.
10. Проверить работоспособность сети утилитой ping, с PC1 на PC3, с PC2 на PC4, PC5, PC6.
11. Результаты о проделанной работе показать преподавателю и обосновать результаты.

Далее необходимо проанализировать совместную работы протоколов агрегирования каналов и STP. Для этого требуется реализовать аналогичную схему, показанную на рис. 9.

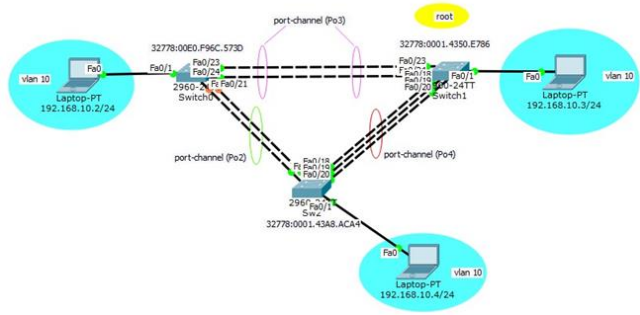



Рисунок 9 – Схема с тремя агрегированными каналами

Необходимо проверить доступность компьютеров в сети с помощью утилиты ping, а также проанализировать работу STP и обосновать индикацию интерфейсов коммутаторов, особое внимание уделить стоимости маршрутов.

Далее требуется усложнить схему и также проанализировать работу протокола STP.

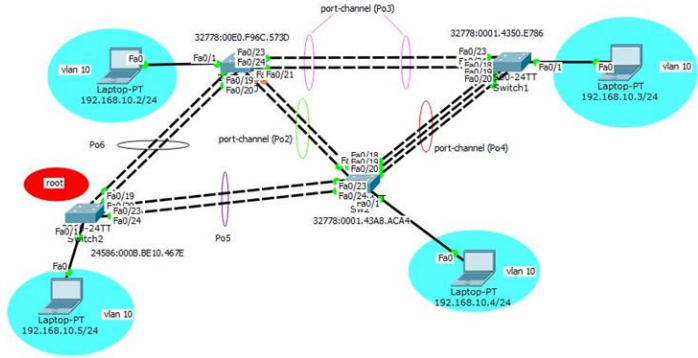



Схема с пятью агрегированными каналами

## 4 Поиск неисправностей

Данная часть работы посвящена поиску неисправностей сети. Исследуемая топология сети представлена на рис. 10. Файл выдается преподавателем. Дано адресное пространство 192.168.99.0/24. Между SW1 и SW2 channel group под номером 2, работающая по протоколу PAgP. Между SW2 и SW3 channel group под номером 1, работающая по

протоколу LACP. Результатом поиска должно являться наличие связи между конечными устройствами.

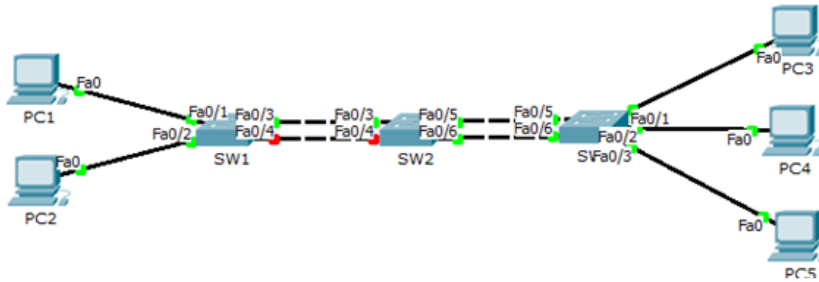



Рисунок 10 – Топология сети

## ЛАБОРАТОРНАЯ РАБОТА №10
## Статическая маршрутизация

### 1 Краткая теоретическая справка

Статические маршруты – это такие маршруты к сетям получателям, которые администратор сети вручную вносит в таблицу маршрутизации. Статический маршрут определяет IP адрес следующего соседнего маршрутизатора или локальный выходной интерфейс, который используется для направления трафика к определенной сети получателю. Как следует из самого названия, статический маршрут не может быть автоматически адаптирован к изменениям в топологии сети. Если определенный в маршруте маршрутизатор или интерфейс становятся недоступными, то маршрут к сети получателю становиться недоступным. Преимуществом этого способа маршрутизации является то, что он исключает весь служебный трафик, связанный с поддержкой и корректировкой маршрутов. Статическая маршрутизация может быть использована в следующих ситуациях:

- администратор нуждается в полном контроле маршрутов используемых маршрутизатором;
- необходимо резервирование динамических маршрутов;
- есть сети достижимые единственно возможным путем;
- нежелательно иметь служебный трафик необходимый для обновления таблиц маршрутизации, например при использовании коммутируемых каналов связи.
- используются устаревшие маршрутизаторы не имеющие необходимого уровня вычислительных возможностей для поддержки динамических протоколов маршрутизации.

Наиболее предпочтительной топологией для использования статической маршрутизации является топология «звезда». При данной топологии маршрутизаторы, подключенные к центральной точки сети, имеют только один маршрут для всего трафика, который будет проходить через центральный узел сети. И один или два маршрутизатора в центральной части сети имеют статические маршруты до всех удаленных узлов. Однако со временем такая сеть может вырасти до десятков и сотен маршрутизаторов с произвольным количеством подключенных к ним подсетей. Количество статических маршрутов в таблицах маршрутизации будет увеличиваться пропорционально увеличению количества маршрутизаторов в сети. Каждый раз при добавлении новой подсети или маршрутизатора, администратор должен будет добавлять новые маршруты в таблицы маршрутизации на всех

необходимых маршрутизаторах. При таком подходе может наступить момент, когда большую часть своего рабочего времени администратор будет заниматься поддержкой таблиц маршрутизации в сети. В этом случае необходимо сделать выбор в сторону использования динамических протоколов маршрутизации. Другой недостаток статической маршрутизации проявляется при изменении топологии корпоративной сети. При этом администратор должен вручную вносить все изменения в таблицы маршрутизации маршрутизаторов, на которые повлияли изменения в топологии сети.

## 2 Последовательность выполнения работы

Для выполнения данной лабораторной работы необходимо знать IP адресацию IPv4, принцип статической маршрутизации и базовые навыки конфигурации маршрутизаторов.

Цель – изучение принципов статической маршрутизации.

Необходимо организовать физическую топологию, аналогичную, представленной на рис. 1. Далее выполнять необходимые настройки только тогда, когда это явно указано в описательной части работы. Требуемая адресация приведена в табл. 1.

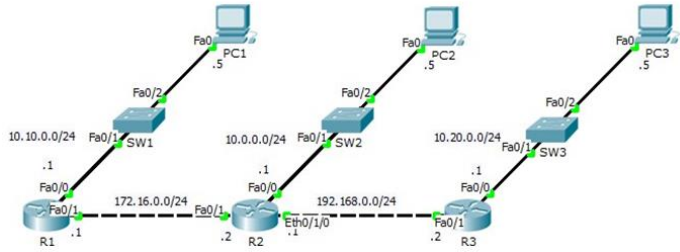



Рисунок 1 – Топология сети

Таблица 1 – Адресация (маска подсети – /24)

| Устройство | Интерфейс | IP адрес | Шлюз по умолчанию |
|---|---|---|---|
| PC1 | Fa0 | 10.10.0.5 | 10.10.0.1 |
| PC2 | Fa0 | 10.0.0.5 | 10.0.0.1 |
| PC3 | Fa0 | 10.20.0.5 | 10.20.0.1 |
| R1 | Fa0/0 | 10.10.0.1 | |

| | | | |
|---|---|---|---|
| R1 | Fa0/1 | 172.16.0.1 | |
| R2 | Fa0/1 | 172.16.0.2 | |
| R2 | Fa0/0 | 10.0.0.1 | |
| R2 | Fa0/1/0 | 192.168.0.1 | |
| R3 | Fa0/1 | 192.168.0.2 | |
| R3 | Fa0/0 | 10.20.0.1 | |

Установка дополнительных Ethernet разъемов для R2. Перед установкой дополнительного разъема, необходимо отключить устройство, нажав на кнопку включения/выключения, далее необходимо перетащить из левого столбца, который содержит в себе различные дополнительные карты, карту WIC-1T в свободный слот на маршрутизаторе (рис. 2). Включить устройство.


Рисунок 2 – Установка дополнительных портов

Назначить IP адреса интерфейсам на R1, R2 и R3.

```
R1>enable
R1#conft
R1(config)#interface fastethernet 0/0
R1(config-if)#ip address 10.10.0.1 255.255.255.0
R1(config-if)#no shutdown
```

Аналогичным образом, назначить ip адреса на всех интерфейсах, согласно таблица адресации. Назначить IP адреса на ПК. Ввод статического маршрута на R1.

Данная команда работает по принципу куда - откуда, R1(config)#ip route (удаленная сеть) (маска удаленной сети) (IP-адрес подключенного интерфейса следующего роутера)

```
R1(config)#ip route 10.0.0.0 255.255.255.0 172.16.0.2
R1(config)#ip route 192.168.0.0 255.255.255.0 172.16.0.2
R1#ip route 10.20.0.0 255.255.255.0 172.16.0.2
```

Ввод статического маршрута на R2.

```
Router(config)#ip route 10.10.0.0 255.255.255.0 172.16.0.1
Router(config)#ip route 10.20.0.0 255.255.255.0 192.168.0.2
```

Ввод статического маршрута на R3.

```
Router(config)#ip route 10.10.0.0 255.255.255.0 192.168.0.1
Router(config)#ip route 10.0.0.0 255.255.255.0 192.168.0.1
Router(config)#ip route 172.16.0.0 255.255.255.0 192.168.0.1
```

Проверить правильности конфигурации статических маршрутов путем использования утилиты ping. В случае отсутствия связи проверить правильность выполненных настрое.

### 3 Задание для самостоятельной работы

Необходимо организовать сеть, аналогичную, представленной на рис. 3. Необходимая инфорсация по адресации приведена в табл. 2.

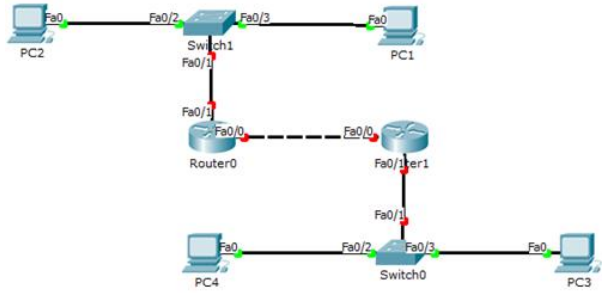



Рисунок 3 – Топология сети

Таблица 2 – Адресация

| **Устройство** | **Интерфейс** | **IP адрес** | **Маска подсети** | **Шлюз по умолчанию** |
|---|---|---|---|---|
| PC1 | Fa0 | 192.168.100.25 | 255.255.255.224 | 192.168.100.1 |
| PC2 | Fa0 | 192.168.100.26 | 255.255.255.224 | 192.168.100.1 |
| PC3 | Fa0 | 192.168.200.25 | 255.255.255.224 | 192.168.200.1 |
| PC4 | Fa0/0 | 192.168.200.26 | 255.255.255.224 | 192.168.200.1 |
| Router0 | Fa0/1 | 192.168.100.1 | 255.255.255.224 | |
| Router0 | Fa0/0 | 172.16.16.1 | 255.255.255.0 | |

| | | | | |
|---|---|---|---|---|
| Router1 | Fa0/1 | 192.168.200.1 | 255.255.255.0 | |
| Router1 | Fa0/0 | 172.16.16.2 | 255.255.255.0 | |

Необходимо:

1. Назначить IP адреса интерфейсам на Router0 и Router1.
2. Назначить IP адреса на ПК.
3. Назначить статический маршрут на Router0.
4. Назначить статический маршрут на Router 1.
5. Проверить правильности конфигурации маршрутов путем использования утилиты ping.
6. Результаты о проделанной работе показать преподавателю и обосновать результаты.

## 4 Поиск неисправностей

Данная часть работы посвящена поиску неисправностей сети. Требуемая топология сети приведена на рис. 4. Файл выдается преподавателем. Дано четыре адресных пространства 192.168.0.0, 192.168.100.0 172.16.0.0 и 172.16.100.0. Маска подсети для них – 255.255.255.0. Результатом поиска неисправностей должно являться наличие связи между конечными устройствами.

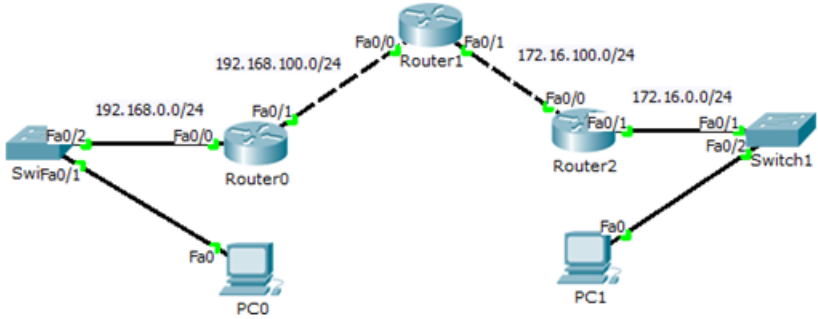



Рисунок 4 – Топология сети

## ЛАБОРАТОРНАЯ РАБОТА №11
## Динамическая маршрутизация: RIP

### 1 Краткая теоретическая справка

Протокол маршрутной информации (Routing Informational Protocol – RIP) был первоначально определен в документе RFC 1058. Наиболее существенны следующие его характеристики:

• является дистанционно-векторным протоколом маршрутизации;

• в качестве метрики при выборе маршрута используется количество переходов;

• максимальная длина маршрута равняется 15 переходам;

• по умолчанию обновления маршрутной информации рассылаются широковещательным способом.

При работе протокола RIP используется транспортный протокол UDP. Все устройства, поддерживающие RIP, прослушивают UDP порт 520 и осуществляют передачу через этот же порт. В сетях общего доступа, таких как Ethernet, эти широковещательные дейтаграммы получают все устройства широковещательного домена. Протокол RIP использует расстояние как единственную метрику для определения наилучшего маршрута, т.е. чем короче маршрут, тем он лучше. Если к пункту назначения существует множество маршрутов, то маршрутизаторы поддерживающие протокол RIP, выбирают из них кротчайший и записывают его в таблицу маршрутизации.

Протокол RIP предотвращает появление петель в маршрутизации, устанавливая максимальное количество переходов на маршруте от отправителя к получателю. Стандартное максимальное значение количества переходов равно 15. При получении маршрутизатором обновления маршрутной информации, содержащего новую или измененную запись, он увеличивает значение метрики на единицу. Если при этом значение метрики превышает 15, то метрика считается бесконечно большой, а маршрут до сети получателя недостижимым. Кроме этого чтобы повысить эффективность работы протокол RIP использует механизмы расщепления горизонта и таймеры удержания информации.

### 2 Последовательность выполнения работы

Для выполнения данной лабораторной работы необходимо знать IP адресацию IPv4, принцип динамической маршрутизации с использованием протокола RIP и базовые навыки конфигурации маршрутизаторов.

Цель – изучение принципов динамической маршрутизации на примере протокола RIP.

Необходимо организовать сеть, аналогичную, представленной на рис. 1.

Используется маршрутизаторы модели 2911. Далее выполнять необходимые настройки только тогда, когда это явно указано в описательной части работы. Требуемая адресация приведена в табл. 1.

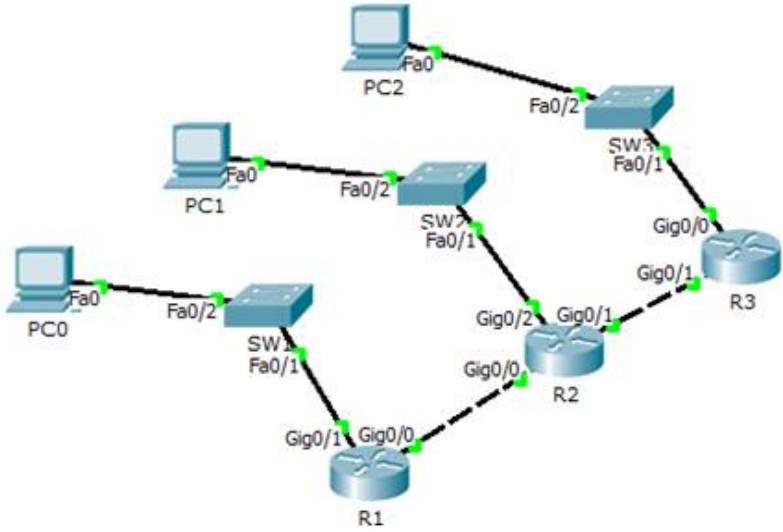



Рисунок 1 – Топология сети

Таблица 1 – Адресация

| Устройство | Интерфейс | IP адрес | Маска подсети | Шлюз по молчанию |
|---|---|---|---|---|
| PC0 | Fa0 | 172.16.0.29 | 255.255.255.224 | 172.16.0.1 |
| PC1 | Fa0 | 192.168.0.29 | 255.255.255.224 | 192.168.0.1 |
| PC2 | Fa0 | 10.16.0.29 | 255.255.255.224 | 10.16.0.1 |
| R1 | Gig0/1 | 172.16.0.1 | 255.255.255.224 | |
| R2 | Gig0/2 | 192.168.0.1 | 255.255.255.224 | |
| R3 | Gig0/0 | 10.16.0.1 | 255.255.255.224 | |
| R1 | Gig0/0 | 10.100.0.1 | 255.255.255.0 | |

| | | | | |
|---|---|---|---|---|
| R2 | Gig0/0 | 10.100.0.2 | 255.255.255.0 | |
| R2 | Gig0/1 | 10.200.0.1 | 255.255.255.0 | |
| R3 | Gig0/1 | 10.200.0.2 | 255.255.255.0 | |

Первоначально требуется назначить IP адреса всем ПК. Далее назначить IP адреса на интерфейсах маршрутизатора согласно таблице адресации (табл. 1).

```
Router1>enable
Router1#configure terminal
Router1(config)#interface Gig0/1
Router1(config-if)#ip address 172.16.0.1 255.255.255.224
Router1(config-if)#no shutdown
```

Аналогичным образом назначить IP-адреса остальным маршрутизаторам. Активировать протокол RIP и настроить его на R1.

```
R1#conf t
режим настройки RIP
R1(config)#router rip
выбор версии 2
R1(config-router)#version 2
добавление присоединенной сети
R1(config-router)#network 172.16.0.0
R1(config-router)#network 10.100.0.0
отключение автосуммаризации
R1(config-router)#no auto-summary
```

Включить протокол RIP и настроить его на R2.

```
Router#conf t
```

```
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 10.100.0.0
Router(config-router)#network 192.168.0.0
Router(config-router)#network 10.200.0.0
Router(config-router)#no auto-summary
```

Включить протокол RIP и настроить его на R3.

```
Router#conf t
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 10.200.0.0
Router(config-router)#network 10.16.0.0
Router(config-router)#no auto-summary
```

Стоит помнить, что добавление сетей в процесс RIP1 осуществляется заданием classful network, а не подсети. Таким образом, например, правильно 172.16.0.0, а не 172.16.10.0.

Проверить содержимое таблицы маршрутизации R1.

```
Router#show ip route
```

Рассмотрим результат выполнения команды.

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 4 subnets, 3 masks
R       10.16.0.0/27 [120/2] via 10.100.0.2, 00:00:00, GigabitEthernet0/0
C       10.100.0.0/24 is directly connected, GigabitEthernet0/0
L       10.100.0.1/32 is directly connected, GigabitEthernet0/0
R       10.200.0.0/24 [120/1] via 10.100.0.2, 00:00:00, GigabitEthernet0/0
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.0.0/27 is directly connected, GigabitEthernet0/1
L       172.16.0.1/32 is directly connected, GigabitEthernet0/1
R    192.168.0.0/24 [120/1] via 10.100.0.2, 00:00:00, GigabitEthernet0/0
```

Видно, что к маршрутизатору R1, присоединены 3 сети с использованием протокола RIP. Далее необходимо проверить доступность между хостами. В случае различия таблиц и отсутствия связи проверить правильность настроек.

## 3 Задание для самостоятельной работы

Необходимо организовать физическую топологию, аналогичную, представленной на рис. 2. Требуемая адресация приведена в табл. 2.

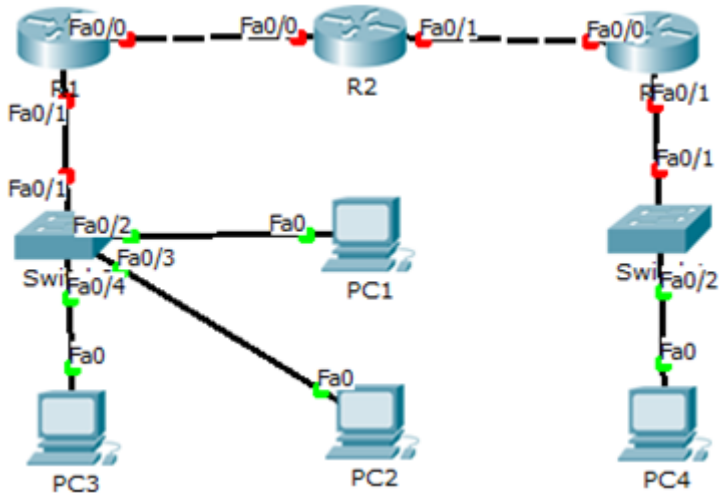



Рисунок 2 – Топология сети

Таблица 2 – Адресация

| **Устройство** | **Интерфейс** | **IP адрес** | **Маска подсети** | **Шлюз открытой сети** |
|---|---|---|---|---|
| PC1 | Fa0 | 89.74.112.11 | 255.255.255.0 | 89.74.112.1 |
| PC2 | Fa0 | 89.74.112.21 | 255.255.255.0 | 89.74.112.1 |
| PC3 | Fa0 | 89.74.112.31 | 255.255.255.0 | 89.74.112.1 |
| PC4 | Fa0 | 112.99.14.41 | 255.255.255.0 | 112.99.14.41 |
| R1 | Fa0/1 | 89.74.112.1 | 255.255.255.0 | |
| R1 | Fa0/0 | 172.16.0.1 | 255.255.255.0 | |
| R2 | Fa0/0 | 172.16.0.2 | 255.255.255.0 | |
| R2 | Fa0/1 | 192.168.0.1 | 255.255.255.0 | |
| R3 | Fa0/0 | 112.99.14.1 | 255.255.255.0 | |

Необходимо:

1. Назначить всем PC IP-адреса.
2. Назначить IP-адреса на интерфейсах маршрутизатора согласно требуемой адресации.
3. Включить и настроить протокол RIP на R1.
4. Включить и настроить протокол RIP на R2.
5. Включить и настроить протокол RIP на R3.

6. Проверить таблицы маршрутизации.

7. Проверить доступность между хостами.

8. Результаты о проделанной работе показать преподавателю и обосновать результаты.

## ЛАБОРАТОРНАЯ РАБОТА №12
## Динамическая маршрутизация: OSPF

### 1 Краткая теоретическая справка

OSPF (Open Shortest Path First) – протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала (link-state technology) и использующий для нахождения кратчайшего пути алгоритм Дейкстры. Разработан в 1988 году (последняя версия представлена в RFC 2328). Протокол является протоколом внутреннего шлюза, распространяющим информацию о доступных маршрутах между маршрутизаторами одной автономной системы. Используются следующие термины:

- Объявление о состоянии канала (link-state advertisement, LSA) – объявление описывает все каналы маршрутизатора, все интерфейсы и состояния каналов.
- Состояние канала (link state) – состояние канала между двумя маршрутизаторами.
- Метрика (metric) – условный показатель «стоимости» пересылки данных по каналу;
- Автономная система (autonomous system) – группа маршрутизаторов, обменивающихся маршрутной информацией.
- Зона (area) – совокупность сетей и маршрутизаторов, имеющих один и тот же идентификатор зоны.
- Соседи (neighbours) – два маршрутизатора, имеющие интерфейсы в общей сети.
- Состояние смежности (adjacency) – взаимосвязь между определёнными соседними маршрутизаторами, установленная с целью обмена информацией маршрутизации.
- Hello-протокол (hello protocol) – используется для поддержания соседских отношений.
- База данных соседей (neighbours database) – список всех соседей.
- База данных состояния каналов (link state database, LSDB) – список всех записей о состоянии каналов.
- Идентификатор маршрутизатора (router ID, RID) – уникальное 32-битовое число, которое уникально идентифицирует маршрутизатор в пределах одной автономной системы.

Принцип работы:

1. Маршрутизаторы обмениваются hello-пакетами через все интерфейсы, на которых активирован OSPF. Маршрутизаторы,

разделяющие общий канал передачи данных, становятся соседями, когда они приходят к договоренности об определённых параметрах, указанных в их hello-пакетах.

2. На следующем этапе работы протокола маршрутизаторы будут пытаться перейти в состояние смежности со своими соседями. Переход в состояние смежности определяется типом маршрутизаторов, обменивающихся hello-пакетами, и типом сети, по которой передаются hello-пакеты. OSPF определяет несколько типов сетей и несколько типов маршрутизаторов. Пара маршрутизаторов, находящихся в состоянии смежности, синхронизирует между собой базу данных состояния каналов.

3. Каждый маршрутизатор посылает объявления о состоянии канала маршрутизаторам, с которыми он находится в состоянии смежности.

4. Каждый маршрутизатор, получивший объявление от смежного маршрутизатора, записывает передаваемую в нём информацию в базу данных состояния каналов маршрутизатора и рассылает копию объявления всем другим смежным с ним маршрутизаторам.

5. Рассылая объявления внутри одной OSPF-зоны, все маршрутизаторы строят идентичную базу данных состояния каналов маршрутизатора.

6. Когда база данных построена, каждый маршрутизатор использует алгоритм «кратчайший путь первым» для вычисления графа без потерь, который будет описывать кратчайший путь к каждому известному пункту назначения с собой в качестве корня. Этот граф — дерево кратчайших путей.

7. Каждый маршрутизатор строит таблицу маршрутизации из своего дерева кратчайших путей.

## 2 Последовательность выполнения работы

Для выполнения данной лабораторной работы необходимо знать IP адресацию IPv4, принцип динамической маршрутизации с использованием протокола OSPF и базовые навыки конфигурации маршрутизаторов.

Цель – изучение принципов динамической маршрутизации на примере протокола OSPF.

Необходимо организовать физическую топологию, аналогичную, представленной на рис. 1. Требуемая адресация приведена в табл. 1. Выполнять необходимые настройки требуется только тогда, когда это явно указано в описательной части работы.

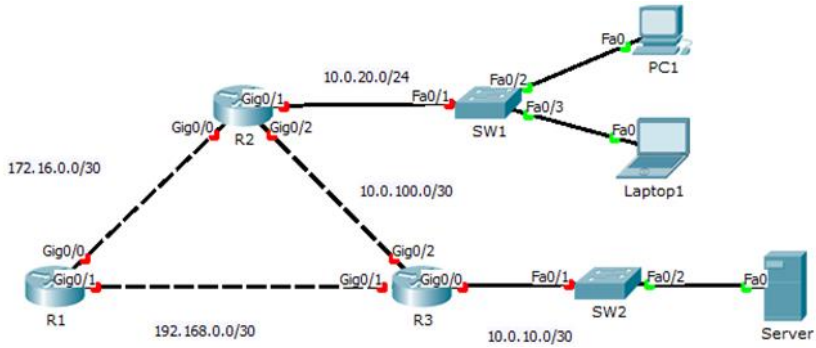



Рисунок 1 – Топология сети

Таблица 1 – Адресация

| Устройство | Интерфейс | IP - адрес | Маска подсети |
|---|---|---|---|
| R1 | Gig0/0 | 172.16.0.1 | 255.255.255.252 |
| R1 | Gig0/1 | 192.168.0.1 | 255.255.255.252 |
| R2 | Gig0/0 | 172.16.0.2 | 255.255.255.252 |
| R2 | Gig0/1 | 10.0.20.1 | 255.255.255.0 |
| R2 | Gig0/2 | 10.0.100.1 | 255.255.255.252 |
| R3 | Gig0/0 | 10.0.10.1 | 255.255.255.252 |
| R3 | Gig0/1 | 192.168.0.2 | 255.255.255.252 |
| R3 | Gig0/2 | 10.0.100.2 | 255.255.255.252 |
| PC1 | Fa0 | 10.0.20.10 | 255.255.255.0 |
| Laptop | Fa0 | 10.0.20.12 | 255.255.255.0 |
| Server | Fa0 | 10.0.10.2 | 255.255.255.0 |

Настроить IP адресацию на маршрутизаторах согласно плану адресации. Проверить выполненные настройки командой show ip interface brief.

```
Router#show ip route
Router#show ip interface brief
```

Назначить IP адреса PC. Настроить протокол динамической маршрутизации OSPF на маршрутизаторе R1.

```
Router#conf term
включение OSPF, значение в диапазоне 1– 65535
идентифицирует номер процесса
Router(config)#router ospf 1
указание присоединенных сетей с обратной маской
Router(config-router)#network 192.168.0.0 0.0.0.3 area 0
Router(config-router)#network 172.16.0.0 0.0.0.3 area 0
```

Настроить протокол динамической маршрутизации OSPF на маршрутизаторе R2.

```
Router#conf term
Router(config)#router ospf 1
Router(config-router)#network 172.16.0.0 0.0.0.3 area 0
Router(config-router)#network 10.0.20.0 0.0.0.255 area 0
Router(config-router)#network 10.0.100.0 0.0.0.3 area 0
```

Настроить протокол динамической маршрутизации OSPF на маршрутизаторе R3.

```
Router#conf term
Router(config)#router ospf 1
Router(config-router)#network 10.0.100.0 0.0.0.3 area 0
Router(config-router)#netwrok 192.168.0.0 0.0.0.3 area 0
Router(config-router)#network 10.0.10.0 0.0.0.3 area 0
```

Настроить router-id на маршрутизаторе R1.

```
Router#conf term
Router(config)#router ospf 1
задание ID маршрутизатора, в противном случае он будет
присвоен автоматически, наибольший IP-адрес из всех
активных интерфейсов будет Router ID
Router(config-router)#router-id 1.1.1.1
Router(config-router)#Reload or use "clear ip ospf process"
command, for this to take effect
Router(config-router)#exit
Router(config)#exit
перезагрузка процесса OSPF, для того чтобы изменения
вступили в силу
Router#clear ip ospf process
Reset ALL OSPF processes? [no]: yes
```

Настроить router-id на маршрутизаторе R2.

```
Router#conf term
Router(config)#router ospf 1
Router(config-router)#router-id 2.2.2.2
Router(config-router)#Reload or use "clear ip ospf process"
command, for this to take effect
Router(config-router)#exit
Router(config)#exit
Router#clear ip ospf process Reset ALL OSPF processes? [no]: yes
```

Настроить router-id на маршрутизаторе R3.

```
Router#conf term
Router(config)#router ospf 1
Router(config-router)#router-id 3.3.3.3
Router(config-router)#Reload or use "clear ip ospf process"
command, for this to take effect
Router(config-router)#exit
Router(config)#exit
Router#clear ip ospf process Reset ALL OSPF processes? [no]: yes
```

Проверить установления соседства с помощью show ip ospf neighbor. Результат показан на рис. 2.

```
R1$show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
3.3.3.3           1   FULL/DR         00:00:31    192.168.0.2     GigabitEtherne
t0/1
2.2.2.2           1   FULL/DROTHER    00:00:35    172.16.0.2      GigabitEtherne
t0/0
```

Рисунок 2 – Результат команды show ip ospf neighbor

Далее установить пассивный интерфейс на маршрутизаторе R2.

```
Router#conf term
Router(config)#router ospf 1
включить интерфейс, «смотрящий» в пользовательскую сеть
в процесс маршрутизации, но запретить пересылать на него
апдейты
Router(config-router)#passive-interface  gig0/1  //
```

Аналогично установить пассивный интерфейс на маршрутизаторе R3. После чего проверить работоспособность сети путем использования утилиты ping. Если связь отсутствует, то проверить настройки.

## 3 Задание для самостоятельной работы

Организовать физическую топологию, аналогичную, представленной на рис. 3. Требуемая адресация приведена в табл. 2.

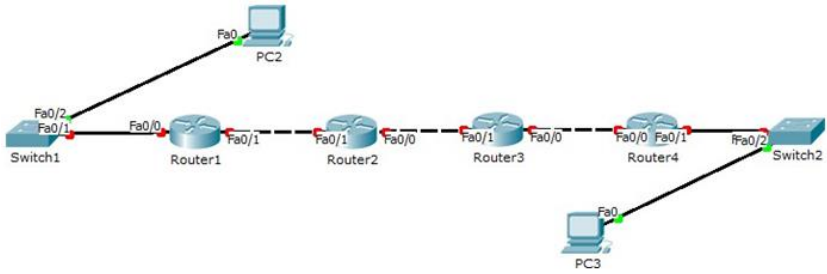



Рисунок 3 – Топология сети

Таблица 2 – Адресация

| Устройство | Интерфейс | IP - адрес | Маска подсети |
|---|---|---|---|
| Router1 | Fa0/0 | 66.91.104.1 | 255.255.255.0 |
| Router1 | Fa0/1 | 192.168.20.1 | 255.255.255.252 |
| Router2 | Fa0/1 | 192.168.20.2 | 255.255.255.252 |
| Router2 | Fa0/0 | 172.16.10.1 | 255.255.255.252 |
| Router3 | Fa0/1 | 172.16.10.2 | 255.255.255.252 |

| | | | |
|---|---|---|---|
| Router3 | Fa0/0 | 172.16.20.1 | 255.255.255.252 |
| Router4 | Fa0/0 | 172.16.20.2 | 255.255.255.252 |
| Router4 | Fa0/1 | 89.101.14.1 | 255.255.255.0 |
| PC2 | Fa0 | 66.91.104.10 | 255.255.255.0 |
| PC3 | Fa0 | 89.101.14.2 | 255.255.255.0 |

Необходимо:

1. Настроить IP адресацию на маршрутизаторах согласно плану адресации.
2. Назначить IP адреса PC согласно плану адресации.
3. Настроить протокол динамической маршрутизации OSPF на маршрутизаторах
4. Настроить router-id на маршрутизаторах.
5. Установить пассивный интерфейс на маршрутизаторе Router1
6. Установить пассивный интерфейс на маршрутизаторе Router4
7. Проверить работоспособность сети путем использования утилиты ping.
8. Результаты о проделанной работе показать преподавателю и обосновать результаты.

## 4 Поиск неисправностей

Данная часть работы посвящена поиску неисправностей сети. Требуемая топология сети приведена на рис. 4. Файл выдается преподавателем. Дано четыре адресных пространства 192.168.0.0, 192.168.100.0, 172.16.100.0 и 172.16.0.0. Маска подсети для них – 255.255.255.0. Результатом поиска неисправностей должно являться наличие связи между конечными устройствами.

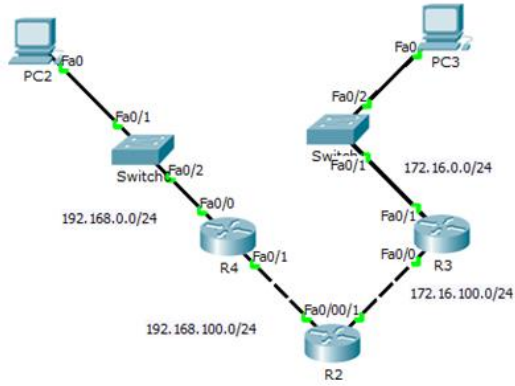



Рисунок 4 – Топология сети

## ЛАБОРАТОРНАЯ РАБОТА №13
## Динамическая маршрутизация: BGP

### 1 Краткая теоретическая справка

BGP (Border Gateway Protocol, протокол граничного шлюза) – динамический протокол маршрутизации. Относится к классу протоколов маршрутизации внешнего шлюза (EGP – External Gateway Protocol). На текущий момент является основным протоколом динамической маршрутизации в сети Интернет.

Протокол BGP предназначен для обмена информацией о достижимости подсетей между автономными системами (АС, англ. AS – autonomous system), то есть группами маршрутизаторов под единым техническим и административным управлением, использующими протокол внутридоменной маршрутизации для определения маршрутов внутри себя и протокол междоменной маршрутизации для определения маршрутов доставки пакетов в другие АС. Передаваемая информация включает в себя список АС, к которым имеется доступ через данную систему. Выбор наилучших маршрутов осуществляет исходя из правил, принятых в сети.

BGP поддерживает бесклассовую адресацию и использует суммирование маршрутов для уменьшения таблиц маршрутизации. С 1994 года действует четвёртая версия протокола, все предыдущие версии являются устаревшими.

BGP, наряду с DNS, является одним из главных механизмов, обеспечивающих функционирование Интернета. BGP является протоколом сетевого уровня и функционирует под протоколом транспортного уровня TCP (порт 179). После установки соединения передаётся информация обо всех маршрутах, предназначенных для экспорта. В дальнейшем передаётся только информация об изменениях в таблицах маршрутизации. При закрытии соединения удаляются все маршруты, информация о которых передана противоположной стороной.

Сообщение BGP начинается с заголовка, после которого, в зависимости от типа сообщения, могут следовать данные. Максимальная длина сообщения – 4096 октетов, минимальная – 19 октетов. Заголовок сообщения содержит следующие поля:

• Маркер (16 октетов) – используется для совместимости, должен быть заполнен единицами;

• Длина (2 октета) – длина сообщения в октетах, включая заголовок;

• Тип (1 октет):

o 1 – Открытие;

o 2 – Обновление информации;

o 3 – Оповещение;

o 4 – Сохранение соединения.

Первое сообщение после установки соединения должно быть «Открытие». Если сообщение успешно обработано, в ответ будет послано «Сохранение соединения». В дополнение к заголовку BGP сообщение «Открытие» содержит следующие поля:

• Версия (1 октет) – версия протокола, текущее значение 4;

• Моя система (2 октета) – номер автономной системы;

• Интервал времени (2 октета) – максимальный интервал времени в секундах между получением сообщений «Обновление информации» или «Сохранение соединения»;

• Идентификатор отправителя (4 октета) – устанавливается равным IP-адресу;

• Длина дополнительных параметров (1 октет);

• Дополнительные параметры:

o Тип параметра (1 октет);

o Длина параметра (1 октет);

o Значение параметра.

Сообщение «Обновление информации» предназначено для передачи информации о маршрутах между АС. Сообщение может указывать новые маршруты и удалять неработающие. Структура сообщения:

• Длина удаляемых маршрутов (2 октета);

• Удаляемые маршруты:

o Длина (1 октет) – длина в битах префикса IP-адреса;

o Префикс IP-адреса, дополненный минимальным количеством бит до полного октета;

• Длина атрибутов пути (2 октета);

• Атрибуты пути:

o Тип атрибута:

- Флаг атрибута;
- Код атрибута;

o Длина атрибута (1 или 2 октета, в зависимости от флага);

o Данные атрибута;

• Информация о достижимости – список префиксов IP-адресов:

o Длина (1 октет) – длина в битах префикса IP-адреса (нулевая длина – соответствие всем IP-адресам);

o Префикс IP-адреса, дополненный минимальным количеством бит до полного октета.

Все атрибуты пути соответствуют всем записям в поле «Информация о достижимости».

Сообщение сохранения соединения должно посылаться не реже чем раз в одну третью часть максимального интервала времени между сообщениями, но не чаще чем один раз в секунду. Если интервал времени установлен равным нулю, то сообщение не должно периодически рассылаться. Сообщение не использует дополнительных полей.

Оповещение посылается в случае обнаружения ошибки, при этом соединение закрывается. Сообщение содержит следующие поля:

- Код ошибки (1 октет);
- Субкод (1 октет);
- Данные.

Для выполнения данной лабораторной работы необходимо знать IP адресацию IPv4, принцип динамической маршрутизации с использованием протокола BGP и базовые навыки конфигурации маршрутизаторов.

Цель – изучение принципов динамической маршрутизации на примере протокола BGP.

## 2 Последовательность выполнения работы

Необходимо организовать физическую топологию, аналогичную, представленной на рис. 1. Требуемая адресация приведена в табл. 1. Выполнять необходимые настройки необходимо только тогда, когда это явно указано в описательной части работы.

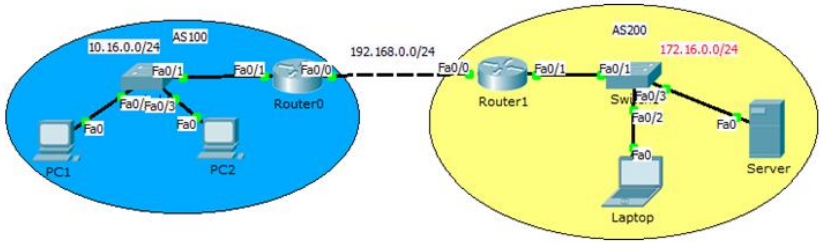



Рисунок 1– Топология сети

Таблица 1 – Адресация

| Устройство | Интер | IP адрес | Маска | Шлюз по |
|---|---|---|---|---|

| | фейс | | подсети | умолчанию |
|---|---|---|---|---|
| Router0(AS100) | Fa0/1 | 10.16.0.1 | 255.255.255.0 | |
| Router0(AS200) | Fa0/0 | 192.168.0.1 | 255.255.255.0 | |
| Router1(AS200) | Fa0/0 | 192.168.0.2 | 255.255.255.0 | |
| Router1(AS200) | Fa0/1 | 172.16.0.1 | 255.255.255.0 | |
| PC1 | Fa0 | 10.16.0.2 | 255.255.255.0 | 10.16.0.1 |
| PC2 | Fa0 | 10.16.0.3 | 255.255.255.0 | 10.16.0.1 |
| Laptop | Fa0 | 172.16.0.2 | 255.255.255.0 | 172.16.0.1 |
| Server | Fa0 | 172.16.0.3 | 255.255.255.0 | 172.16.0.1 |

Назначить IP адреса интерфейсам маршрутизаторов. Назначить IP адреса устройствам PC, Laptop и Server. Создать процесс BGP на Router0.

```
Router#conf term
<1-65535> номер автономной системы, которой
принадлежит локальный маршрутизатор (приватный
диапазон 64512-65535). На основании его сравнения с
номерами автономных систем соседей, маршрутизатор
будет использовать iBGP или eBGP.
Router(config)#router bgp 100
```

Создать процесс BGP на Router1.

```
Router#conf term
Router(config)#router bgp 200
```

На Router0 указать соседа.

```
Router#conf term
Router(config)#router bgp 100
ip-address – идентифицирует соседний маршрутизатор, а
remote-as <as-number> – номер автономной системы соседа
Router(config-router)#neighbor 192.168.0.2 remote-as 200
```

Аналогично на Router1 указать соседа.

```
Router(config)#router bgp 200
Router(config-router)#neighbor 192.168.0.1 remote-as 100
```

На Router0 указать какие сети необходимо анонсировать по протоколу BGP.

```
Router(config)#router bgp 100
Указать какой prefix будет анонсироваться из AS
Router(config-router)#network 10.16.0.0 mask 255.255.255.0
```

Аналогично указать на Router1.

```
Router(config)#router bgp 200
Router(config-router)#network 172.16.0.0 mask 255.255.255.0
```

Проверить содержимое таблицы маршрутизации Router0.

```
Router#show ip route
```

Рассмотрим результат выполнения команды.

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
C       10.16.0.0 is directly connected, FastEthernet0/1
     172.16.0.0/24 is subnetted, 1 subnets
B       172.16.0.0 [20/0] via 192.168.0.2, 01:05:15
C    192.168.0.0/24 is directly connected, FastEthernet0/0
```

Видно, что к данному маршрутизатору R1, присоединены 3 сети по протоколу RIP.

Аналогично проверить таблицу маршрутизации Router1 и затем проверить работоспособность сети, путем использования утилиты ping. Если связь отсутствует, то проверить настройки.

### 3 Задание для самостоятельной работы

Организовать физическую топологию, аналогичную, представленной на рис. 11.

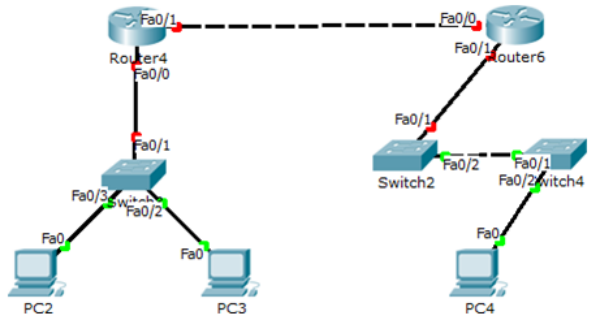



Рисунок 2 – Топология сети

Таблица 2– Таблица адресации

| Устройство | Интерфейс | IP адрес | Маска подсети | Шлюз по умолчанию |
|---|---|---|---|---|
| Router4(AS11) | Fa0/0 | 10.16.0.1 | 255.255.255.0 | |
| Router4(AS11) | Fa0/1 | 169.254.0.1 | 255.255.255.0 | |
| Router6(AS89) | Fa0/0 | 169.254.0.2 | 255.255.255.0 | |
| Router6(AS289) | Fa0/1 | 129.213.11.1 | 255.255.255.0 | |
| PC2 | Fa0 | 10.16.0.12 | 255.255.255.0 | 10.16.0.1 |
| PC3 | Fa0 | 10.16.0.13 | 255.255.255.0 | 10.16.0.1 |
| PC4 | Fa0 | 129.213.11.10 | 255.255.255.0 | 129.213.11.1 |

Необходимо:

1. Назначить IP адреса интерфейсам маршрутизаторов.
2. Назначить IP адреса всем ПК.
3. Запустить процесс BGP на Router4 и Router6.
4. Указать соседа на Router4 и Router6.
5. Указать какие сети анонсировать по протоколу BGP на Router4 и Router6.
6. Проверить таблицы маршрутизации.
7. Проверить работоспособность сети, путем использования утилиты ping.
8. Результаты о проделанной работе показать преподавателю и обосновать результаты.

## 4 Поиск неисправностей

Данная часть работы посвящена поиску неисправностей сети. Требуемая топология сети приведена на рис. 2. Файл выдается преподавателем. Дано три адресных пространства 192.168.0.0,

192.168.100.0 и 172.16.0.0. Маска подсети для них – 255.255.255.0. Две автономные системы под номером 150 и 250. Во всех сегментах сети первые адреса назначаются интерфейсам маршрутизаторов, а адреса на PC назначаются администратором исходя из адресного пространства на его усмотрение. Результатом поиска неисправностей, должно являться наличие связи между конечными устройствами.

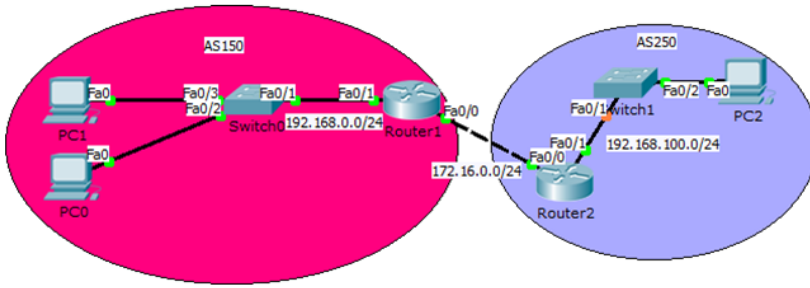



Рисунок 2 – Топология сети

## ЛАБОРАТОРНАЯ РАБОТА №14
## DHCP сервер на маршрутизаторе

### 1 Краткая теоретическая справка

Протокол DHCP – позволяет производить автоматическую настройку сети на компьютерах и других устройствах. DHCP может быть настроен на маршрутизаторах или на базе любого сервера. DCHP позволяет автоматически настраивать на клиенте следующие основные параметры:

1. IP адрес.
2. Основной шлюз.
3. Маска подсети.
4. DNS сервера.
5. Имя домена.

Это наиболее частое использование DHCP, но можно передавать и огромное количество других параметров. Например, можно передавать дополнительные маршруты, чтобы в разные сети компьютер ходил через разные шлюзы. Или, с помощью DHCP можно организовывать загрузку устройств по сети.

Когда клиент, например обычный компьютер, запускается, ОС видит, что для некой сетевой карты стоит «Получить параметры по DHCP». Такой компьютер не имеет пока IP адреса и происходит следующая процедура получения:

1. Компьютер отправляет широковещательный запрос. Такое DHCP сообщение называется «DHCP discover».

2. Далее все устройства в сети получают это широковещательное сообщение. DHCP сервера (если их несколько) отвечают клиенту. Сервер резервирует в своём пуле адресов какой-то адрес и выделяет этот IP-адрес клиенту на какое-то время (lease time). Добавляются другие настройки и всё вместе высылается. При этом в качестве адресов получателя используется уже новый, выделенный IP-адрес. Это называется

«DHCP offer».

3. Клиент выбирает сервер, как правило, который ответил первым, и отправляет «DHCP request» – согласие с полученными параметрами.

4. Сервер резервирует за клиентом выделенный адрес на какое-то время (lease time). До этого момента адрес был выделен, но не зарезервирован. Теперь же он окончательно закреплён за клиентом.

Сервер вносит так же строчку в свою ARP таблицу и высылает клиенту, сообщение, что он успешно зарегистрирован – «DCHP Acknowledge».

## 2 Последовательность выполнения работы

Для выполнения работы необходимо знание IP адресации IPv4, принцип работы протокола OSPF, принцип работы DHCP сервера и базовые навыки конфигурации маршрутизаторов.

Цель работы – получение навыков настройки DHCP сервера на маршрутизаторе. Топология сети приведена на рис. 1. Требуемая адресация приведена в табл. 1.

В ней расположен DHCP-сервер, который централизованно выдает адреса в сети LAN10, LAN20 и LAN30. Маршрутизаторы R1, R2 и R3 в данной схеме являются DHCP-Relay агентами.

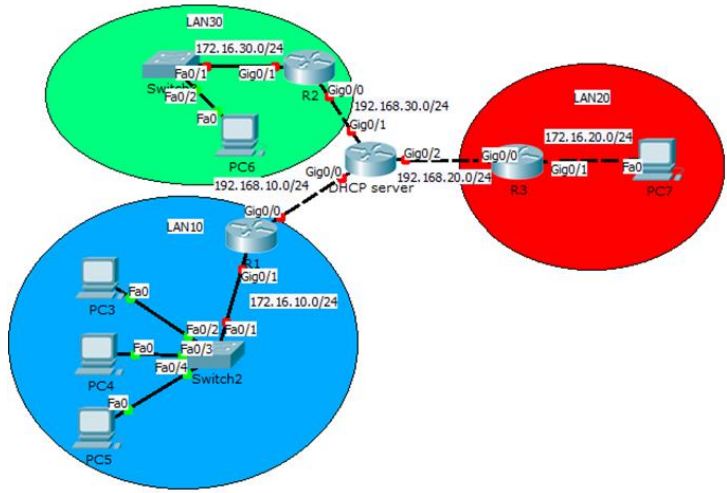



Рисунок 1 – Топология сети

Таблица 1 – Адресация

| Устройство | Интерфейс | IP-адрес | Маска подсети |
|---|---|---|---|
| R1 | Gig0/1 | 172.16.10.1 | 255.255.255.0 |
| R1 | Gig0/0 | 192.168.10.2 | 255.255.255.0 |
| R2 | Gig0/1 | 172.16.30.1 | 255.255.255.0 |
| R2 | Gig0/0 | 192.168.30.2 | 255.255.255.0 |
| R3 | Gig0/1 | 172.16.20.1 | 255.255.255.0 |
| R3 | Gig0/0 | 192.168.20.2 | 255.255.255.0 |
| DHCP Server | Gig0/0 | 192.168.10.1 | 255.255.255.0 |

| | | | |
|---|---|---|---|
| DHCP Server | Gig0/1 | 192.168.30.1 | 255.255.255.0 |
| DHCP Server | Gig0/2 | 192.168.20.1 | 255.255.255.0 |

Назначить IP адреса всем маршрутизаторам согласно требуемой адресации.

Назначение IP адреса на DHCP Server.

```
Router>enable
Router#conf term
Router(config)#interface gig0/1
Router(config-if)#ip address 192.168.30.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#ex
Router(config)#interface gig0/0
Router(config-if)#ip address 192.168.10.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#ex
Router(config)#interface gig0/2
Router(config-if)#ip address 192.168.20.1 255.255.255.0
Router(config-if)#no shutdown
```

Сконфигурировать на DHCP сервере 3 пула адресов для каждой локальной сети. Пул адресов для LAN10.

```
Router#conf term
Создание пула адресов с именем LAN10
Router(config)#ip dhcp pool LAN10
Указание подсети для которой будут раздаваться ip адреса
Router(dhcp-config)#network 172.16.10.0 255.255.255.0
шлюз для этой подсети
Router(dhcp-config)#default-router 172.16.10.1
```

Создать пул адресов для LAN20.

```
Router(config)#ip dhcp pool LAN20
Router(dhcp-config)#network 172.16.20.0 255.255.255.0
Router(dhcp-config)#default-router 172.16.20.1
```

Аналогично создать пул для LAN30.

```
Router(config)#ip dhcp pool LAN30
Router(dhcp-config)#network 172.16.30.0 255.255.255.0
Router(dhcp-config)#default-router 172.16.30.1
```

Далее настаиваются агентов DHCP-Relay. Агент R1.

```
R1#conf term
R1(config)#interface gig0/1
R1(config-if)#ip helper-address 192.168.10.1
```

Агент для R2.

```
R2#conf t
R2(config)#interface gig0/1
R2(config-if)#ip helper-address 192.168.30.1
```

Агент для R3.

```
R3#conf t
R3(config)#interface gig0/1
R3(config-if)#ip helper-address 192.168.20.1
```

Настроить исключение выдачи указанных IP-адресов DHCP сервера.

```
Router#conf term
Router(config)#ip dhcp excluded-address 172.16.10.1 172.16.10.5
Router(config)#ip dhcp excluded-address 172.16.20.1 172.16.20.5
Router(config)#ip dhcp excluded-address 172.16.30.1 172.16.30.5
```

Настроить динамическую маршрутизацию на всех маршрутизаторах и DHCP сервере используя протокол OSPF и проверить таблицу маршрутизации с помощью show ip route. В результате получим.

```
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 3 subnets
O       172.16.10.0/24 [110/2] via 192.168.10.2, 00:19:15, GigabitEthernet0/0
```

```
O     172.16.20.0/24 [110/2] via 192.168.20.2, 00:02:21, GigabitEthernet0/2
O     172.16.30.0/24 [110/2] via 192.168.30.2, 00:04:20, GigabitEthernet0/1
   192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C     192.168.10.0/24 is directly connected, GigabitEthernet0/0
L     192.168.10.1/32 is directly connected, GigabitEthernet0/0
   192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C     192.168.20.0/24 is directly connected, GigabitEthernet0/2
L     192.168.20.1/32 is directly connected, GigabitEthernet0/2
   192.168.30.0/24 is variably subnetted, 2 subnets, 2 masks
C     192.168.30.0/24 is directly connected, GigabitEthernet0/1
L     192.168.30.1/32 is directly connected, GigabitEthernet0/1
```

Видно, что удаленные сети доступны через протокол OSPF.

Далее проверить работоспособность DHCP Server. Для этого необходимо нажать на хост, выбрать в меню вкладку рабочий стол «Desktop», открыть IP конфигурацию и выбрать вместо static, DHCP, как показано на рис. 2.

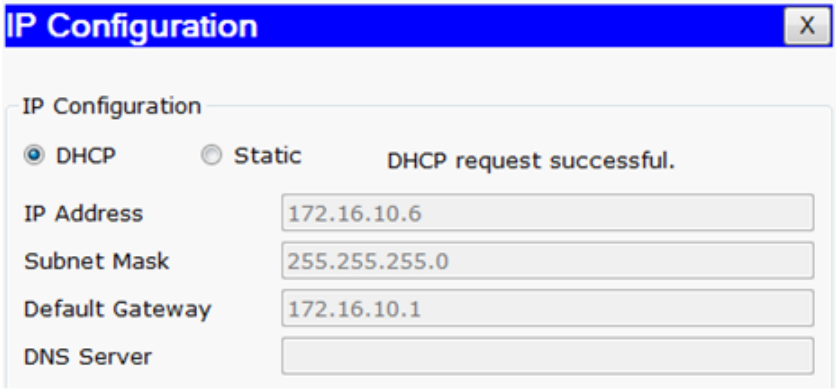



Рисунок 2 – Выбор получения IP-адреса от DHCP сервера

Если все PC получают IP-адреса от DHCP сервера, это означает о правильности его настройки. Выполненные настройки DHCP исключают выдачу хостам адресов с 172.16.10.1 по 172.16.10.5, поэтому раздача IP-адресов начнется с 172.16.10.6.

Далее проверить работоспособность сети, используя утилиту ping.

## 3 Задание для самостоятельной работы

Требуемая топология сети приведена на рис. 3, а адресация в табл. 2.

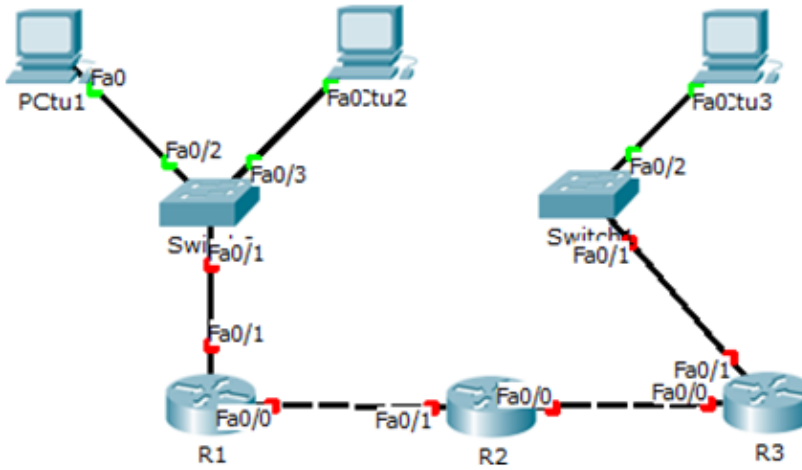



Рисунок 3 – Топология сети

Таблица 2 – Адресация

| Устройство | Интерфейс | IP адрес | Маска подсети |
|---|---|---|---|
| R1 | Fa0/1 | 192.168.0.1 | 255.255.255.0 |
| R1 | Fa0/0 | 172.16.0.1 | 255.255.255.0 |
| R2 | Fa0/1 | 172.16.0.8 | 255.255.255.0 |
| R2 | Fa0/0 | 192.168.100.1 | 255.255.255.0 |
| R3 | Fa0/0 | 192.168.100.8 | 255.255.255.0 |
| R3 | Fa0/1 | 10.0.10.1.9 | 255.255.255.0 |

Необходимо:

1. Назначить IP-адреса на всех интерфейсах маршрутизаторов согласно требуемой адресации.

2. На R2 настроить два пула адресов для каждой локальной сети, исключая первые 10 адресов.

3. Сконфигурировать агентов DHCP-Relay на R1 и R3

4. Настроить динамическую маршрутизацию на R1–R3, используя протокол OSPF.

5. Проверить работоспособность DHCP сервера.

6. Проверить работоспособность сети, используя утилиту ping

7. Результаты о проделанной работе показать преподавателю и обосновать результаты.

## 4 Поиск неисправностей

Данная часть работы посвящена поиску неисправностей сети. Требуемая топология сети приведена на рис. 4. Файл выдается преподавателем. Дано адресное пространство 192.168.0.0. Маска подсети – 255.255.255.0. Адресный пул имеет имя compclub. Первый адрес сети назначен DHCP server. Исключены адресы из пула с 192.168.0.1 по 192.168.0.15. Результатом поиска неисправностей должно являться наличие связи между конечными устройствами.

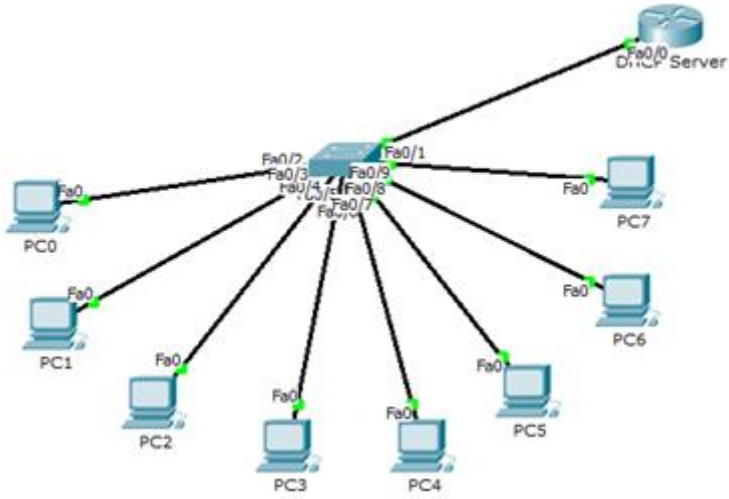



Рисунок 4 – Топология сети

## ЛАБОРАТОРНАЯ РАБОТА №15
## Списки контроля доступа и трансляция сетевых адресов: ACL и NAT

### 1 Краткая теоретическая справка

Списки доступа (access-lists) используются в целом ряде случаев и являются механизмом задания условий, которые маршрутизатор проверяет перед выполнением каких-либо действий. Так, проверяется каждый пакет и на основании условий, указанных в ACL определяется, что нужно сделать с пакетом, пропустить или отбросить. Типичными условиями являются адреса отправителя и получателя пакета, тип протокола. Каждое условие в списке доступа записывается отдельной строкой. Список доступа в целом представляет собой набор условий, объединенных под одним номером. Проверка пакета на соответствие списку производится последовательным применением условий из данного списка (в порядке, в котором они были введены). Пакет, который не соответствует ни одному из условий уничтожается. Для каждого протокола на интерфейсе может быть назначен только один список доступа. Стоит отметить одну особенность. Может быть назначено сочетание условий разрешения и запрета. Это может быть использовано, для того чтобы указать вложенный разрешенный или запрещенный диапазон IP-адресов.

Рассмотрим два примера стандартных списков.

```
Разрешение прохождения трафика от узла 10.0.0.10
Router(config)#access-list  1 permit host 10.0.0.10
Запрещение прохождения трафика из подсети 10.0.1.0/24
Router(config)# access-list  2 deny 10.0.1.0 0.0.0.255
```

Списки доступа бывают нескольких видов: стандартные, расширенные, динамические и другие. В стандартных ACL есть возможность задать только IP-адрес источника пакетов для их запретов или разрешений.

Стандартные списки не так гибки, как хотелось бы. В отличие от них, расширенные позволяют создавать списки фильтрующие определенные виды трафика. Так, возможно включение фильтрации по протоколам и портам. Для указания портов указываются следующие обозначения (табл. 1).

Таблица 1 – Обозначение портов в ACL

| Обозначение | Действие |
|---|---|
| lt n | Все номера портов, меньшие N |

| | |
|---|---|
| gt n | Все номера портов, большие N |
| eq n | Порт N |
| neq n | Все порты, за исключением N |
| range n m | Все порты от N до M включительно |

NAT (Network Address Translation) – , технология трансляции сетевых адресов, позволяющая преобразовывать (изменять) IP-адреса и порты в сетевых пакетах. NAT чаще всего используется для осуществления доступа устройств из локальной сети предприятия в Интернет, либо, наоборот, для доступа из Интернет на какой-либо ресурс внутри сети. Локальные сети предприятий строится на частных IP адресах:

- 10.0.0.0 — 10.255.255.255 (10.0.0.0/255.0.0.0 (/8))
- 172.16.0.0 — 172.31.255.255 (172.16.0.0/255.240.0.0 (/12))
- 192.168.0.0 — 192.168.255.255 (192.168.0.0/255.255.0.0 (/16))

Данные адреса не маршрутизируются в Интернете, и провайдеры должны отбрасывать пакеты с такими IP-адресами отправителей или получателей. Для преобразования частных адресов в Глобальные (маршрутизируемые в Интернете) как раз и применяют NAT.

Существует три вида трансляции Static NAT, Dynamic NAT, Overloading (PAT).

• Статический (Static) NAT осуществляет преобразование IP-адреса один к одному, то есть сопоставляется один адрес из внутренней сети с одним адресом из внешней сети. Иными словами, при прохождении через маршрутизатор, адрес меняется на строго заданный адрес. Запись о такой трансляции хранится неограниченно долго, пока есть соответствующая строчка в конфигурации маршрутизатора. Такой тип NAT бывает полезным, когда есть сервер внутри сети, к которому необходим полный доступ извне. То есть запросы на публичный адрес сервера будут переправляться на его частный адрес. К примеру, такой NAT не обеспечит, чтобы все пользователи сети выходили в интернет.

• Динамический (Dynamic) NAT осуществляет преобразование внутреннего адреса(ов) в один из группы внешних адресов. В этом случае при прохождении через маршрутизатор, новый адрес выбирается динамически из некоторого диапазона адресов, называемого пулом (pool). Запись о трансляции хранится некоторое время, чтобы ответные пакеты могли быть доставлены адресату. Если в течение некоторого времени трафик по этой трансляции отсутствует, трансляция удаляется и адрес возвращается в пул. Если требуется создать трансляцию, а свободных адресов в пуле нет, то пакет отбрасывается.

• Overloading (или PAT) позволяет преобразовывать несколько внутренних адресов в один внешний. Для осуществления такой трансляции используются порты, поэтому такой NAT называют PAT (Port Address Translation). С помощью PAT можно преобразовывать внутренние адреса во внешний адрес, заданный через пул или через адрес на внешнем интерфейсе.

## 2 Последовательность выполнения работы

Топология сети, предназначенная для изучения ACL, приведена на рис. 1 (требуемая адресация приведен на рисунке).

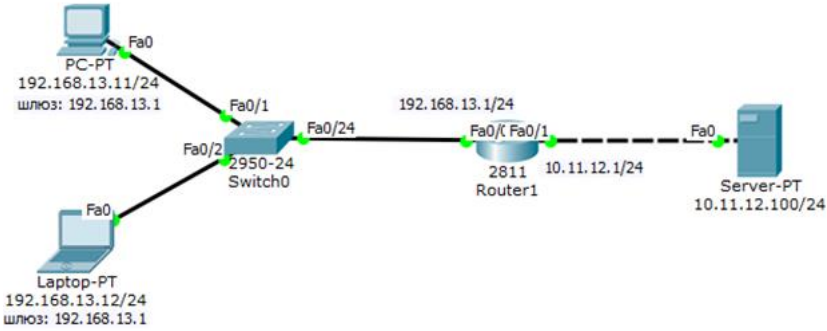



Рисунок 1 – Топология сети с указанием требуемой адресации

Первоначально необходимо настроить персональный компьютер, ноутбук и сервер (назначить IP-адрес, маску подсети и шлюз).

Затем включить интерфейсы маршрутизатора и назначить им требуемые IP-адреса, после чего проверить с помощью утилиты ping доступность сервера с персонального компьютера и ноутбука.

```
Router>enable
Router#configure terminal
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 192.168.13.1 255.255.255.0
Router(config-if)#no shutdown
Router(config)#interface fastEthernet 0/1
Router(config-if)#ip address 10.11.12.1 255.255.255.0
Router(config-if)#no shutdown
```

Далее требуется с помощью ACL разрешить доступ к серверу с ноутбука, а с персонального компьютера запретить.

Правило запрета и разрешения доступа будем составлять с использованием стандартных списков доступа (ACL). Пока не задан список доступа на интерфейсе всё разрешено (permit). Однако стоит создать список, сразу действует принцип «Всё, что не разрешено, то запрещено». Поэтому нет необходимости что-то запрещать (deny). Поэтому указав, что разрешено, получим, что остальным – запрещено.

Таким образом, необходимо создать условие (например, номером 13), разрешающее пересылку трафика хосту с адресом 192.168.13.12.

```
Router(config)#access-list  13 permit host 192.168.13.12
```

Условие готового, осталось назначить его на соответствующий интерфейс маршрутизатора.

```
Router(config)#interface  fastEthernet 0/0
Router(config-if)#ip  access-group  13 in
```

Входящий трафик (in) – который приходит на интерфейс извне. Исходящий (out) – который отправляется с интерфейса вовне. Список доступа можно применить либо на входящий трафик (неугодные пакеты не будут попадать на маршрутизатор и соответственно, дальше в сеть), либо на исходящий (пакеты приходят на маршрутизатор, обрабатываются им, доходят до целевого интерфейса и только на нём обрабатываются). Как правило, списки применяют на входящий трафик.

Если необходимо добавить новый хост (например, компьютер с адресом 192.168.13.13) в разрешённые, то достаточно выполнить команду Router(config)#access-list 13 permit host 192.168.13.13 и компьютер с этим адресом сможет «общаться» к серверу. Для отмены какого-либо правила, необходимо повторить соответствующую команду дополнив её приставкой no. Для просмотра списков доступа используется команда Router#show access-lists.

Для изучения расширенных списков предназначена сеть, представленная на рис. 2. Необходимо разрешить доступ к FTP серверу 10.11.12.100 для узла 192.168.13.2 и запретить для узла 192.168.13.13.

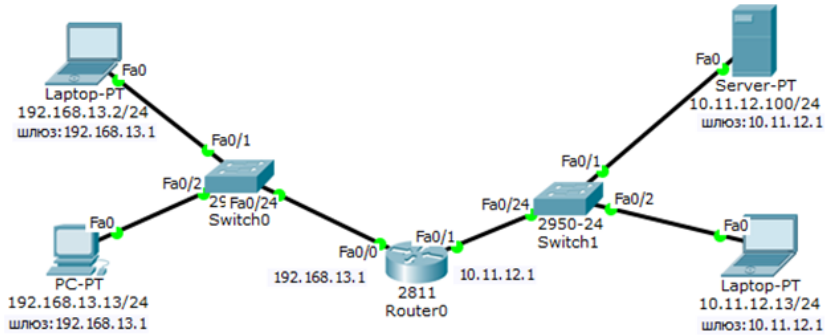



Рисунок 2 – Топология сети

Изначально на сервере 10.11.12.100 FTP сервис по умолчанию активен со значениями имя пользователя Cisco, пароль Cisco. Для проверки связи зайти на ноутбук (192.168.13.2), установить соединение (рис. 3) и выполнить команду DIR – чтение директории. Данная команда выводит общее число перечисленных файлов и каталогов, их общий размер и свободное пространство (в байтах) на диске.

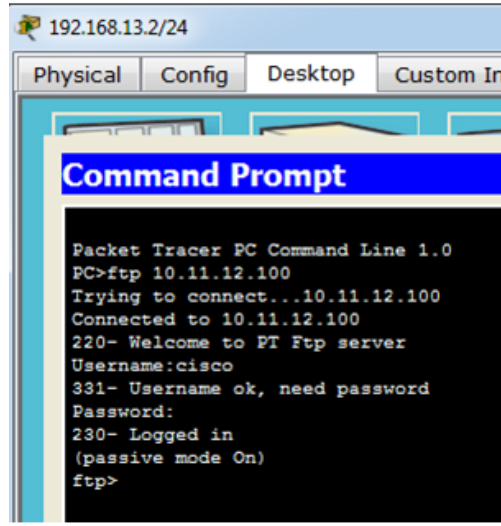



Рисунок 3 – Проверка доступности FTP сервера

Далее создать расширенный список с номером 113 в котором указать разрешающее и запрещающее правила для порта сервера 21, предназначенного для передачи команд и данных с помощью протокола FTP.

```
Router(config)#ip access-list extended 113
Router(config-ext-nacl)#permit tcp 192.168.13.2 0.0.0.0 10.11.12.100 0.0.0.0 eq 21
Router(config-ext-nacl)#deny tcp 192.168.13.13 0.0.0.0 10.11.12.100 0.0.0.0 eq 21
```

После этого применить этот список на входной трафик (in) интерфейса fa0/0.

```
Router(config-if)#ip access-group 113 in
```

Правильно настроек проверить подключением с персонального компьютера и ноутбука к FTP серверу (10.11.12.100).

Для изучения статического NAT используется сеть, представленная на рис. 4. Постановка задачи. Необходимо отправить данные устройству B, которое находится в сети интернет. Устройство A отправляет пакет, на шлюз по умолчанию (10.10.13.1). В пакете в качестве адреса источника будет адрес 10.10.13.13, а назначения 20.20.20.2. Пакет поступает на маршрутизатор (Router). Router снимает заголовок адреса источника 10.10.13.13 и меняет его на новый 185.20.1.3, затем выпускает измененный пакет в сеть в интернет. Пакет, достигнув места назначения, обрабатывается устройством B, которое готовит ответ на полученный пакет. В качестве адреса отправителя, собственно, адрес устройства B, адрес назначения – 185.20.1.3. Далее пакет возвращается обратно через сеть интернет на маршрутизатор, который всю информацию о ранее выполненной трансляции сохраняет в таблице. Получив пакет от устройства B маршрутизатор меняет обратно адрес 185.20.1.3 на адрес 10.10.13.13 в заголовке адреса назначения. Затем пакет возвращается к устройству A.

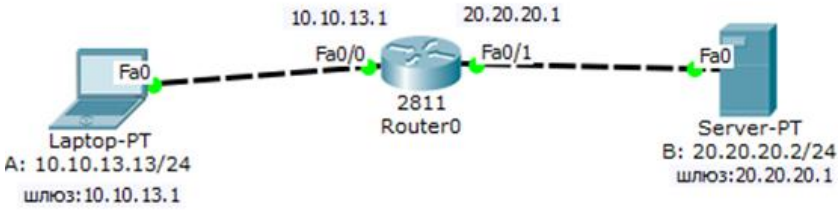



Рисунок 4 – Топология сети для изучения статического NAT

Первоначально необходимо включить интерфейсы маршрутизатора fa 0/0 и fa 0/1 с помощью команды no shutdown и

назначить им IP-адреса (в соответствие с требуемой адресацией) с помощью команды ip add. Далее назначить IP-адреса компьютерам и серверу, указав соответствующие адреса шлюзов. После этого приступить к настройке NAT.

Далее необходимо указать маршрутизатору какой порт у него входящий (в данном случае fa0/0), а какой исходящий (fa0/1).

```
Router(config)#int fa0/0
Router(config-if)#ip nat inside
Router(config-if)#int fa0/1
Router(config-if)#ip nat outside
```

Затем используя статический NAT настроить требуемую трансляцию.

```
Router(config)#ip nat inside source static 10.10.13.13 185.20.1.3
```

Перейдя в режим симуляции и воспользовавшись утилитой ping проверить работу

NAT. Посмотреть существующие трансляции можно с помощью команды Router#show ip nat translations.

Для изучения динамического NAT используется сеть, представленная на рис. 5 (требуемая адресация указана на рисунке). Постановка задачи. Провайдер выделил сеть 185.20.1.0/2, которая состоит из 16 адресов. Два из них – адрес сети и широковещательный, ещё два адреса назначаются на оборудование для обеспечения маршрутизации, а 12 оставшихся адресов можно использовать для NAT.

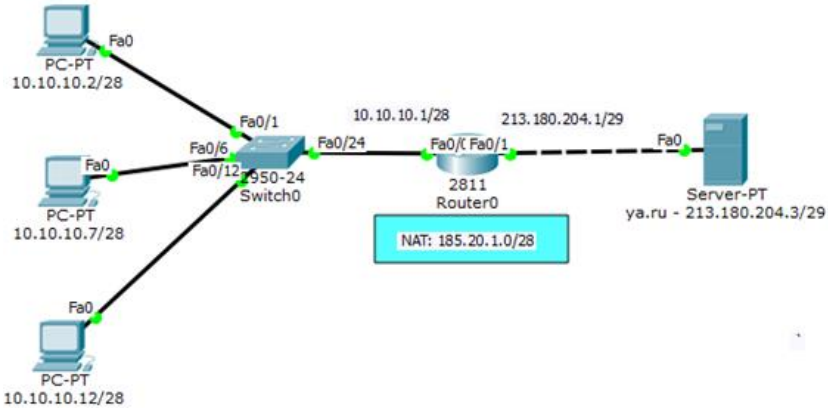



Рисунок 5 – Топология сети для изучения динамического NAT

Первоначально необходимо включить интерфейсы маршрутизатора fa 0/0 и fa 0/1 с помощью команды no shutdown и назначить им IP-адреса (в соответствие с требуемой адресацией) с помощью команды ip add. Далее назначить IP-адреса компьютерам и серверу, указав соответствующие адреса шлюзов. После этого приступить к настройке NAT.

Для этого указать интерфейс маршрутизатора, к которому подключена внутренняя сеть и интерфейс, к которому подключена сеть интернет и имеющему публичный адрес.

```
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip nat inside
Router(config)#interface fastEthernet 0/1
Router(config-if)#ip nat outside
```

При помощи списка доступа, указать диапазон частной сети (или сетей), которые необходимо транслировать в публичные адреса.

```
Router(config)#access-list 100 permit ip 10.10.10.0 0.0.0.15 any
```

Указать диапазон публичных адресов.

```
Router(config)#ip nat pool studNAT 185.20.1.3 185.20.1.14 netmask
255.255.255.240
```

Далее включить NAT, объединяя список доступа и пул внешних адресов.

```
Router(config)#ip nat inside source list 100 pool studNAT
```

При использовании данного NAT, трансляции будут происходить до тех пор пока публичные адреса не будут все использованы. То есть, если в сети 200 устройств, а адресов внешних 12, то получить доступ смогут первые 12 пользователей. Сбросить все действующие трансляции можно командой Router#clear ip nat translation.

## 3 Задание для самостоятельной работы

Топология сети и требуемая адресация приведена на рис. 6. Настроить статическую маршрутизацию и динамическую или статическую трансляцию адресов. С помощью списков доступа разрешить доступ ноутбука, а персональному компьютеру запретить к серверу. Для трансляции использовать адреса подсети 195.100.1.0/27.

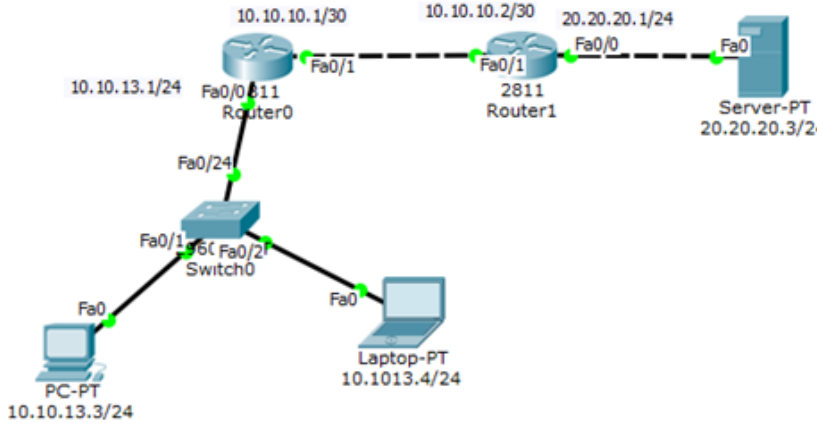



Рисунок 6 – Топология сети и требуемая адресация

## ЛАБОРАТОРНАЯ РАБОТА №16
## Одноранговые сети

### 1. Цель работы

Целью данной работы является получение навыков работы в локальных компьютерных сетях с ОС Windows.

### 2. Краткие теоретические сведения

Одноранговая сеть – это сеть равноправных компьютеров, каждый из которых имеет уникальное имя и может иметь пароль для входа во время загрузки ОС. Имя компьютера и пароль входа назначаются владельцем компьютера средствами ОС. Каждый компьютер такой сети может одновременно являться и сервером, и клиентом сети, хотя допустимо назначение одного компьютера только сервером, а другого только клиентом.

Достоинством одноранговых сетей является их высокая гибкость: в зависимости от конкретной задачи сеть может использоваться очень активно, либо совсем не использоваться. Из-за большой самостоятельности компьютеров в таких сетях редко бывает ситуация перегрузки, тем более, что количество компьютеров в таких сетях обычно невелико. Установка одноранговых сетей довольно проста, для них не требуются дополнительные дорогостоящие серверы. Кроме того, нет необходимости в системном администрировании, пользователи могут сами управлять своими ресурсами.

В одноранговых сетях допускается определение различных прав пользователей на доступ к сетевым ресурсам, но система разграничения прав не слишком развита. Если каждый ресурс защищен своим паролем, то пользователю приходится запоминать большое число паролей.

К недостаткам одноранговых сетей относятся также слабая система контроля и протоколирования работы сети, трудности с резервным копированием распределенной информации. Выход из строя любого компьютера-сервера приводит к потере части общей информации, по возможности все компьютеры должны быть высоконадежными. Эффективная скорость передачи информации по одноранговой сети часто оказывается недостаточной, поскольку трудно обеспечить быстродействие процессоров, большой объем оперативной памяти и высокие скорости обмена с жестким диском для всех компьютеров сети. К тому же компьютеры сети работают не только на сеть, но и решают другие задачи.

### 3. Ход работы

### 3.1. Рабочие группы

Данная лабораторная работа выполняется на двух виртуальных машинах под управлением операционной системы Windows 7.

Для работы с рабочими группами на виртуальных машинах необходимо проверить, что в параметрах сетевого адаптера установлен пункт «Внутренняя сеть».

При настройке сети Windows автоматически создает рабочую группу и присваивает ей имя. Существует возможность присоединиться к уже существующей рабочей группе в сети и создать новую.

На виртуальных машинах, используемых в данной лабораторной работе, используются учетные записи admin Admin505 (win7) и Администратор Qwerty_123.

Для проверки принадлежности компьютера к рабочей группе откройте свойства компьютера, перейдите на вкладку «Имя компьютера» (Пуск – Компьютер – Свойства – Дополнительные параметры системы – Имя компьютера). Чтобы компьютеры могли взаимодействовать они должны принадлежать одной рабочей группе (рис. 1).

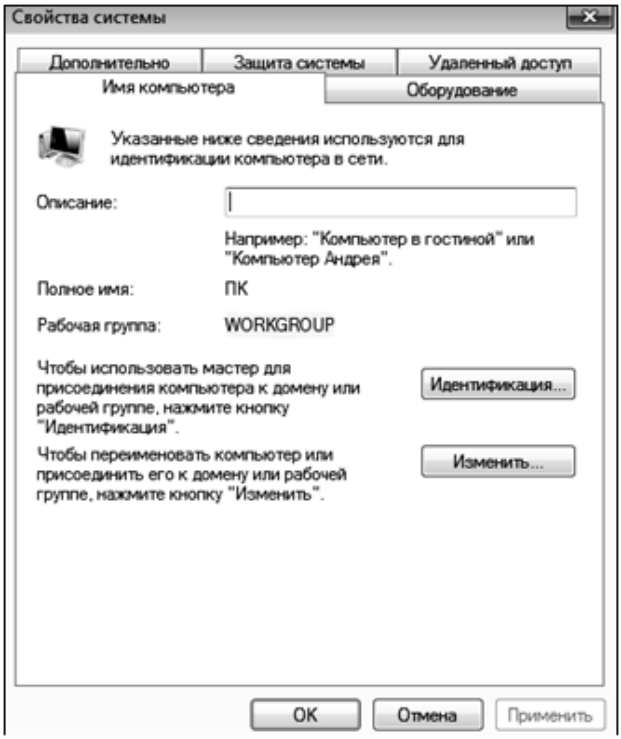



Рис. 1. Проверка принадлежности компьютера к рабочей группе

Чтобы переименовать компьютер или присоединить его к рабочей группе, нажмите кнопку «Изменить».

Чтобы присоединиться к существующей рабочей группе, необходимо ввести имя новой рабочей группы и нажать «ОК».

Для создания новой рабочей группы, также нужно ввести имя новой рабочей группы и нажать «ОК».

Присоедините гостевые ОС к одной рабочей группе: пользователей:

- в свойствах системы на вкладке «Имя компьютера» нажмите кнопку «Изменить»;
- выберите параметр «Является членом рабочей группы», введите имя рабочей группы (рис. 2) и нажмите «ОК»;
- в появившемся окне с сообщением о вступлении в рабочую группу нажмите «ОК» и перезагрузите гостевую ОС.

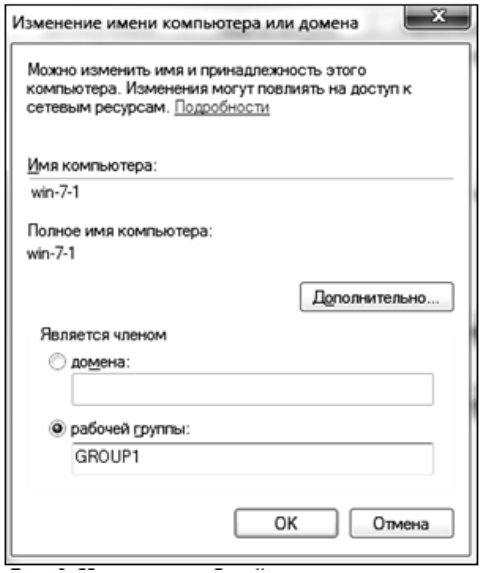


Рис. 2. Изменение рабочей группы компьютера

Для просмотра компьютеров рабочей группы в графическом интерфейсе нужно открыть Сетевое окружение и нажать «Отобразить компьютеры рабочей группы».

Для просмотра компьютеров рабочей группы в командной строке запустите командную строку и выполните команду: net view (рис. 3).

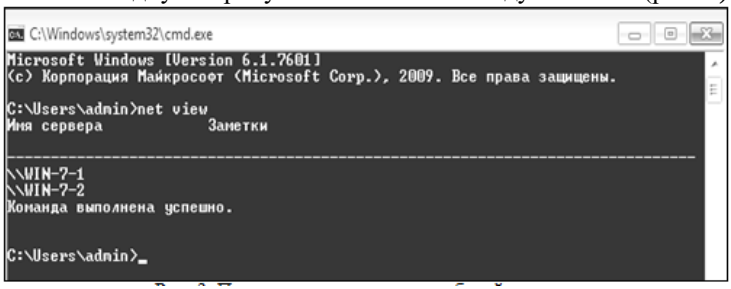


Рис. 3. Просмотр компьютеров рабочей группы

### 3.2. Настройка общего доступа к каталогам

Настройте общий доступ к папке, находящейся на сервере. Для этого выберите папку (можете создать папку на рабочем столе), нажми-

те на неё правой кнопкой мыши и выберете Свойства. Перейдите на вкладку Доступ и откройте «Общий доступ…», в выпадающем списке выберите пункт «Все» (рис. 4).

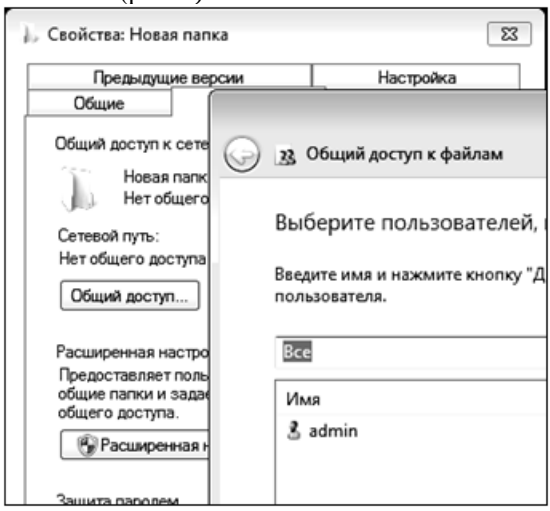



Рис. 4. Настройка общей папки

После настройки общего доступа к папке найдите ее в Сетевом окружении на второй машине и проверьте возможность добавления и изменения файлов.

Для подключения сетевой папки (т.е. для подключения общей папки как сетевого диска) на второй машине, вызовите контекстное меню Компьютера и выберите «Подключить сетевой диск». В появившемся окне (рис. 5) задайте букву сетевого диска и установите параметр

«Восстанавливать при входе в систему», нажмите «Готово». Теперь об- щая папка будет отображаться в папке «Компьютер» как сетевой диск.

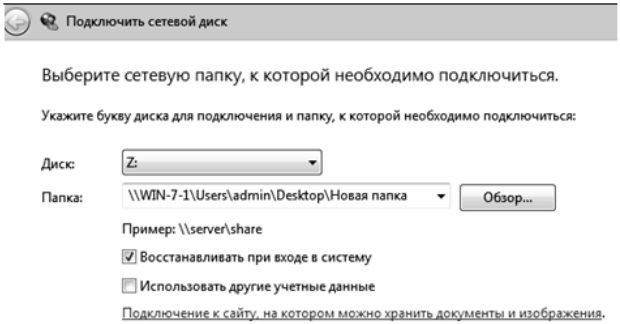



Рис. 5. Подключение сетевого диска

### 3.2. Настройка удаленного доступа

Для настройки удаленного доступа к компьютеру можно воспользоваться стандартными средствами Windows. Для этого удаленный компьютер должен быть включен и подключен к сети, удаленный доступ должен быть включен.

Настройте удаленный доступ:

- откройте свойства компьютера (win-7-1), выберите «Дополнитель-

ные параметры системы» и перейдите на вкладку «Удаленный доступ»;

- в группе «Удаленный помощник» установите параметр «Разре- шить отправку приглашений удаленному помощнику» (рис. 6), нажмите кнопку «Дополнительно», установите параметр «Разрешить удаленное управление этим компьютером», задайте предельный срок 8 часов и на- жмите «ОК»;
- в группе «Удаленный рабочий стол» выберите третий параметр и нажмите кнопку «Выбрать пользователей»;
- в появившемся окне нажмите кнопку «Добавить», введите имя пользователя, нажмите кнопку «Проверить имена» и нажмите ОК (рис. 7).

Если учетные записи на машинах совпадают, как в данном случае, то этот пункт проделывать нет необходимости;

- нажмите кнопку «Применить» на вкладке «Удаленные сеансы» для вступления изменений в силу.

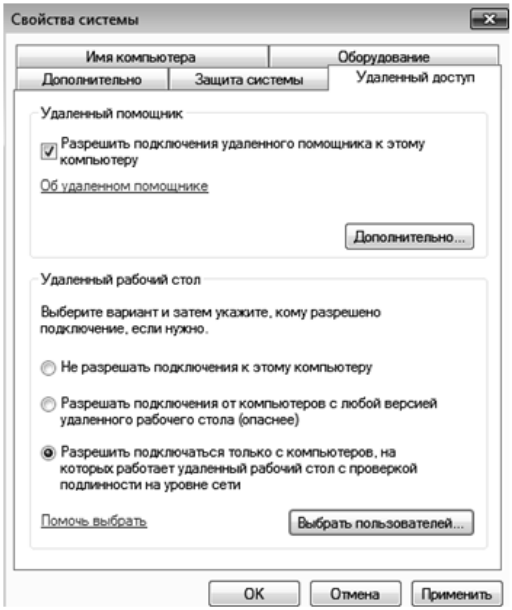



Рис. 6. Настройка параметров удаленного использования компьютера

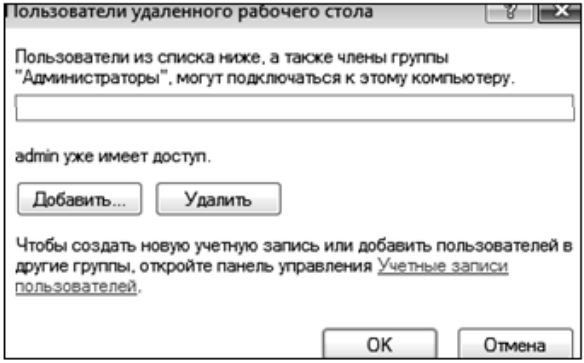



Рис. 7. Добавление пользователей удаленного доступа

Для того, чтобы подключиться к компьютеру с использованием удаленного доступа, войдите в компьютер-клиент (win-7-2), перейдите в меню Пуск – Все программы – Стандартные – Подключение к удаленному рабочему столу (рис. 8). Введите имя компьютера или его ip-адрес. Далее нажмите кнопку «Подключить». Необходимо выполнить вход в

систему, после чего можно работать с компьютером с помощью удаленного доступа.

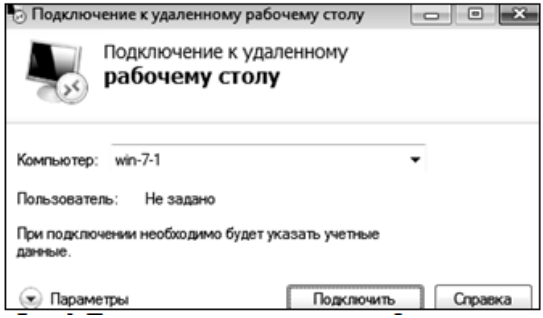



Рис. 8. Подключение к удаленному рабочему столу

## 4. Задание на лабораторную работу

**1.** Изучить теоретические сведения.

2. Создать рабочую группу из двух компьютеров.

3. Настроить общий доступ и проверить его работу.

4. Написать отчет по проделанной работе и защитить его у преподавателя.

## 5. Контрольные вопросы

1. Что такое одноранговая сеть?

2. Каковы достоинства и недостатки одноранговых сетей?

3. Что нужно сделать, чтобы создать рабочую группу?

4. Какое условие должно выполняться, чтобы компьютеры могли взаимодействовать?

5. Какую команду необходимо ввести в командной строке для просмотра компьютеров рабочей группы?

6. Что такое удаленный доступ?

7. Как настроить удаленный доступ?

8. Существуют ли альтернативные способы создания рабочей группы в операционных системах Windows? Если да, то какие?

9. Как просмотреть компьютеры рабочей группы в графическом интерфейсе?

10. Как присоединить гостевую ОС к рабочей группе?

## ЛАБОРАТОРНАЯ РАБОТА №17
## Высокоуровневые службы
### 1. Цель работы

Целью данной работы является изучение теоретических сведения о высокоуровневых службах и получение практических навыков в их установке и настройке.

### 2. Краткие теоретические сведения

Веб-сервер – это сервер, принимающий HTTP-запросы от клиентов и выдающий им HTTP-ответы, обычно вместе с запрошенными ресурсами. Веб-сервером называют как программное обеспечение, выполняющее функции веб-сервера, так и непосредственно компьютер на котором это программное обеспечение работает. Клиент, которым обычно является веб-браузер, передаёт веб-серверу запросы на получение ресурсов, обозначенных URL-адресами. Ресурсы – это HTML-страницы, изображения, файлы, медиа-потоки или другие данные, которые необходимы клиенту. В ответ веб-сервер передаёт клиенту запрошенные данные. Этот обмен происходит по протоколу HTTP.

Веб-серверы могут иметь различные дополнительные функции, например:

- автоматизация работы веб страниц;
- ведение журнала обращений пользователей к ресурсам;
- аутентификация и авторизация пользователей;
- поддержка динамически генерируемых страниц;
- поддержка HTTPS для защищённых соединений с клиентами.

В качестве HTTP сервера могут использоваться такие программные продукты, как Apache, IIS, ngnix.

FTP-сервер – это удаленный компьютер, с файловой системой которого можно работать через специальный одноименный протокол. Протокол FTP – один из стандартных протоколов передачи данных через Интернет, он позволяет переносить файлы с одного компьютера на другой. Чтобы установить соединение и обменяться файлами в Интернете, согласно протоколу FTP, необходимо запустить специальную прикладную программу, называемую клиентской частью FTP. Клиентское программное обеспечение устанавливается вместе с коммуникационными утилитами TCP/IP. FTP-клиент – программа, позволяющая подключаться к удаленному FTP-серверу и получать/передавать файлы по протоколу FTP. Получить доступ к другому компьютеру для обмена файлами можно, указав пользовательское имя и пароль.

При работе с FTP широко используются два понятия: скачивание и закачивание. Скачивание (download) означает процесс сохранения папок и файлов с FTP-сервера на ваш компьютер. Закачивание (upload) – это передача папок и файлов с вашего компьютера на FTP-сервер. Обычно каждой папке (реже – файлу) на FTP-сервере назначают права доступа: чтение, запись и выполнение. Право на чтение означает, что вы можете просматривать файл или содержимое папки. Право на запись позволяет изменять содержимое файлов. Право на выполнение даёт возможность запускать исполняемые файлы и скрипты на сервере. С управлением правами доступа вы можете столкнуться, например, при разработке веб-сайта, когда посетителям нужно запретить доступ в одни каталоги сайта и разрешить выполнение скриптов из других каталогов. Для FTP-сервера наиболее распространенным программным продуктом является FileZilla.

Почтовым сервером (сервером электронной почты) в системе пересылки электронной почты называют агент пересылки сообщений (mail transfer agent, MTA). Это компьютерная программа, которая передаёт сообщения от одного компьютера к другому. Обычно почтовый сервер работает «за кулисами», а пользователи имеют дело с другой программой – клиентом электронной почты (англ. mail user agent, MUA).

Когда пользователь набрал сообщение и отправляет его получателю, почтовый клиент взаимодействует с почтовым сервером, используя протокол SMTP. Почтовый сервер отправителя взаимодействует с почтовым сервером получателя (напрямую или через промежуточный сервер – релей). На почтовом сервере получателя сообщение попадает в почтовый ящик, откуда при помощи агента доставки сообщений (mail delivery agent, MDA) доставляется клиенту получателя. Часто последние два агента совмещены в одной программе (к примеру, sendmail), хотя есть специализированные MDA, которые в том числе занимаются фильтрацией спама. Для финальной доставки полученных сообщений используется не SMTP, а другой протокол – POP3 или IMAP, который также поддерживается большинством почтовых серверов. Хотя в простейшей реализации MTA достаточно положить полученные сообщения в личный каталог пользователя в файловой системе центрального сервера («почтовый ящик»).

В качестве почтового сервера используются такие программные продукты, как Exchange Server, Courier Mail Server или Office mail Server (для ОС семейства Windows); для Unix-подобных ОС – sendmail или сочетание exim (MTA) и dovecot (MDA). В данной лабораторной работе

рассматривается IIS (Internet Information Services) – проприетарный набор серверов для нескольких служб Интернета от компании Майкрософт. IIS распространяется с операционными системами семейства Windows NT. Основным компонентом IIS является веб-сервер, который позволяет размещать в Интернете сайты. IIS поддерживает протоколы HTTP, HTTPS, FTP, POP3, SMTP, NNTP

## 3. Ход работы

### 3.1. Веб-сервер

Войдите в операционную систему WinServer2012 под учётной записью администратора.

В первую очередь, необходимо установить IIS. Для этого в меню «Пуск» выберите пункт «Панель управления» запустите компонент «Установка и удаление программ». Откройте вкладку «Включение и отключение компонентов Windows». В пункте «Роли сервера» выберите компонент «Сервер приложений» и «Веб-сервер IIS». При выборе компонентов добавьте «SMTP-сервер». При выборе службы ролей для роли веб-сервера «IIS» установите флажки как на рисунке 1.

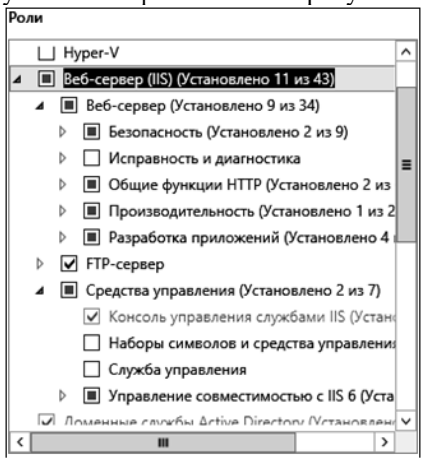



Рис. 1. Установка веб-сервера

Теперь необходимо подготовить тестовую страницу, вызываемую по умолчанию. Для этого, в приложении «Блокнот» напишите любой текст и сохраните файл как «Default.html» в каталоге C:\Inetpub\wwwroot.

Для настройки Web-сервера откройте «Диспетчер служб IIS» (Пуск – Администрирование – Диспетчер служб IIS) и перейдите к Веб-узлу по умолчанию (рис. 2).

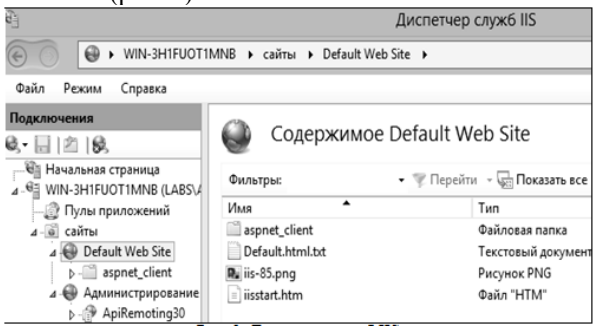



Рис. 2. Диспетчер служб IIS

Чтобы добавить страницу по умолчанию, перейдите на вкладку «Просмотр возможностей» и выберите «Документ по умолчанию». Оставьте в списке только тот документ, который был создан ранее (рис. 3).

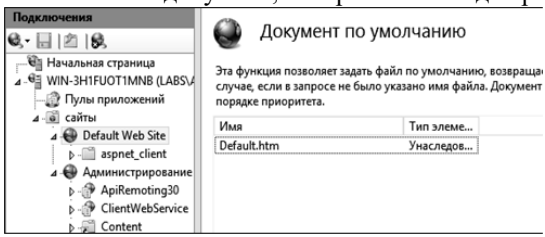



Рис. 3. Документ по умолчанию

Следующим шагом необходимо проверить настройку Web-сервера. Сначала уточните IP-адрес (Пуск – Выполнить – cmd – ipconfig/all). Затем, откройте браузер и в адресной строке наберите уточненный Вами IP-адрес (рис. 4).

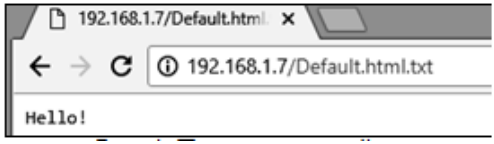



Рис. 4. Проверка настройки

Попробуйте открыть эту же страницу с другого рабочего места. Для этого войдите в операционную систему win7 под учётной записью администратора. Убедитесь, что на обеих виртуальных машинах установлена внутренняя сеть (Устройства – Настроить сеть – Тип подключения – Внутренняя сеть). Откройте браузер и в адресной строке наберите снова тот же адрес. На странице должен отобразиться текст созданного Вами документа «Default.html» в каталоге C:\Inetpub\wwwroot.

Создайте самостоятельно другой Web-узел. Для этого создайте новую папку на диске C для хранения образца содержимого web-узла, отключите веб-узел по умолчанию (правая кнопка мыши – Отключить). Щелкните правой кнопкой мыши на узле «сайты», выберите «Создать\Веб-сайт». Работа с мастером веб-сайтов (рис. 5) не вызовет у Вас сложностей, так как необходимо заполнить только пустые поля, стандартные же параметры можно не изменять.


Рис. 5. Создание нового веб-сайта

Проверьте настройку вашего Web-сервера с виртуальной машины win7.

### 3.2. FTP-сервер

Для настройки папки службы FTP и виртуального корневого каталога создайте новую папку для хранения файлов. Папке можно дать любое имя. Например, назовите новую папку «Example», тогда путь к ней будет таким: C:\inetpub\ftproot\Example.

В диспетчере служб IIS нажмите «Добавить FTP-сайт». Откроется окно добавления нового FTP-сайта.

В мастере укажите имя, которое пользователи могут использовать для получения доступа к папке FTP, созданной в начале. Можно задать любое имя. Удобнее всего в качестве имени псевдонима использовать имя каталога.

Для пути напечатайте путь или перейдите к каталогу, который Вы создали, например, Inetpub\ftproot\Example (рис. 6).

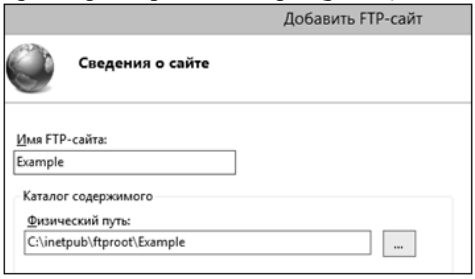



Рис. 6. Создание FTP-сайта

На следующем этапе в окне SSL отметьте пункт «Без SSL», нажмите «Далее».

Далее следует настройка разрешений. Предоставьте пользователям разрешения на чтение информации и на запись (рис. 7).

Чтобы установить разрешения для папки службы FTP, кликните правой кнопкой мыши на узел виртуального каталога для определенной папки службы FTP (например, Example) и нажмите «Редактировать разрешения». На вкладке «Безопасность» выберите или добавьте вашу учетную запись и присвойте разрешение на изменение (рис. 8).

Следующий шаг – это создание виртуального каталога веб-сервера. Чтобы веб-сервер мог получить доступ к корневому каталогу службы FTP, обычно создается виртуальный каталог для веб-сервера, соответствующий FTP-узлу. Имя виртуального каталога веб-сервера может быть таким же, как имя виртуального каталога FTP-сервера, однако это необязательно.

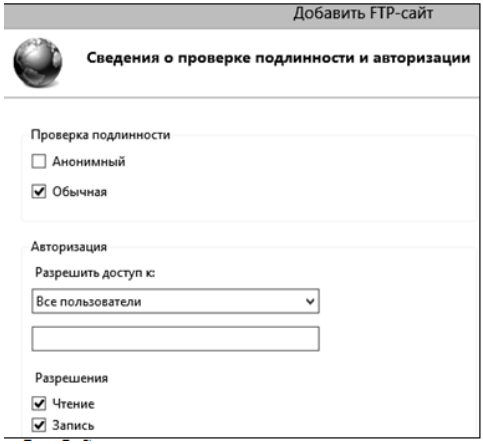



Рис. 7. Сведения о проверке подлинности и авторизации


Рис. 8. Разрешения

Чтобы создать виртуальный каталог веб-сервера, в диалоговом окне «Службы IIS» разверните узел «Веб-узлы». Кликните правой кнопкой мыши на узел «Веб-узел по умолчанию», нажмите «Добавить виртуальный каталог» (рис. 9).

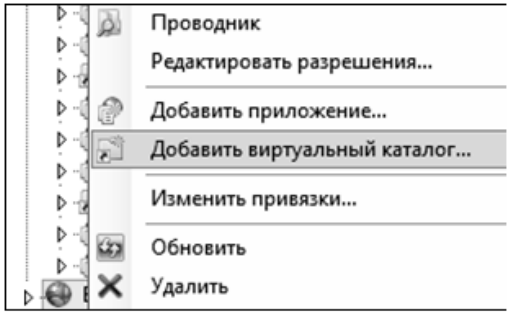


Рис. 9. Контекстное меню

В мастере задайте псевдоним, для пути напечатайте путь или перейдите к каталогу службы FTP, например, C:\inetpub\ftproot\Example (рис.10).

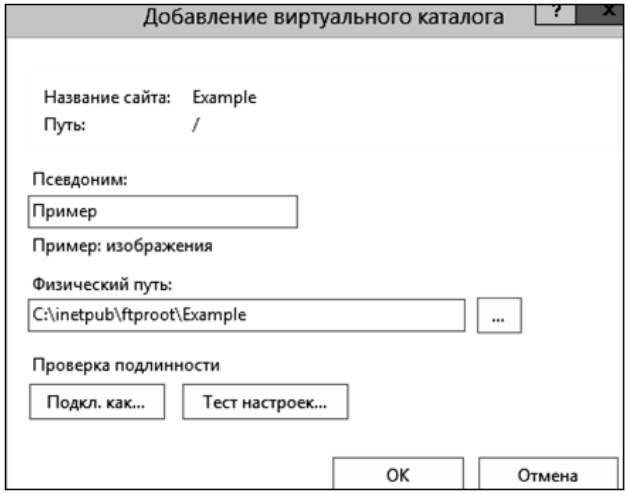


Рис. 10. Добавление виртуального каталога

Для разрешений доступа выберите чтение и выполнение.

Нажмите «Готово», чтобы создать виртуальный каталог и закрыть мастера. Проверьте настройку FTP-сервера с виртуальной машины win-7. Для этого откройте «Мой компьютер» и в адресной строке введите ftp://(ip-адрес сервера) (рис. 11).

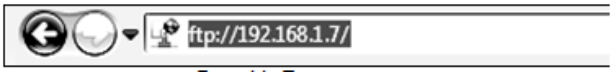



Рис. 11. Ввод запроса

Создайте самостоятельно другой FTP-узел по аналогии с представленным примером и заданием для Web-узла. Установите разрешение на запись. Проверьте работоспособность с удаленного рабочего места.

### 3.3. Почтовый сервер

Необходимо настроить SMTP-сервер. Управляется SMTP сервер через консоль управления «Диспетчер служб IIS 6.0». Открыть эту консоль можно через Server Manager: Средства – Диспетчер служб IIS 6. В консоли разверните ветку с именем сервера, щёлкните правой кнопкой мыши по SMTP Virtual Server и откройте его свойства.

На вкладке «Общие», если необходимо, выберите IP адрес, на котором должен отвечать SMTP сервер и включите ведение журнала, чтобы сохранялась информация обо всех отправленных письмах (рис.12).

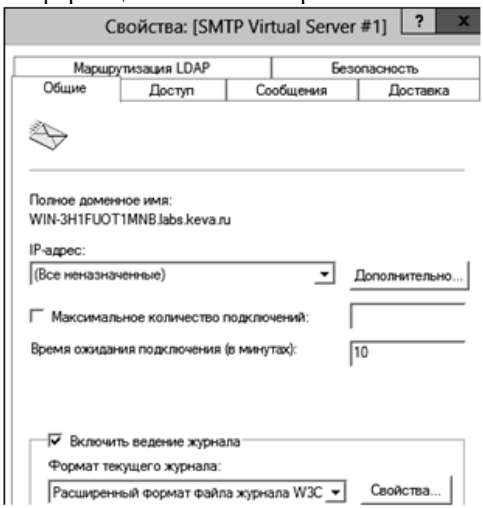



Рис. 12. Свойства SMTP

Перейдите на вкладку «Доступ». Нажмите на кнопку «Проверка подлинности» и убедитесь, что разрешен анонимный доступ (рис.13).

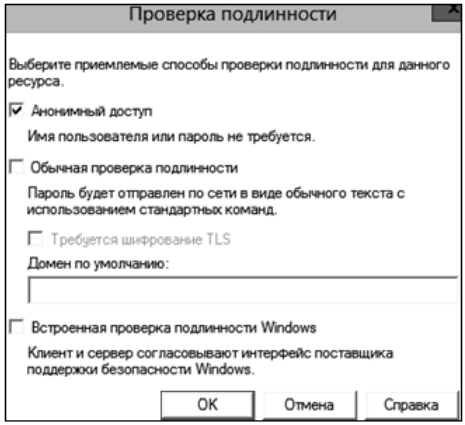



Рис. 13. Проверка подлинности

Вернитесь на вкладку «Доступ» и нажмите кнопку «Подключение». Здесь можно ограничить, с каких устройств могут отправлять почту через наш релей. Выберите опцию «Только компьютеры из списка ниже» и укажите список IP-адресов (рис. 14), не забыв себя (127.0.0.1).

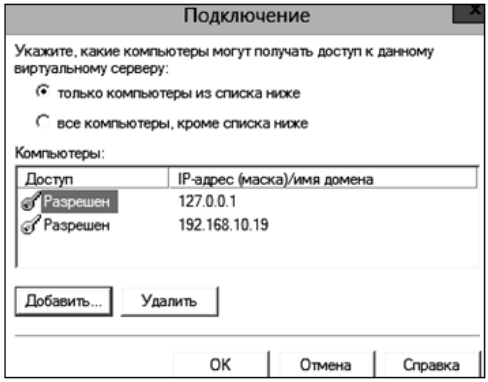



Рис. 14. Подключение

Перейдите на вкладку «Сообщения» (рис. 15). Здесь указывается административный email, куда будут приходить копии NDR сообщений, ограничения на максимальный размер писем, и количество получателей.

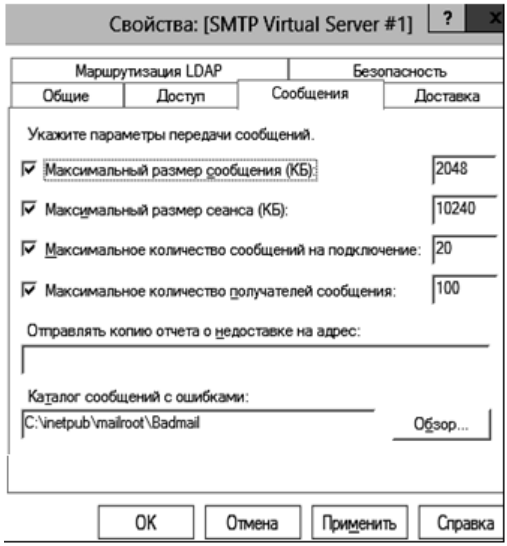


Рис. 15. Сообщения

Перейдите на вкладку «Доставка». Нажмите на кнопку «Безопасность исходящих подключений» (рис. 16). Здесь указывается, как нужно авторизоваться на сервере, куда будет пересылаться почта. К примеру, если вся почта будет отправляться на почтовый сервер Gmail и уже с него пересылаться адресатам, нужно выбрать «Обычная проверка подлинности», указав в качестве пользователя и пароля данные почтового ящика на сервисе Gmail (в настройках аккаунта Google нужно разрешить отправку через их smtp сервера).

Нажмите на кнопку «Дополнительно». Здесь указывается FQDN имя нашего SMTP-сервера (рис. 17). Нажмите на кнопку «Проверка DNS», чтобы проверить корректность записи в DNS.

Сохраните настройки SMTP-сервера.

Запустите службу из командной строки PoSh: start-service smtpsvc. Проверьте, что служба SMTPSVC запущена при помощи команды get-service smtpsvc (рис. 18).

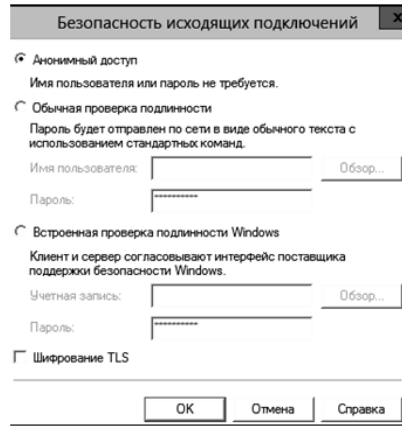



Рис. 16. Безопасность исходящих подключений

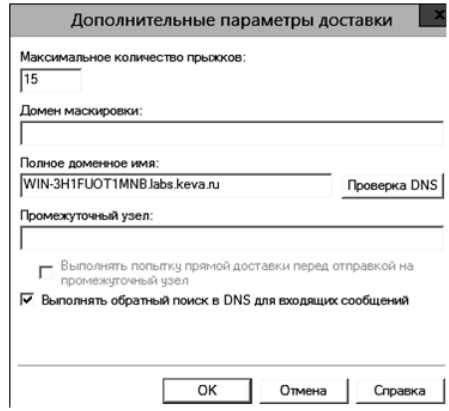



Рис. 17. Дополнительные параметры доставки

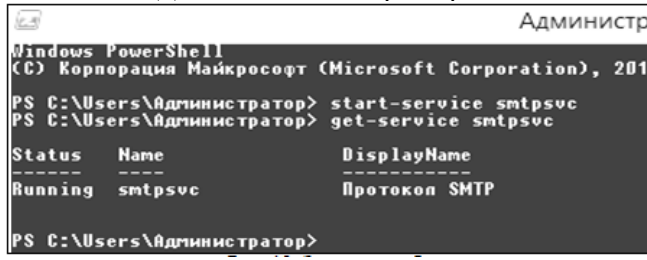



Рис. 18. Запуск службы

Необходимо проверить работу созданного SMTP сервера. Проще всего это сделать, создав на рабочем столе текстовый файл smtp-test-email.txt и, записать в него следующий текст, заменив имя отправителя и получателя на ваши (рис. 19).

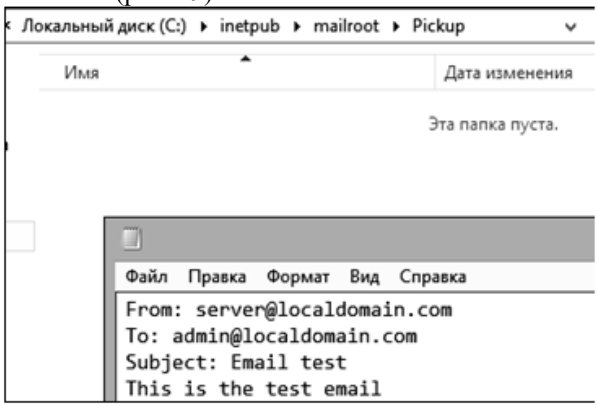



Рис. 19. Создание текстового документа

Скопируйте файл smtp-test-email.txt в каталог C:\inetpub\mailroot\Pickup. SMTP сервер следит за появлением файлов в этой каталоге и при обнаружении файла прочтет его содержимое и попытается отправить письмо с данной темой и текстом адресату, указанному в разделе To:.

Проверьте ящик получателя, в него должно упасть такое письмо.

## 4. Задание на лабораторную работу

1. Изучить теоретические сведения.
2. Создать Web-сервер. Проверить его работу.
3. Настроить FTP-сервер и проверить его работу.
4. Создать почтовый сервер. Изучить его работу.
5. Написать отчет и защитить его у преподавателя.

## 5. Контрольные вопросы

1. Что такое HTTP-сервер?
2. Что из себя представляет клиент для HTTP-сервера?
3. Приведите примеры программных продуктов, которые можно использовать в качестве HTTP-серверов?
4. Что такое FTP-сервер?
5. Что такое почтовый сервер?

6. Что такое MTA и MDA?

7. Что такое IIS? Каким образом устанавливается?

8. Какие протоколы поддерживает IIS?

9. Почему письма не отображаются во «Входящих», пока не пройдет синхронизация с сервером? В чем особенность протокола POP3?

10. Какой каталог предназначен для работы с Веб-сервером по умолчанию?

**Литература**

1. Корячко, В. П. Корпоративные сети [Электронный ресурс]: технологии, протоколы, алгоритмы : монография / В. П. Корячко, Д. А. Перепелкин. — Москва : Горячая линия-Телеком, 2015. — 216 с.

2. Основы построения инфокоммуникационных систем и сетей: Учебное пособие / А. В. Пуговкин - 2022. 128 с.