Федеральное агентство связи

Сибирский Государственный Университет Телекоммуникаций и Информатики СибГУТИ

Кафедра вычислительных систем

Расчетно-графическая работа

Выполнил: студент 2 курса группы ИП-014

Обухов Артём Игоревич Преподаватель: Мамойленко Сергей Николаевич

Новосибирск, 2021 г.

## Оглавление

[ВВЕДЕНИЕ 3](#_bookmark0)

[ОПИСАНИЕ ИСПОЛЬЗУЕМЫХ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ПРОТОКОЛОВ4](#_bookmark1) [ЗАДАНИЕ КУРСОВОГО ПРОЕКТА 9](#_bookmark2)

[ВЫПОЛНЕНИЕ РАБОТЫ 11](#_bookmark3)

[ЗАКЛЮЧЕНИЕ 22](#_bookmark4)

[ПРИЛОЖЕНИЕ 1 – Таблица 24](#_bookmark5)

## ВВЕДЕНИЕ

В данном курсовом проекте будет реализована настройка сети некоторого предприятия. В которой имеется три сети, объединенных при помощи пяти маршрутизаторов. Для организации связи внутри сетей воспользуемся тремя коммутаторами. Схема сети предприятия и соединения маршрутизаторов представлена на Рис. 1.

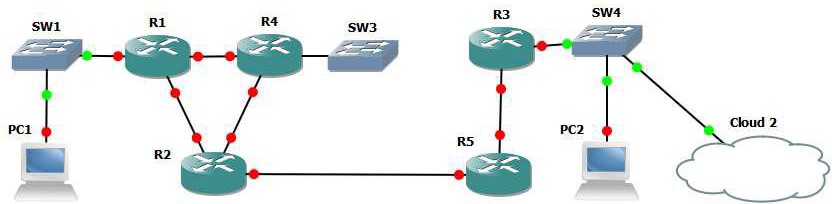


Рисунок 1 - Схема предприятия и связей сети

Выполнение курсового проектирования означает конфигурирование сети в соответствии с заданием и реализации услуги VoIP. Ознакомимся с программами такие как Graphical Network Simulator3 (GNS3), VirtualBox, WireShark. Для реализации курсового проекта используется среда моделирования GNS3, виртуальная машины на базе VirtualBox, операционные системы Microsoft Windows или GNU/Linux, Asterisk. Также ознакомимся с динамической маршрутизацией, основанной на технологии отслеживания состояния канала Open Shortest Path First (OSPF), о системе доменных имен Domain Name System (DNS) и о протоколе группового вещания версии разряженного режима Protocol Independent Multicast — Sparse Mode (Multicast-PIM-SM). Предполагается, что в рамках курсового проектирования в среде GNS3 эмулируется работа сетей, объединяемых маршрутизаторами CISCO семейства 3700 (версия ПО – 3725-adventerprisek9-mz.124-15.T14). Сеть должна быть полностью работоспособной.

**ОПИСАНИЕ ИСПОЛЬЗУЕМЫХ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ПРОТОКОЛОВ**

# Программное обеспечение

**Graphical Network Simulator3** [1] (GNS3)- если перевести дословно, то это графический симулятор сети, который позволяет создавать различные сетевые топологии прямо на вашем компьютере. Чаще всего GNS используется в качестве лабораторного стэнда, где можно проверить ту или иную технологию или схему. На самом деле GNS3 — это эмулятор.

Эмулятор позволяет создать модель компьютера или другого устройства и запускать внутри оригинальное программное обеспечение. Эмулируются все основные компоненты устройства, в том числе процессор, память и устройства ввода/вывода. Преимущества GNS3:

* Полный функционал эмулируемых устройств. Т.е. запустив тот же маршрутизатор Cisco, нам будут доступны практически все функции, которые работают на реальном маршрутизаторе;
* Возможность построения гетерогенных сетей. Имеется ввиду, что мы можем собрать схему где будут не только устройства Cisco, но и Juniper, Mikrotik, CheckPoint и т.д.;
* Добавление в сеть полноценных рабочих станций и серверов. В GNS3 мы можем добавить полноценный компьютер с Windows 7 или Ubuntu. Можем использовать в схеме Windows Server или RedHat. Забегая чуть вперед, можно сказать, что делается это с помощью технологий виртуализации (VirtualBox или VMWare) или подключив GNS3 к реальной сети. Таким образом можно проверить в лабораторных условиях установку VPN клиента на рабочую станцию, аутентификацию пользователей через сервер AAA, использовать настоящий браузер при подключении к настоящему Интернету. В общем что угодно, как в реальной жизни;
* И еще одна, четвертая, не мало важнейшее преимущество — Бесплатность! GNS3 находится в свободном доступе и не имеет каких-либо ограничений по использованию, что не может не радовать. Есть еще куча популярных симуляторв\эмуляторов, таких как Boson NetSim или Cisco VIRL, но все они платные. Конечно, также есть еще один известный бесплатный проект это Unified Networking Lab (UNetLab).

Теперь о недостатках. Их не так много, но они есть:

* Главный недостаток — отсутствие возможности эмулировать коммутаторы. Дело в том, что в реальных коммутаторах большое кол-во ASIC микросхем, которые пока что невозможно эмулировать на обычном компьютере. Именно эти ASIC микросхемы обеспечивают огромную скорость обработки пакетов. А вот маршрутизаторы работают на основе процессора, который очень похож на процессор обычного компьютера, а иногда и точно такой же. Поэтому проблем с эмуляцией маршрутизатора не возникает. Однако процессор значительно медленнее ASIC микросхем.
* Еще один важный недостаток — очень высокие требования к системным ресурсам. Хотя это скорее не проблема GNS3, а проблема запускаемых в нем устройств, которые жрут очень

много ресурсов. GNS3 в отличии от Cisco Packet Tracer работает с реальными прошивками устройств.

* Третий недостаток — баги или глюки, называйте, как хотите. В GNS3 их довольно много. Причем сейчас участились релизы новых версий GNS3 и, если честно, это даже немного раздражает, только установил последнюю версию, через неделю тебе уже пишут, что доступна новая. Так вот почти каждый релиз несет новый баг. Старые глюки конечно тоже исправляют.

**VirtualBox** [2] — это программное обеспечение, которое имитирует настоящий компьютер, что дает возможность пользователю устанавливать, запускать и использовать другие операционные системы, как обычные приложения. Такой себе компьютер в компьютере.

Виртуальная машина создает некое изолированное окружение на компьютере, которое состоит из виртуальных компонентов реального ПК: жесткого диска, видеокарты, оперативной памяти, различных контроллеров устройств и т.п. Таким образом, установленная в VirtualBox операционная система будет полностью уверенна в том, что она работает на реальном железе. Для чего нужен VirtualBox? Способов применения виртуальных машин существует множество.

Рассмотрим наиболее популярные среди обычных пользователей:

* Знакомство с другими операционными системами. В независимости от того, какая операционная система установлена на вашем компьютере, в VirtualBox можно установить любую из поддерживаемых ею, а это: множество дистрибутивов Linux, FreeBSD, MacOS, любая из версий Windows, Android и другие. Не нужно бояться того, что такой установкой вы сломаете реальную систему, или удалите важные данные — виртуальная машина работает изолированно и вы можете экспериментировать с ней как пожелаете. Когда она вам больше будет не нужна, просто удалите, и она не оставит никаких следов за собой;
* Еще один способ применения VirtualBox — необходимость запуска программы, не работающей в вашей основной ОС или ее версии. Например, вы работаете, в Windows и вам понадобилось приложение, которое доступно только под Linux. Иногда единственным выходом будет установка Linux в VirtualBox и использование нужного ПО оттуда. Подробная же ситуация может быть, когда вам нужна программа, работающая лишь под старыми версиями Windows;
* Тестирование различного ПО. Может случиться так, что вам понадобится воспользоваться какой-либо программой, или вам в общем часто приходится тестировать различные приложения, при этом вы не особо желаете засорять свою рабочую машину. Снова же, на помощь придет VirtualBox. Кроме того, используя виртуальную машину, вы можете не бояться заразить свой компьютер вирусами, даже если подобное произойдет с запущенной в VirtualBox ОС.

Это самые распространенные способы применения виртуальной машины среди обычных пользователей, но также VirtualBox часто используют:

* Разработчиками, для тестирования своего продукта на различных платформах;
* Учащимися для практики в построении сети, и тому подобное.

**WireShark** [3]— это достаточно известный инструмент для захвата и анализа сетевого трафика, фактически стандарт как для образования, так и для траблшутинга.

WireShark работает с подавляющим большинством известных протоколов, имеет понятный и логичный графический интерфейс на основе GTK+ и мощнейшую систему фильтров.

Кроссплатформенный, работает в таких ОС как Linux, Solaris, FreeBSD, NetBSD, OpenBSD, Mac OS X, и, естественно, Windows. Распространяется под лицензией GNU GPL v2. Он нужен для того чтобы проводить исследования сетевых приложений и протоколов, а также, чтобы находить проблемы в работе сети, и, что важно, выяснять причины этих проблем. Вполне очевидно, что для того чтобы максимально эффективно использовать снифферы или анализаторы трафика, необходимы хотя бы общие знания и понимания работы сетей и сетевых протоколов.

**VLC** [4]— проигрыватель для любой операционной системы, поддерживает сетевое вещание и локальное воспроизведение. Проект активно развивается и выдает новые версии своего детища, что немало важно, кодеки поставляются вместе с проигрывателем. Справедливо ли название

«проигрыватель»? Сомнительно, поскольку VLC способен не только воспроизводить, но и

записывать информацию, считываемую из источника воспроизведения в файл, вести вещание в локальную сеть и просто выдавать изображение или звук на вашем компьютере. Выбирать нужное из списка не нужно, можно выбрать все сразу. Не смотря на обилие поддерживаемых операционных систем, основной поддерживаемой ОС является семейство ОС Linux и Windows.

Если вникать в возможности VLC досконально, выяснится, что описать их все не так уж и просто.

Плеер VLC можно использовать в качестве сервера для трансляции потока аудио/видео по сети (поддерживает протоколы IPv4 и IPv6). Для воспроизведения файлов мультимедиа не требуется установка дополнительных кодеков, они уже «встроены» в программу. VLC может воспроизводить DVD и потоковое незашифрованное (без DRM) видео (IPTV), и интернет-радио. Также программа может записывать потоковое аудио/видео на компьютер.

# Используемые протоколы

**Open Shortest Path First** [5] (OSPF) - протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала (link-state technology) и использующий для нахождения кратчайшего пути алгоритм Дейкстры. Протокол OSPF был разработан IETF в 1988 году. Протокол OSPF представляет собой протокол внутреннего шлюза (Interior Gateway Protocol

* IGP). Протокол OSPF распространяет информацию о доступных маршрутах между маршрутизаторами одной автономной системы. OSPF имеет следующие преимущества:
  + Высокая скорость сходимости по сравнению с дистанционно-векторными протоколами маршрутизации;
  + Поддержка сетевых масок переменной длины (VLSM);
  + Оптимальное использование пропускной способности с построением дерева кратчайших путей.

## Описание работы протокола:

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 петель, 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.

**Domain Name System** [6] (DNS)- компьютерная распределённая система для получения информации о доменах. Чаще всего используется для получения IP-адреса по имени хоста (компьютера или устройства). Ключевые характеристики DNS. DNS обладает следующими характеристиками:

* + Распределённость администрирования. Ответственность за разные части иерархической структуры несут разные люди или организации.
  + Распределённость хранения информации. Каждый узел сети в обязательном порядке должен хранить только те данные, которые входят в его зону ответственности, и (возможно) адреса корневых DNS-серверов.
  + Кэширование информации. Узел может хранить некоторое количество данных не из своей зоны ответственности для уменьшения нагрузки на сеть.
  + Иерархическая структура, в которой все узлы объединены в дерево, и каждый узел может или самостоятельно определять работу нижестоящих узлов, или делегировать (передавать) их другим узлам.
  + Резервирование. За хранение и обслуживание своих узлов (зон) отвечают (обычно) несколько серверов, разделённые как физически, так и логически, что обеспечивает сохранность данных и продолжение работы даже в случае сбоя одного из узлов.

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.

**Protocol Independent Multicast** [7] (PIM) /Мультикастинг не зависящий от протокола/ — семейство многоадресных протоколов маршрутизации для IP сетей, созданный для решения проблем групповой маршрутизации. PIM называется протоколо-независимым, потому что базируется на традиционных маршрутных протоколах (например, Border Gateway Protocol) вместо того, чтобы создавать собственную сетевую топологию.

В курсовом проекте используем разреженный режим (Sparse Mode) протокола. **Protocol Independent Multicast-Sparse Mode** (PIM-SM) строит однонаправленные общие деревья с корнем в точке рандеву (Rendezvous Point — RP) для каждой мультикастинг-группы. В качестве RP может быть использован любой маршрутизатор, который поддерживает протокол PIM. Дополнительно PIM-SM создает деревья кратчайшего пути для каждого отправителя. PIM-SM используется для сетей с произвольным рассредоточением пользователей с ограниченной пропускной способностью сетевых каналов.

## ЗАДАНИЕ КУРСОВОГО ПРОЕКТА

Предприятию выделена сеть 10.9.0.0/16. Администратором сети (т.е. Нами) имеющаяся сеть разделена на необходимое количество подсетей. Маршрутизаторы реализуют протокол автоматического обмена таблицами маршрутизации OSPF.

В сети имеется один сервер системы имен DNS (на компьютере PC2). Указанный сервер функционирует под управлением операционной системы Microsoft Windows Server (версия не ниже 2003). Компьютер PC2 выступает источником многоадресной рассылки видеопотока (один канал, транслируется бесконечно). Для рекурсивных запросов DNS использует сервер физической сети. Для доступа к этой сети компьютер PC2 либо оснащается дополнительным сетевым интерфейсом, либо реализует IP-алиас.

Компьютер PC1 – пользовательская рабочая станция. Он может подключаться к произвольной сети (в процессе отладки сети должна быть проверена его работоспособность во всех сетях предприятия). Указанный компьютер используется для просмотра видеопотока.

## Задания:

1. Рассчитайте схему деления имеющейся сети на подсети исходя из следующего количества компьютеров в каждой из них: SW1 – (день Вашего рождения \* количество полных лет Вам на текущий момент), SW3 – (номер Вашей группы + месяц Вашего рождения), SW4 – (год Вашего рождения). Приведите обоснование своего решение (почему разделили сеть именно таким образом).
2. Установите операционную систему и программное обеспечение просмотра IpTV на рабочую станцию пользователя. Обоснуйте выбор операционной системы и программного обеспечения для просмотра IpTV.
3. Сконфигурируйте маршрутизаторы сети так, чтобы они имели связь к непосредственно подключенными сетями. Продемонстрируйте работоспособность текущей конфигурации (с использованием ping).
4. Настройте маршрутизаторы на использование протокола динамической маршрутизации. Используя сетевой монитор Wireshark приведите структуру пакетов, используемых протоколом динамической маршрутизации для своего функционирования. Объясните какой тип пакета для чего используется в рамках реализации протокола
5. Установите на сервере PC2 операционную систему. Сконфигурируйте службу DNS так, чтобы она обрабатывала запросы от клиентов для одной зоны (имя зоны выбирается

самостоятельно). Для обработки рекурсивных запросов настройте сервер так, чтобы он ретранслировал их на внешний DNS. Используя рабочую станцию и сетевой монитор приведите пример диалога, происходящего при получении DNS запросов и ответом на них.

1. Установите на сервере VLC media player и настройте его так, чтобы он осуществлял многоадресную рассылку видеопотока (содержание видеопотока выбирается произвольно и передается непрерывно «в цикле»).
2. Используя сетевой монитор Wireshark продемонстрируйте работу протокола IGMP.
3. Сконфигурируйте маршрутизаторы для передачи многоадресного трафика. В качестве протокола динамической маршрутизации многоадресного трафика используйте протокол PIM-SM. Продемонстрируйте работу этого протокола с использованием сетевого монитора.

## ВЫПОЛНЕНИЕ РАБОТЫ

Предприятию была выделена сеть 10.9.0.0/16. На данный момент сетей на предприятия не хватает для этого надо воспользоваться VLSM (variable-length subnet mask)- это маска под сети переменной длины. VLSM позволит сконфигурировать сеть с различными масками которые позволят разделить выделенную сеть на подсети. Тем самым сможем воспользоваться выделенной сетью для предприятия и распределить между маршрутизаторами. Для полного распределения по сети предприятия нам понадобится восемь подсетей. Для этого нам надо добавить к шестнадцати битом маски еще три бита тем самым мы получим девятнадцатую маску, и она позволит нашу сеть распределить между всеми подключенными интерфейсами маршрутизатора. Отсюда следует вот такое разбиение выделенной сети см. Таблица 1.

Таблица 1 - Разбиение сети предприятия на подсети

|  |  |  |  |
| --- | --- | --- | --- |
| Network | Диапазон IP- адресов | Broadcast | Маска подсети |
| 10.9.0.0 | 10.9.0.1-10.9.31.254 | 10.9.31.255 | 255.255.224.0 |
| 10.9.32.0 | 10.9.32.1-10.9.63.254 | 10.9.63.255 |
| 10.9.64.0 | 10.9.64.1-10.9.95.254 | 10.9.95.255 |
| 10.9.96.0 | 10.9.96.1-10.9.127.254 | 10.9.127.255 |
| 10.9.128.0 | 10.9.128.1-10.9.159.254 | 10.9.159.255 |
| 10.9.160.0 | 10.9.160.1-10.9.191.254 | 10.9.191.255 |
| 10.9.192.0 | 10.9.192.1-10.9.223.254 | 10.9.223.255 |
| 10.9.224.0 | 10.9.224.1-10.9.255.254 | 10.9.255.255 |

Распределим сети по интерфейсам см. Рис 2

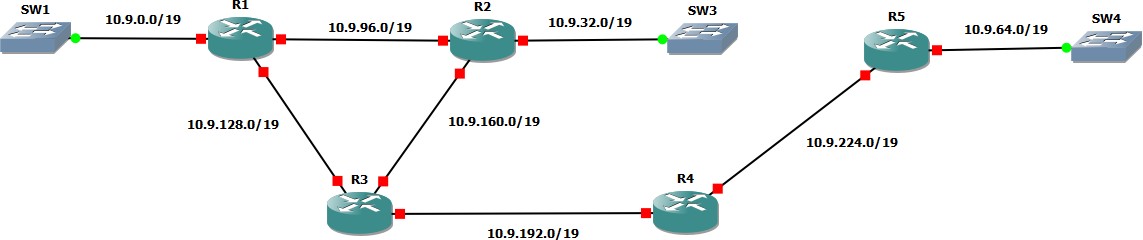


Рисунок 2 - Распределенные сети по интерфесам предприятия Для сетей куда подключены коммутаторы SW1, SW3 и SW4 у каждого интерфейса

настраивается сеть, зависимая от максимального количества подключенных узлов. Максимальное количество подключаемых узлов указано в задании. В таблице 1 (см. Приложение 1) указаны сеть и маска для каждого подключенного интерфейса от коммутаторов.

Также для выполнения курсового проекта нам понадобится две виртуальные машины на базе VirtualBox-а. Операционной системой воспользуемся серии Windows7 x64 для рабочей станции РС1 и Windows Server2003 R2 так как в нем есть уже готовое решение для настройки серверного функционала.

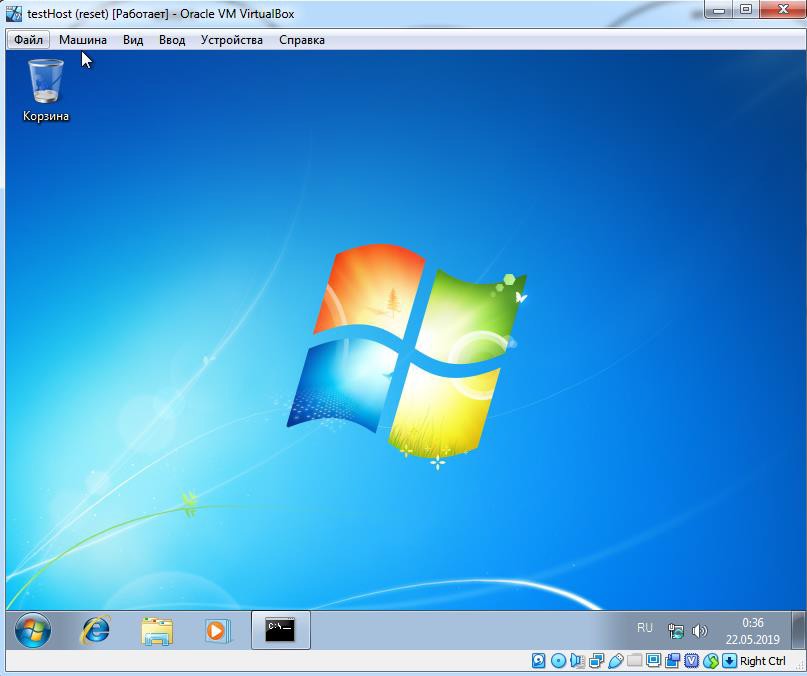


Рисунок 3 - Установленная операционная система Windows7 x64

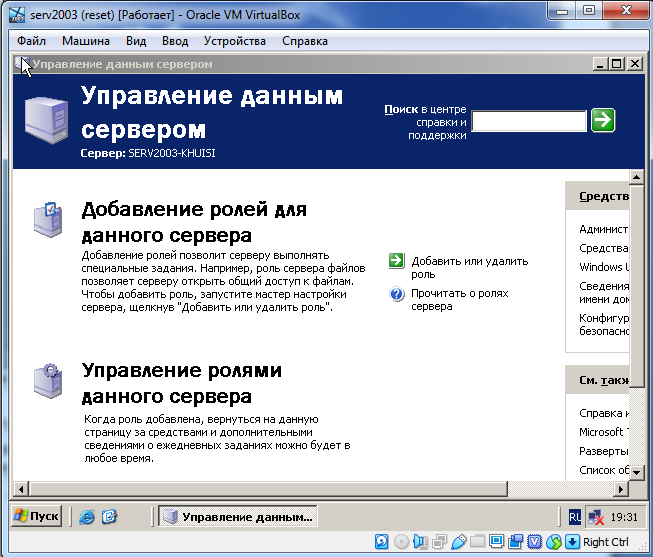


Рисунок 4 - Установленная операционная система Windows Server 2003 R2

Для просмотра потокового видео IpTV воспользуемся программой VLC.VLC бесплатен и имеет очень разнообразные возможности в плане воспроизведения, записи и передачи видео, так же он является кросплатформеным.

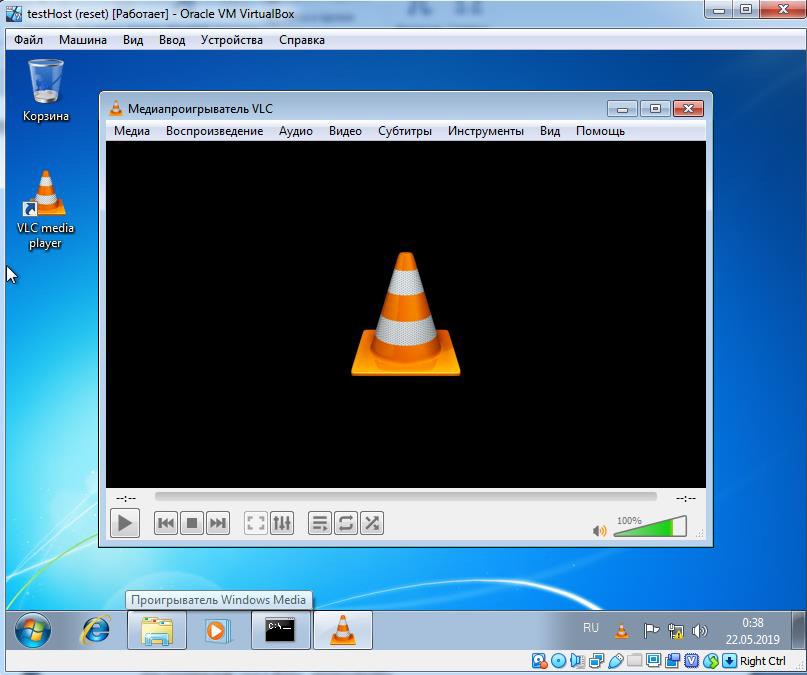


Рисунок 5 - Установленный и открытый медиаплеер VLC

Сконфигурируем сетевые интерфейсы маршрутизаторов сети. После этого проверим связь между интерфейсами с помощью команды ping. Конфигурация интерфейсов маршрутизатора R1:

R1#configure terminal R1(config)#interface fastEthernet 0/0

R1(config-if)#ip address 10.9.96.1 255.255.224.0 R1(config-if)#no shutdown

R1(config-if)#exit R1(config)#interface fastEthernet 0/1

R1(config-if)#ip address 10.9.128.1 255.255.224.0 R1(config-if)#no shutdown

R1(config-if)#exit R1(config)#interface fastEthernet 1/0

R1(config-if)#ip address 10.9.0.1 255.255.255.192 R1(config-if)#no shutdown

R1(config-if)#end

После выполнения всех команд по настройке маршрутизатора требуется сохранить конфигурацию в энергонезависимой памяти с помощью команды copy running-config startup-config, для того чтобы после перезагрузки маршрутизатора не потерять настройку.

Конфигурация интерфейсов маршрутизатора R2:

R2#configure terminal

R2(config)#interface fastEthernet 0/0

R2(config-if)#ip address 10.9.96.2 255.255.224.0 R2(config-if)#no shutdown

R2(config-if)#exit R2(config)#interface fastEthernet 0/1

R2(config-if)#ip address 10.9.160.1 255.255.224.0 R2(config-if)#no shutdown

R2(config-if)#exit R2(config)#interface fastEthernet 1/0

R2(config-if)#ip address 10.9.32.1 255.255.252.0 R2(config-if)#no shutdown

R2(config-if)#end

Конфигурация интерфейсов маршрутизатора R3: R3#configure terminal R3(config)#interface fastEthernet 0/0

R3(config-if)#ip address 10.9.128.2 255.255.224.0 R3(config-if)#no shutdown

R3(config-if)#exit R3(config)#interface fastEthernet 0/1

R3(config-if)#ip address 10.9.160.2 255.255.224.0 R3(config-if)#no shutdown

R3(config-if)#exit R3(config)#interface fastEthernet 1/0

R3(config-if)#ip address 10.9.192.1 255.255.224.0 R3(config-if)#no shutdown

R3(config-if)#end

Конфигурация интерфейсов маршрутизатора R4: R4#configure terminal R4(config)#interface fastEthernet 0/0

R4(config-if)#ip address 10.9.192.2 255.255.224.0 R4(config-if)#no shutdown

R4(config-if)#exit R4(config)#interface fastEthernet 0/1

R4(config-if)#ip address 10.9.224.2 255.255.224.0 R4(config-if)#no shutdown

R4(config-if)#end

Конфигурация интерфейсов маршрутизатора R5: R5#configure terminal R5(config)#interface fastEthernet 0/0

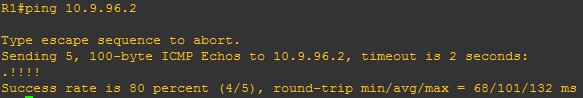
R5(config-if)#ip address 10.9.224.2 255.255.224.0 R5(config-if)#no shutdown

R5(config-if)#exit R5(config)#interface fastEthernet 0/1

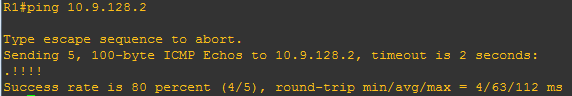
R5(config-if)#ip address 10.9.64.2 255.255.248.0 R5(config-if)#no shutdown

R5(config-if)#end

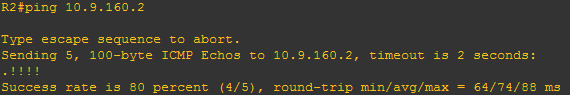
Проверим связи между соседними интерфейсами, находящимися в одной сети. Ping от R1 до R2:



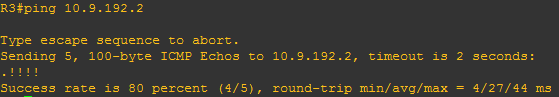
Ping от R1 до R3:



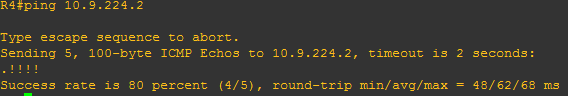
Ping от R2 до R3:



Ping от R3 до R4:



Ping от R4 до R5:



Для того чтобы появилась связь между разными сетями нам потребуется настроить протокол динамической маршрутизации OSPF. Для этого нам понадобится всю сеть разбить на четыре зоны. Пограничными маршрутизаторами будут R1, R2 и R5 (см. Рисунок 5). В первую зону будет входить все узлы сети коммутатора SW1, во вторую входят узлы коммутатора SW3, в третью зону войдут узлы коммутатора SW4 и в нулевую зону войдут все подключенные интерфейсы между маршрутизаторами.

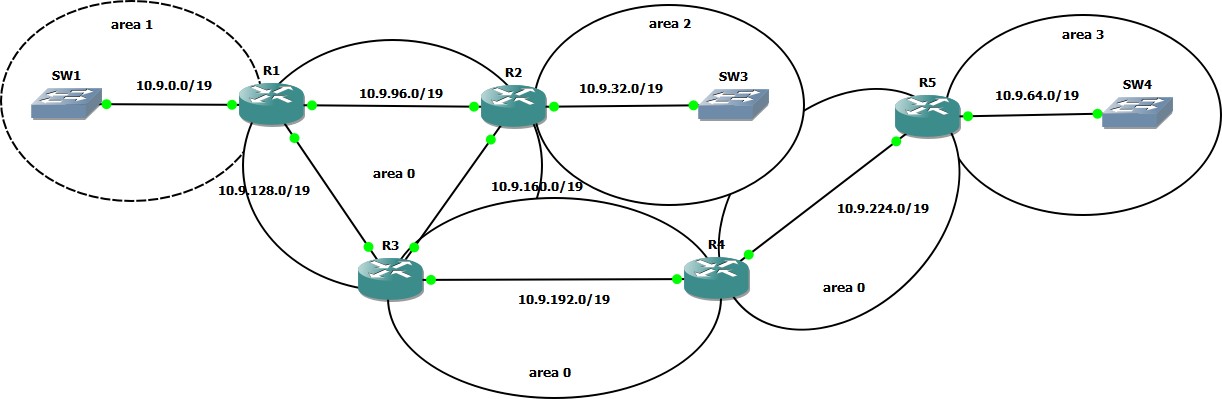


Рисунок 6 - Распределение сети по зонам Для запуска OSPF [8] достаточно выполнить следующие команды: Router(config)# router ospf номер\_процесса

Router(config-router)#network IP\_адрес инверсная\_маска (Wildcard mask) area

номер\_зоны или

Router(config-router)# network IP\_адрес маска (Wildcard mask) area номер\_зоны где номер\_процесса - означает, что на маршрутизаторе могут быть запущены несколько

независимых друг от друга OSPF процессов. Причем каждый процесс строит свою собственную базу данных. Номер процесса играет исключительно локальное значение и может не совпадать с номером процесса на других маршрутизаторах;

инверсная\_маска (Wildcard mask) - используется для более гибкого управления объявления подсетей в анонсах LSA, например когда требуется включить в анонсы LSA первые 8 или последние 64 подсетей определенной сети - вариантов много. Без инверсной маски пришлось бы вводить много похожих команд вручную. В OSPF данный функционал используется редко.

Поэтому для настройки OSPF вместо обратной маски можно с успехом использовать обычную маску.

Приступим к настройке OSPF на R1: R1#configure terminal R1(config)#router ospf 1

R1(config-router)# network 10.9.0.0 0.0.0.63 area 1

R1(config-router)# network 10.9.96.0 0.0.31.255 area 0

R1(config-router)# network 10.9.128.0 0.0.31.255 area 0 R1(config-router)# end

Настройка настройке OSPF на R2: R2#configure terminal R2(config)#router ospf 1

R2(config-router)# network 10.9.32.0 0.0.3.255 area 2

R2(config-router)# network 10.9.96.0 0.0.31.255 area 0

R2(config-router)# network 10.9.160.0 0.0.31.255 area 0 R2(config-router)# end

Настройка настройке OSPF на R3: R3#configure terminal R3(config)#router ospf 1

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R3(config-router)# | network | 10.9.192.0 | 0.0.31.255 | area | 0 |
| R3(config-router)# | network | 10.9.128.0 | 0.0.31.255 | area | 0 |
| R3(config-router)# | network | 10.9.160.0 | 0.0.31.255 | area | 0 |
| R3(config-router)# | end |  |  |  |  |

Настройка настройке OSPF на R4: R4#configure terminal R4(config)#router ospf 1

R4(config-router)# network 10.9.192.0 0.0.31.255 area 0

R4(config-router)# network 10.9.224.0 0.0.31.255 area 0 R4(config-router)# end

Настройка настройке OSPF на R5: R5#configure terminal R5(config)#router ospf 1

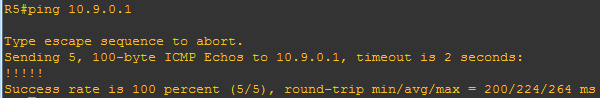
R5(config-router)# network 10.9.192.0 0.0.31.255 area 3

R5(config-router)# network 10.9.224.0 0.0.31.255 area 0 R5(config-router)# end

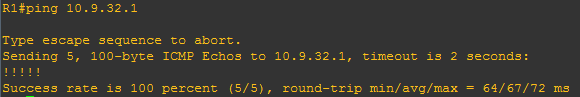
С помощью команд просмотра настроек протокола можно проверить и про диагностировать работу протокола. Такие команды как:

* + show ip route выводит содержимое таблицы маршрутизации;
  + show ip protocols показывает протокол маршрутизации, который в данный момент сконфигурирован;
  + show ip ospf neighbor показывает таблицу соседей и состояния смежности, установленные с ними;
  + ip ospf <interface> показывает тип сети, DR/BDR и ID маршрутизатора:
  + show ip ospf database показывает топологическую базу данных, пограничный маршрутизатор содержит топологию всех подключенных зон.

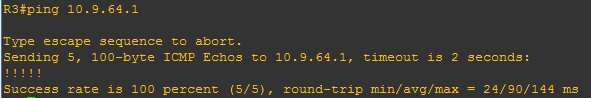
Проверим связи между разными сетями командой ping от R5 до R1 с зоной 1:



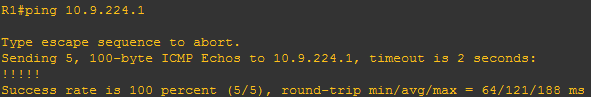
Проверим связи между разными сетями командой ping от R1 до R2 с зоной 2:



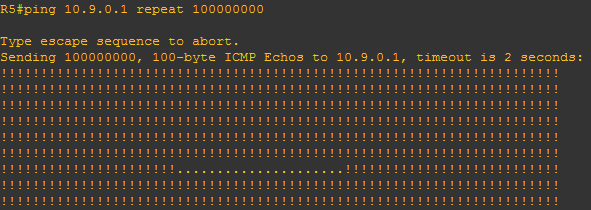
Проверим связи между разными сетями командой ping от R3 до R5 с зоной 3:



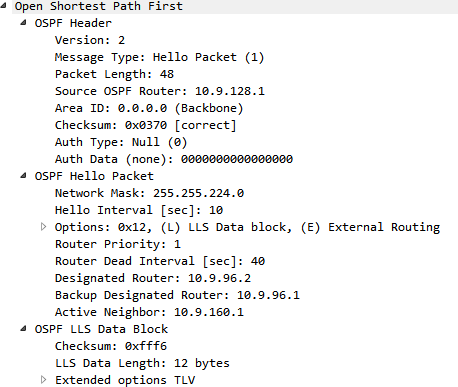
Проверим связи между разными сетями командой ping от R1 до R5 внутри зоны 0:



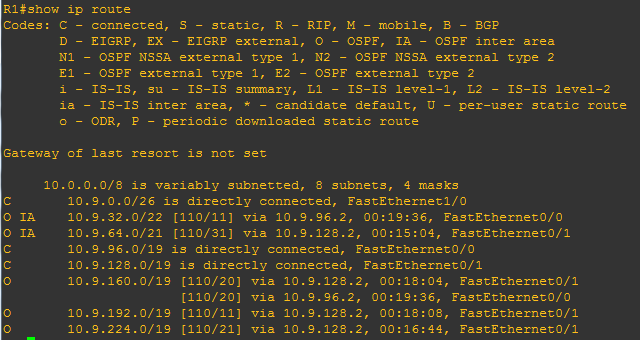
Отправим бесконечный ping с маршрутизатора R5 на один из сетевых интерфейсов маршрутизатора R1 и затем отключим интерфейс для проверки отказоустойчивости сети.



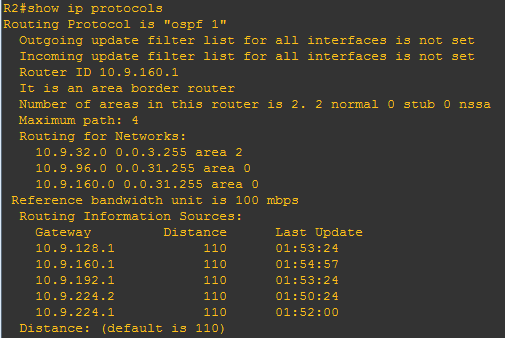
Проверка OSPF через программу WireShark:



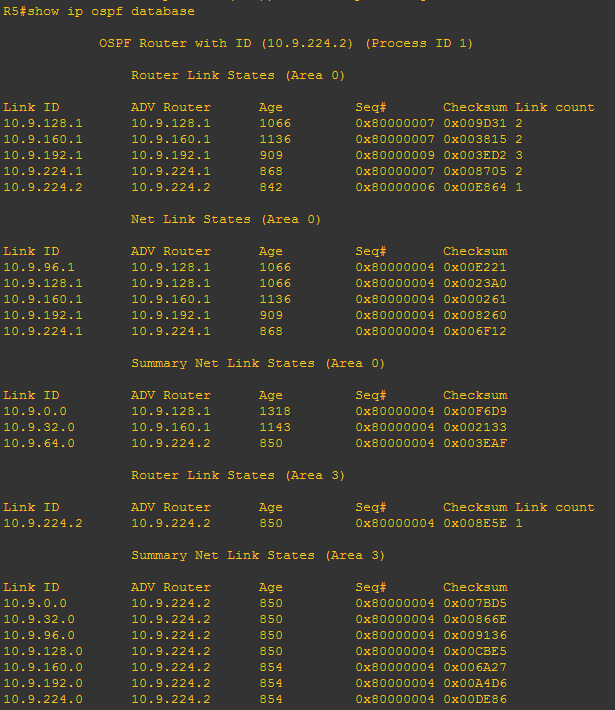
Содержимое таблицы маршрутизации на R1:

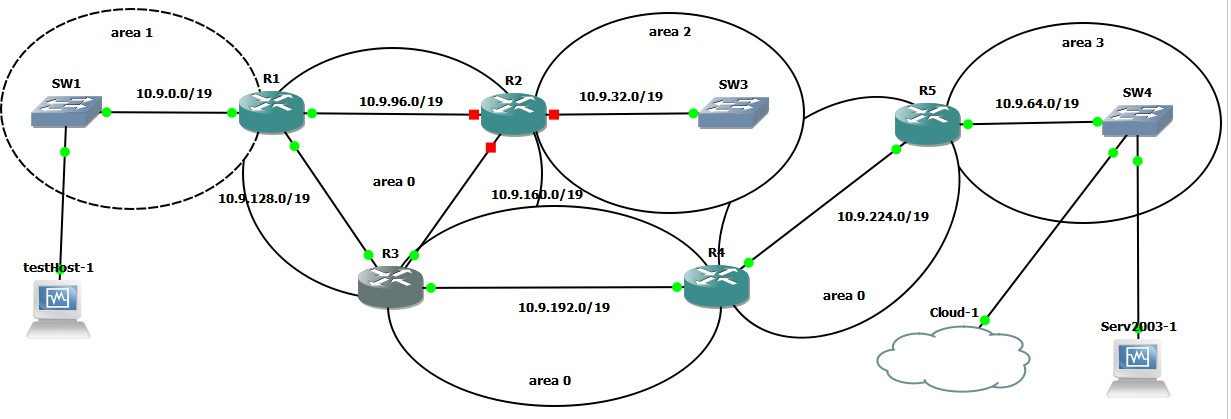


Проверка вывода на экран команды на маршрутизаторе R2:



Топологическая база данных на маршрутизаторе R5:





Настраивам DNS сервер [9] с именной зонной serv.test.com. Незабываем настроить сетевые интерфейсы сервера и хоста на использование DNS сервера.

Проверим связь между узлом и сервером по IP-адрессу и по его доменному имени:

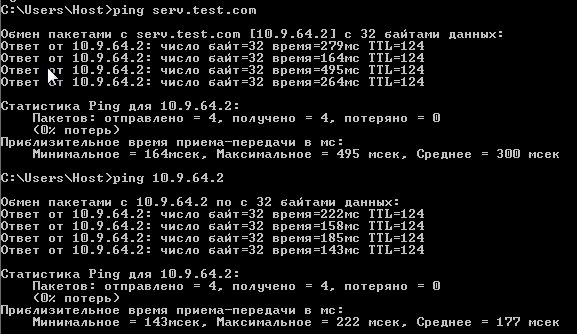


Рисунок 7 - Результат проверки связи по IP-адресу и доменному имени Установили VLC (см. Рисунок 8) медиаплеер на сервер и выводим видеофайл на постоянное

вещание в сеть [10].

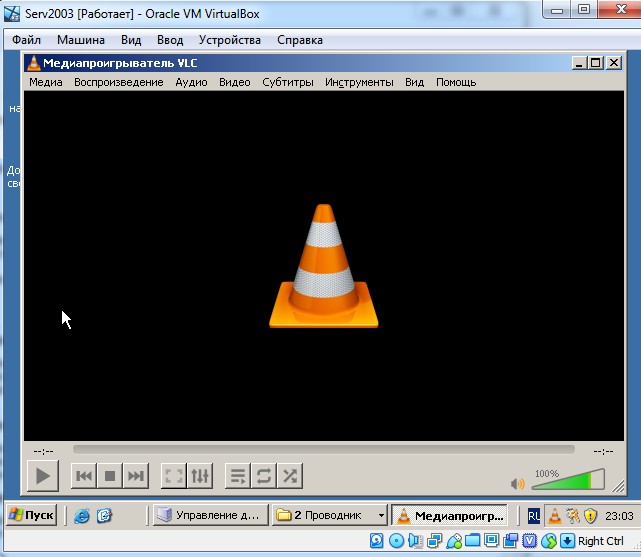


Рисунок 8 - VLC медиа плеер на сервере

Сконфигурировали видео на постоянный поток в сеть. Так же произвели настройку интерфейсов маршрутизаторов на потоковую передачу данных [11].На примере маршрутизатора R3:

R3#configure terminal

R3(config)# ip pim rp-address 10.9.64.2 IPTV override R3(config)#ip multicast-routing

R3(config)#interface fastEthernet 0/0 R3(config-if)#ip pim sparse-mode R3(config-if)#exit R3(config)#interface fastEthernet 0/1 R3(config-if)#ip pim sparse-mode R3(config-if)#exit R3(config)#interface fastEthernet 1/0 R3(config-if)#ip pim sparse-mode R3(config-if)#end

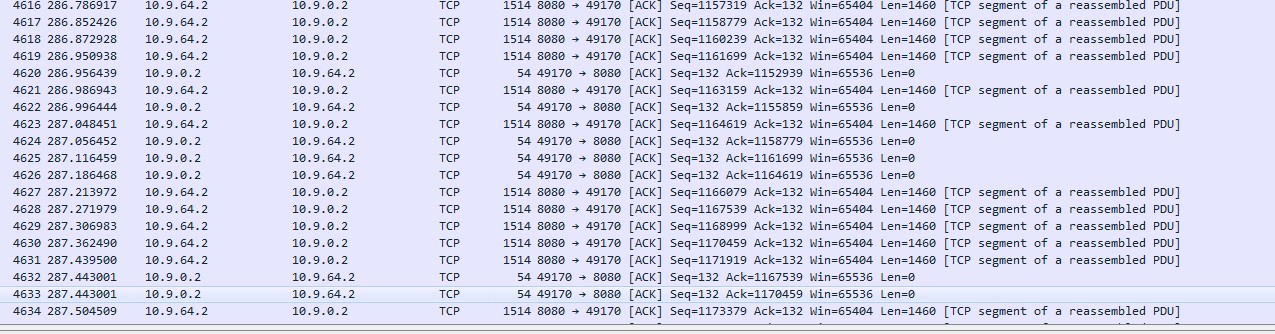
Команда ip multicast-routing включает соответствующий routing, если же он выключен, то роутер не пересылает multicast пакеты.

Рисунок 9 - Передача фрагментов по сети

Как видим, идет постоянная передача фрагментов фильма по сети между источником и приемником.

## ЗАКЛЮЧЕНИЕ

В данном курсовом проекте реализовали сети некоторого предприятия. В которой имеется три сети, объединенных при помощи пяти маршрутизаторов.

Входе курсового проекта настроили сеть в соответствии с заданием и реализовали услугу Internet Protocol Television (IpTV). Ознакомились с программами такие как Graphical Network Simulator3 (GNS3), VirtualBox, WireShark. Также настроили динамическую маршрутизацию, основанную на технологии отслеживания состояния канала Open Shortest Path First (OSPF), систему доменных имен Domain Name System (DNS) и протокол группового вещания версии разряженного режима Protocol Independent Multicast — Sparse Mode (Multicast-PIM-SM). Рамках курсового проектирования задание было реализованно в среде GNS3 и объединили всю сеть маршрутизаторами CISCO семейства 3700 (версия ПО – 3725-adventerprisek9-mz.124-15. T14).

## СПИСОК ЛИТЕРАТУРЫ

1. Олков Е. «Основы GNS3. Обзор» [Электронный ресурс]. - Режим доступа https://habr.com/ru/post/266503/ - Хабр;
2. «Что такое VirtualBox и как ей пользоваться» [Электронный ресурс]. - Режим доступа <https://geekkies.in.ua/crossplatform/chto-takoe-virtualbox-i-kak-ej-polzovatsja.html>- GEEKKIES полезно про PC, Linux, Windows и Web;
3. Нурулин А. «Что такое VLC и как это можно использовать? Часть 1. Знакомство с VLC: установка» [Электронный ресурс]. - Режим доступа [http://linuxsam.org.ua/chto-takoe-vlc-i-kak-eto-](http://linuxsam.org.ua/chto-takoe-vlc-i-kak-eto-mozhno-ispolzovat-chast-1-znakomstvo-s-vlc-ustanovka/) [mozhno-ispolzovat-chast-1-znakomstvo-s-vlc-ustanovka/](http://linuxsam.org.ua/chto-takoe-vlc-i-kak-eto-mozhno-ispolzovat-chast-1-znakomstvo-s-vlc-ustanovka/) - LinuxSam Linux для юзеров;
4. «OSPF» [Электронный ресурс]. - Режим доступа https://ru.wikipedia.org/wiki/OSPF - ВикипедиЯ Свободная энциклопедия;
5. «Protocol Independent Multicast» [Электронный ресурс]. - Режим доступа https://ru.wikipedia.org/wiki/Protocol\_Independent\_Multicast - ВикипедиЯ Свободная энциклопедия;
6. «Wireshark — приручение акулы» [Электронный ресурс]. - Режим доступа https://habr.com/ru/post/204274/ - Хабр;
7. «DNS» [Электронный ресурс]. - Режим доступа https://ru.wikipedia.org/wiki/DNS - ВикипедиЯ Свободная энциклопедия;

**ПРИЛОЖЕНИЕ 1 – Таблица**

Таблица 1 - Разбиение сетевых интерфейсов на максимальное количество подключаемых узлов для коммутаторов

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| вание коммутатора | Network | иапазон IP- адресов | Broadcast | Маска подсети | олученное ество узлов | Требуемое чество узлов |
| SW1 | 10.9.0.0 | .0.1 -10.9.0.62 | 10.9.0.63 | 55.255.255.192 | 62 | 48 |
| SW3 | 10.9.32.0 32 | .1-10.9.35.254 | 10.9.35.255 | 255.255.252.0 | 1022 | 632 |
| SW4 | 10.9.64.0 64 | .1-10.9.71.254 | 10.9.71.255 | 255.255.248.0 | 2046 | 1998 |