МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Казахский национальный исследовательский технический университет
имени К.И. Сатпаева

Институт информационных и телекоммуникационных технологий

Кафедра «Электроника, телекоммуникации и космические технологии»

Махамбетова Б.С.

Анализ виртуальных локальных сетей

ДИПЛОМНАЯ РАБОТА

специальность 5В071900 – Радиотехника, электроника и телекоммуникация

Алматы 2019

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Казахский национальный исследовательский технический университет
имени К.И. Сатпаева

Институт информационных и телекоммуникационных технологий

Кафедра «Электроника, телекоммуникации и космические технологии»

ДОПУЩЕН К ЗАЩИТЕ
Заведующий кафедройЭТиКТ
канд.техн.наук
_____Е. Таштай
"13" 05 2019г

ДИПЛОМНАЯ РАБОТА

На тему: Анализ виртуальных локальных сетей

по специальности 5В071900 – Радиотехника, электроника и телекоммуникация

Выполнила Махамбетова Б.С.

Рецензент
канд.техн. наук, профессор АУЭС
_____А.С. Байкенов
"13" 05 2019г.

Научный руководитель
маг-р техн. наук, лектор
_____Г.М. Байкенова
"13" 05 2019г.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Казахский национальный исследовательский технический университет имени К.И. Сатпаева

Институт информационных и телекоммуникационных технологий

Кафедра «Электроника, телекоммуникации и космические технологии»

5В071900 – Радиотехника, электроника и телекоммуникации

УТВЕРЖДАЮ
Заведующий кафедрой ЭТиКТ
канд.техн.наук
_____ Е. Таштай
"08" 02 2019 г.

ЗАДАНИЕ
на выполнение дипломной работы

Обучающемуся *Махамбетовой Ботагоз Сериковне*
Тема *Анализ виртуальных локальных сетей*
Утверждена приказом Ректора Университета № 1162-б от "16" 10 2018г.
Срок сдачи законченной работы "16" мая 2019г.
Исходные данные к дипломной работе: *базовые концепции Ethernet-коммутации; коммутаторы Cisco Catalyst 2960; маршрутизатор Cisco; стандарт IEEE802.1Q.*
Краткое содержание дипломной работы:
а) Предпосылки внедрения технологии виртуальных локальных сетей (VLAN);
б) Анализ виртуальных локальных сетей;
в)Моделирование и расчет VLAN с использованием программы Cisco Packet Tracer.
Перечень графического материала (с точным указанием обязательных чертежей): *1. Физические топологии для сети 10BASE2 и сети 10BASET с использованием концентратора; 2. Построение VLAN на основе одного коммутатора способом группировки портов; 3. Магистральное соединение VLAN между двумя коммутаторами; 4. Дополнительные 4 байта позволяют использовать технологии QoS и VLAN; 5. Схема расположения отделов компании "AdilGroup".*
Рекомендуемая основная литература: *1. Гергель А.В. Компьютерные сети и сетевые технологи; 2. Амато Вито. Основы организации сетей Cisco; 3. Максим Кульгин «Технологии корпоративных сетей. Энциклопедия».*

ГРАФИК

подготовки дипломной работы (проекта)

Наименования разделов, перечень разрабатываемых вопросов	Сроки представления научному руководителю и консультантам	Примечание
Предпосылки внедрения технологии виртуальных локальных сетей (VLAN)	8.02.2019	выполнено
Анализ виртуальных локальных сетей	22.03.2019	выполнено
Моделирование и расчет VLAN с использованием программы CiscoPacketTracer	21.04.2019	выполнено

Подписи

консультантов и нормоконтролера на законченную дипломную работу (проект) с указанием относящихся к ним разделов работы (проекта)

Наименования разделов	Консультанты, И.О.Ф. (уч. степень, звание)	Дата подписания	Подпись
Нормоконтролер	доктор PhD Тайсариев К.Н	13.05.19	

Научный руководитель _____ Г.М. Байкенова

Задание принял к исполнению обучающийся _____ Б.С. Махамбетова

Дата "__16__"____10_____2018г.

АННОТАЦИЯ

Виртуальные локальные сети (VLAN) являются на сегодняшний день неотъемлемой частью архитектуры любой сети предприятия. VLAN обладает теми же свойствами, что и физическая локальная сеть, но помимо этого, дает возможность конечным станциям группироваться, даже если они расположены разных физических сетях. Подобная реорганизация может быть осуществлена с использованием программного обеспечения вместо физического перемещения устройств.

В дипломной работе проанализирована работа и способы организации виртуальных локальных сетей. Рассмотрены основные преимущества и причины широкого использования данной технологии.

С помощью программы Cisco Packet Tracer показана модель создания VLAN для предприятия. Проведен анализ существующей сети предприятия, из которого был сделан вывод о необходимости внедрения виртуальной локальной инфраструктуры, а также произведены расчеты по распределению трафика в данной сети.

АҢДАТПА

Виртуалды жергілікті желілер (VLAN) бүгінгі таңда кез келген корпоративтік желінің архитектурасының ажырамас бөлігі болып табылады. VLAN физикалық жергілікті желі ретінде бірдей қасиеттерге ие, бірақ одан басқа, әр түрлі физикалық желілерде болса да, соңғы станцияларды бірге топтастыруға мүмкіндік береді. Мұндай қайта құру физикалық қозғалатын құрылғылардың орнына бағдарламалық жасақтаманы пайдалану арқылы жүзеге асырылуы мүмкін.

Дипломдық жұмыста виртуалды жергілікті желілерді ұйымдастырудың жолдары мен жұмысын талдады. Осы технологияны кеңінен қолданудың негізгі артықшылықтары мен себептері қарастырылады.

Cisco Packet Tracer пайдалану арқылы кәсіпорын құру VLAN үлгісі көрсетіледі. Виртуалды жергілікті инфрақұрылымды енгізу қажет болатын, сондай-ақ осы желідегі трафикті бөлу туралы есептер жасалды деп есептелетін қолданыстағы кәсіпкерлік желісін талдау жүргізілді.

ANNOTATION

Virtual local area networks (VLANs) are today an integral part of the architecture of any enterprise network. A VLAN has the same properties as a physical local area network, but beyond that, it allows end stations to group together, even if they are located on different physical networks. Such a reorganization can be carried out using software instead of physically moving devices.

In the thesis work analyzed the work and ways of organizing virtual local area networks. The main advantages and reasons for the wide use of this technology are considered.

Using Cisco Packet Tracer, the enterprise creation VLAN model is shown. The analysis of the existing enterprise network was carried out, from which it was concluded that it was necessary to introduce a virtual local infrastructure, as well as calculations were made on the distribution of traffic in this network.

СОДЕРЖАНИЕ

Введение		9
1	Предпосылки внедрения технологии виртуальной локальной сети в локальных сетях	10
1.1	Принципы построения современных локальных сетей. Базовые концепции коммутации в локальных сетях	10
1.1.1	Методы коммутации. Преимущества и недостатки механизмов коммутации в сетях LAN	11
1.2	Широковещательный домен и домен коллизий	13
1.3	Использование технологии VLAN для эффективной организации работы предприятий	15
1.4	Постановка задачи	18
2	Анализ виртуальных локальных сетей	19
2.1	Функции и назначение VLAN	19
2.2	Создание VLAN на основе одного коммутатора	20
2.2.1	Создание VLAN на основе нескольких коммутаторов	21
2.2.2	Концепции назначения тегов	23
2.3	Протоколы VLAN	24
2.3.1	Протокол VLAN Trunking- VTP	24
2.3.2	Протокол Spanning-Tree – STP	26
2.3.3	VLAN на базе меток – стандарт IEEE 802.1Q	29
2.3.4	Использование сетевого протокола	32
3	Моделирование виртуальных локальных сетей для предприятия	33
3.1	Пример разделения локальной сети предприятия с использованием программы Cisco Packet Tracer	33
3.2	Способ оптимизации прохождения трафика при заданной топологии сети на уровне доступа	41

ВВЕДЕНИЕ

В настоящее время в число важнейших стратегических направлений почти всех крупнейших производителей сетевого оборудования входят виртуальные сети (VLAN). Сложно указать точное время появления концепции "виртуальных сетей" (VLAN) в том виде, в котором она существует сейчас, но можно сказать, что это произошло, когда интеллектуальность производимых коммутаторов начала расти буквально день ото дня.

Около десяти лет назад с целью создания кампусных сетей разработчики использовали ограниченное число аппаратных средств. Традиционная сеть с разделяемой средой передачи не могла предоставить большую полосу пропускания, которая была необходима постоянно увеличивающейся мощности процессоров рабочих станций, появлению мультимедийных приложений и приложений клиент-сервер. Именно эти требования сподвигли проектировщиков к созданию различных технологий для защиты и разделения информации внутри сети. Одной из технологий и является виртуальная локальная сеть - VLAN.

VLAN (англ. Virtual Local Area Network, Виртуальная Локальная Сеть) – это группа устройств, которая взаимодействует напрямую на канальном уровне, несмотря на то, что на физическом уровне все эти устройства подключены к разным коммутаторам. К достоинствам виртуальной локальной сети по сравнению с другими LAN можно отнести:

- гибкое разделение устройств на группы: то есть, одному VLAN соответствует одна подсеть. Компьютеры, которые располагаются в разных VLAN, будут изолированы друг от друга.
- сокращение широковещательного трафика в сети: каждый VLAN определяет отдельный широковещательный домен. Широковещательный трафик не будет транслироваться между разными VLAN.
- сокращение числа оборудования и сетевого кабеля: при создании новой виртуальной локальной сети нет необходимости покупать и устанавливать коммутатор и прокладку сетевого кабеля.

Моя дипломная работа посвящена анализу виртуальных локальных сетей и методам их реализации.

1 Предпосылки внедрения технологии виртуальной локальной сети

1.1 Принципы построения современных локальных сетей. Базовые концепции коммутации в локальных сетях

С момента создания первых локальных сетей, было разработано большое количество самых различных сетевых технологий, но, несмотря на это, большое распространение смогли получить немногие из них. Это, в первую очередь, связано с высоким уровнем стандартизации принципов организации сетей и с поддержкой их известными компаниями. Но при всем этом, стандартные сети не всегда обладают наилучшими характеристиками и могут обеспечить наиболее благоприятные режимы обмена. Но основными и большими преимуществами технологий являются большие объемы выпуска их аппаратуры и ее невысокая стоимость. Важным фактором также является то, что разработчики программных средств, прежде всего, обращают внимание на самые распространенные сети. Вследствие этого, пользователь, который выбирает стандартные сети, обладает полной гарантией взаимосовместимости аппаратуры и программ. В данный момент постепенное уменьшение количества типов, которые используют сети, становится тенденцией. Причина кроется в том, что для увеличения скорости передачи в локальных сетях до 100 и даже до 1000 Мбит/с также требуется применение самых новейших технологий и осуществление достаточно дорогостоящих научных исследований. Разумеется, это могут позволить себе только крупнейшие фирмы, поддерживающие свои стандартные сети и их более совершенные разновидности.

Наиболее распространенной среди стандартных сетей стала сеть под названием Ethernet. Первым вариантом технологии Ethernet была физическая шинная топология, в основе которой лежал коаксиальный кабель. Следующим не менее распространенным вариантом технологии стал стандарт 10BASET, который благодаря тому, что проблемы, возникшие в одном кабеле, не влияли на всю остальную сеть (что является характерной ситуацией для сетей 10BASE2 и 10BASE5 с топологией разделяемой шины) был намного надежнее. В технологии 10BASET была использована неэкранированная витая пара, которая была намного дешевле, чем коаксиальный кабель [3]. Более того, благодаря тому, что многие организации использовали витую пару для телефонии, стандарт 10BASET в короткие сроки стал разумной альтернативой Ethernet сетям стандартов 10BASE2 и 10BASE5. Типичные топологии для сети стандарта 10BASE2 и сети 10BASET с использованием концентратора показаны на рисунке 1.1.

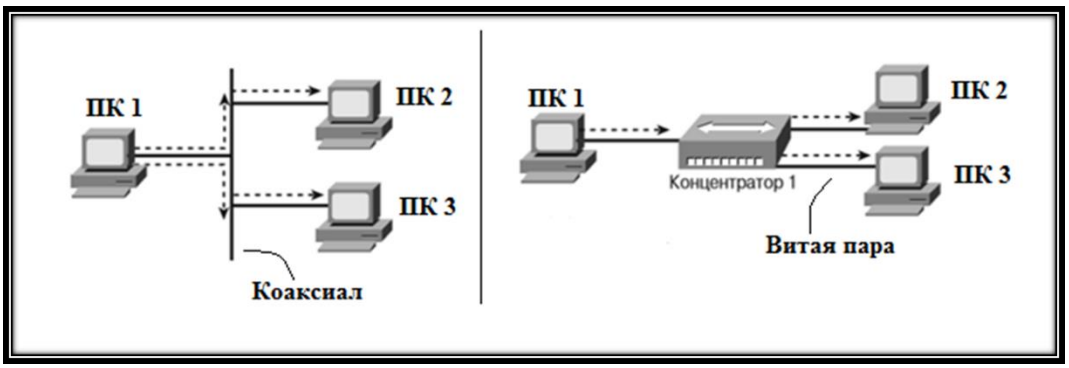

Рисунок 1.1 - Физические топологии для сети 10BASE2 и сети 10BASET с использованием концентратора

Тем не менее, невзирая на то, что технология 10BASET была значительным продвижением в эволюции сетевых технологий, она все же обладала несколькими значительными недостатками, которые связаны с применением концентраторов:

- фрейм, который передается любым имеющимся устройством, может стать причиной коллизии в сети, при условии, если он ‘‘столкнется’’ с фреймом, передаваемым от другого устройства, который находится в том же самом сегменте;
- только одно устройство из всех имеющихся имеет возможность передавать фрейм в один временной промежуток, другими словами устройства в одном сегменте работают в режиме конкуренции и разделяют общую полосу пропускания (в 10 Мбит/с);
- широковещательные фреймы, которые отправляются одним устройством, будут получены и обработаны всеми устройствами, которые находятся в данной локальной сети [3].

В то время, когда три стандарта Ethernet, которые были описаны выше, были разработаны, полоса пропускания в 10 Мбит, которую они разделяли, казалась гигантской величиной! До появления локальной сети (LAN), для работы очень часто применялись более простые терминалы, которые подключались к центральному серверу в сети с помощью канала в 56 Кбит/с. После разработки технологии 10BASET Ethernet, ее скорость оказалась удивительной для того времени.

Через некоторое время, производительность Ethernet сетей стала постепенно снижаться. Разработчики программного обеспечения начали создавать приложения, которые использовали довольно таки большую полосу пропускания в локальной сети. В локальных сетях стали появляться такие проблемы, как заторы трафика, так как устройства в одном и том же сегменте Ethernet были неспособны передавать больше чем 10 Мбит/с потоков данных, помимо этого они еще и разделяли данную полосу пропускания между собой. В результате увеличения объемов трафика стало возникать большое количество коллизий в локальных сетях.

1.1.1 Методы коммутации. Преимущества и недостатки механизмов коммутации в сетях LAN

При принятии решения о передаче фрейма, коммутатор может воспользоваться одним из механизмов передачи, которые будут рассмотрены далее. Большая часть устройств на данный момент применяет метод коммутации с буферизацией фреймов (англ. Store and forward), но, несмотря на это, все рассмотренные далее методы внутренней обработки потоков данных реализованы и применяются в различных устройствах.

Большая часть прозрачных мостов и коммутаторов в настоящее время использует метод коммутации с буферизацией фреймов (англ. Store and forwar dprocessing). В данном методе, прежде чем начать передачу первого бита фрейма через выходной интерфейс, устройство должно получить фрейм полностью. Известны еще два метода внутренней обработки фреймов: сквозная коммутация (англ. cutthrough) и бесфрагментная коммутация (англ. Fragment free). Благодаря тому, что MAC адрес получателя располагается в начале Ethernet заголовка, коммутатор может начать пересылку еще до того, как он получит весь фрейм. Сквозная и бесфрагментная коммутации работают по такому принципу, то есть передача начинается задолго до того, как будет получен весь фрейм, из этого следует, что время обработки и передачи (т.е. задержка, delay) значительно уменьшается [3].

Метод сквозной коммутации (англ. cutthrough) заключается в том, что устройство начинает пересылку фрейма сразу же после принятия той части заголовка, которая содержит адрес назначения. Особенностью данного метода коммутации является то, что он значительно снижает задержку в сети, но имеет недостаток в виде распространения ошибок в сети. В результате того, что контрольная сумма фрейма (англ. Frame check sequence FCS) располагается в Ethernet концевике, перед началом пересылки, коммутатор не имеет возможности определить, имеются ли какие-либо ошибки во фрейме. При использовании данного метода коммутации, важно учитывать две основные особенности: задержка за счет обработки фреймов устройством заметно снижается, но результатом этого является последующая передача фрейма с имеющимися ошибками.

Метод бесфрагментной коммутации (англ. Fragment freep rocessing) работает по тому же принципу, что и метод сквозной коммутации, но отличается значительно меньшим числом ошибок, передающихся через устройство. Отличительной особенностью технологии CSMA/CD (англ. Carrier Sense Multiple Access With Collision Detection - множественный доступ с контролем несущей и обнаружением коллизий) является то, что большое число коллизий существуют на первых 64 байтах фрейма. Сходство бесфрагментной коммутации и сквозной коммутации заключается в том, что в бесфрагментной коммутации передача начинается только после получения 64 байтов передаваемого фрейма. Задержка из-за обработки фрейма коммутатором в

таком случае значительно уменьшается, в сравнении с методом коммутации с буферизацией, но при этом будет превышать время задержки сквозного метода. Количество ошибок, которое посылается устройством, также будет значительно меньше, чем в методе коммутации с буферизацией.

В настоящее время большая часть рабочих станций подключены к сети с помощью соединений со скоростью 100 Мбит/с, вышестоящие каналы обычно работают на скорости 1 Гбит/с, в коммутаторах применяются специализированные микросхемы (англ. Application Specific Integrated Circuits, ASIC), которые работают на очень высокой скорости и предназначены для аппаратной обработки потоков данных. Следовательно, в нынешних коммутаторах по большей части применяется метод коммутации с буферизацией фреймов, так как на таких скоростях передачи данных заметного уменьшения задержки не происходит.

Внутренние механизмы обработки фреймов в коммутаторах значительно отличаются в зависимости от производителей, но, несмотря на это, все методы можно свести к трем основным или к некоторым их производным, которые были описаны выше.

В коммутаторах также имеется большое количество дополнительных функций, которые отсутствуют в устаревших устройствах для локальных сетей (LAN), например, концентраторы и мосты. Основные преимущества коммутаторов перечислены далее.

В случаях, когда к порту коммутатора подключается всего одно сетевое устройство, он выполняет микросегментацию сети и предоставляет выделенную полосу пропускания для устройства.

Коммутаторы дают возможность осуществить пересылку множественных одновременных потоков данных между устройствами, которые подключены к разным интерфейсам.

В случаях, когда к порту коммутатора подключается только одно сетевое устройство, которое работает в дуплексном режиме, эффективная полоса пропускания увеличивается вдвое.

Коммутаторы имеют возможность выполнять согласование скорости, что означает, что устройства, которые подключены через разные по скорости технологии Ethernet, способны взаимодействовать через коммутатор, но не через концентратор.

1.2 Широковещательный домен и домен коллизий

Два значимых принципа сегментации локальных компьютерных сетей могут быть описаны двумя терминами: домен коллизий (англ. Collision domain) и широковещательный домен (англ. Broadcast domain).

Домены коллизий.

Домен коллизий является набором интерфейсов локальной сети, фреймы данных интерфейсов имеют возможность вступать в коллизии друг с другом, но это не относится к фреймам от остальных устройств в сети. На рисунке 1.2 можно увидеть иллюстрацию доменов коллизий.

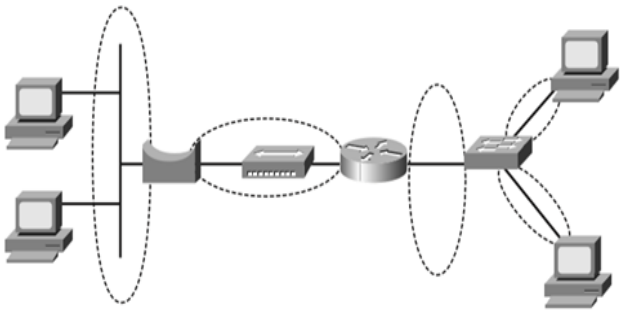

Рисунок 1.2 - Домены коллизий

Коммутатор, который изображен на правой стороне схемы, подразделяет локальную сеть на отдельные домены коллизий на каждом порту. Соответственно, маршрутизатор и мост подразделяют сеть на отдельные домены коллизий. Из всех присутствующих на схеме устройств только концентратор, который изображен в центре схемы сети, не создает множество раздельных доменов коллизий для каждого интерфейса. Это устройство выполняет функцию повторения фреймов на всех своих портах без буферизации и задержки фрейма перед передачей в загруженный сегмент сети.

Широковещательный домен.

Термин широковещательный домен (англ. Broadcast domain) применяется для описания определенного участка сети, на котором могут распространяться широковещательные фреймы. Широковещательный домен состоит из набора устройств, который обеспечивает получение и обработку широковещательного сообщения всеми устройствами в случаях, когда одно устройство передает данное широковещательное сообщение. В частности, в результате того, что коммутаторы передают все широковещательные и многоадресатные сообщения через все свои порты, коммутатор создает единый широковещательный домен. В качестве барьера между широковещательными фреймами выступают маршрутизаторы, их функцией является не пропускать фреймы через себя. На рисунке 1.3 проиллюстрированы границы широковещательных доменов для схемы сети, показанной на рисунке 1.2.

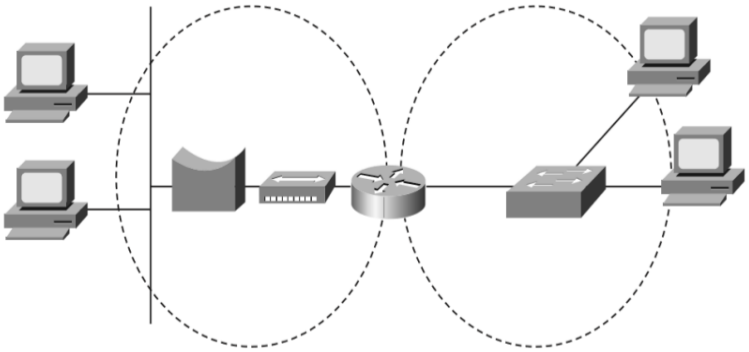

Рисунок 1.3 - Широковещательные домены

Широковещательное сообщение, которое было отправлено одним устройством в широковещательном домене, не передается устройствам в другом широковещательном домене. В примере, показанном на рисунке 1.3, имеется два широковещательных домена, т.е. маршрутизатор не будет передавать широковещательные фреймы, отправленные компьютером, который изображен на схеме слева, в сетевой сегмент, который проиллюстрирован на схеме справа.

1.3 Использование технологии VLAN для эффективной организации работы предприятий

Первоначально коммутаторы не имели возможности обеспечивать создание виртуальных локальных сетей, поскольку они применялись для непосредственной пересылки фреймов между устройствами. В результате того, что концентраторы коллективного доступа к среде передачи данных были не в состоянии справляться с увеличивающимися запросами на расширение полосы пропускания сети в связи с применением приложение клиент-сервер, которые обеспечивали Графический Интерфейс Пользователей (GUI), рынок коммутаторов быстро расширялся.

Коммутатор работает с кадрами “интеллектуально”, то есть он считывает MAC адрес поступающего, или входящего, кадра и сохраняет полученную информацию в таблице коммутации. Таблица коммутации содержит MAC адреса сети и номера портов, которые связаны с ними. После создания такой таблицы, коммутаторы проверяют каждый кадр, который был занесен в память, и записывают новые адреса, которые отсутствуют в таблице. В качестве примера на рисунке 1.4 показана таблица коммутации коммутатора [5].

```
Cat5500> show cam dynamic
VLAN        Destination MAC        Destination Ports or VCs
----------  ---------------------  ------------------------
1           00-60-2f-9d-a9-00      3/1
1           00-b0-2f-9d-b1-00      3/5
1           00-60-2f-86-ad-00      5/12
1           00-c0-0c-0a-bd-4b      4/10
Cat5500>
```

Рисунок 1.4 - Таблица коммутации

По мере того, как технологии улучшались и захватывали рынок, стали появляться виртуальные локальные сети – VLAN.

В настоящее время в число важнейших стратегических направлений почти всех крупнейших производителей сетевого оборудования входят виртуальные сети (VLAN). Указать точное время появления концепции "виртуальных сетей" в том виде, в котором она существует сейчас сложно, но можно сказать, что это произошло, когда интеллектуальность производимых коммутаторов начала расти буквально день ото дня.

VLAN (от англ. Virtual Local Area Network) - топологическая, или виртуальная, локальная сеть. VLAN - это логическое комбинирование некоторого числа конечных станций в одном сегменте (широковещательном домене) на канальном уровне, даже если они физически подключены к разным коммутаторам. VLAN позволяет полностью изолировать трафик группы узлов от остальной сети [1].

Технология виртуальных локальных сетей является очень востребованной, благодаря ряду преимуществ:

1) VLAN помогает структурировать сеть – возможность выделения в отдельную сеть отдела организации или группы компьютеров (например, сегмента серверов, обычных пользователей, ip-телефонов, ip-видеокамер и т.д), используя общий коммутатор (рис.1.5);

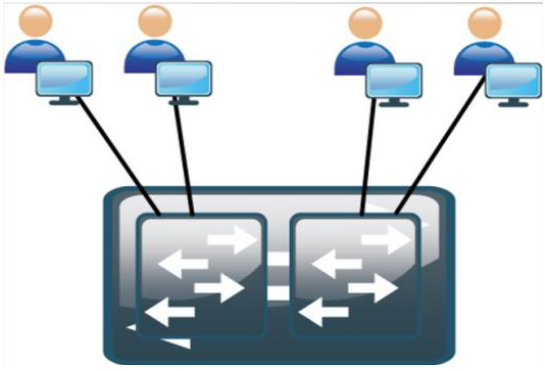

Рисунок 1.5 – Структурирование сети с помощью общего коммутатора при организации VLAN

2) VLAN используется для обеспечения безопасности – например, при разделении сети гостевых пользователей и сети серверов, злоумышленники не будут иметь доступ в другой сегмент сети, так как пользователи разных сегментов могут взаимодействовать только на сетевом уровне, то есть с помощью маршрутизатора;

3) VLAN используется для объединения пользователей на канальном уровне, даже при подключении к разным физическим коммутаторам. Благодаря данной технологии, нет необходимости в протягивании кабеля от пользователя до нужного свитча, достаточно, link-а между коммутаторами (рис.1.6).

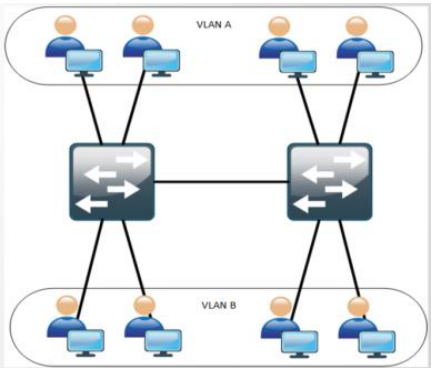

Рисунок 1.6 – Объединение пользователей на канальном уровне при организации VLAN

4) VLAN уменьшает количество широковещательного трафика. Каждый VLAN - это отдельный широковещательный домен, внутри которого передаются широковещательные кадры. Создание дополнительных VLAN-ов на коммутаторе означает разбиение коммутатора на несколько широковещательных доменов, благодаря чему, при генерировании широковещательного запроса пользователем, данный запрос получат только пользователи данного широковещательного домена.

В коммутаторах могут использоваться три типа VLAN:

– VLAN на базе портов;
– VLAN на базе MAC-адресов;
– VLAN на основе меток в дополнительном поле кадра - стандарт IEEE 802.1Q.

Организация VLAN на базе портов и MAC адресов, является устаревшей и не рекомендуется для применения в современных реализациях виртуальных сетей.

Стандарт IEEE 802.1Q определяет изменения в структуре кадра Ethernet, позволяющие передавать информацию о VLAN по сети. С точки зрения удобства и гибкости настроек, VLAN на основе меток является лучшим решением. Его основные преимущества - это гибкость и удобство в настройке и изменении – добавление меток позволяет VLAN распространяться через множество 802.1Q-совместимых коммутаторов по одному физическому соединению. VLAN 802.1Q позволяет VLAN работать с коммутаторами и

сетевыми адаптерами серверов и рабочих станций, которые не распознают метки. В силу указанных свойств, VLAN на базе тэгов используются на практике гораздо чаще остальных типов.

С использованием VLAN, один коммутатор имеет возможность создать два широковещательных домена. Коммутатор VLAN также способен настроить часть интерфейсов на один широковещательный домен, а часть на другой, в результате чего, будет создано два широковещательных домена. Данные индивидуальные широковещательные домены, которые были созданы коммутатором, и являются виртуальными локальными сетями (англ. virtual LAN — VLAN).

1.4 Постановка задачи

Цель моей дипломной работы – провести анализ работы виртуальных локальных сетей. Для этого я должна выполнить следующие задачи:

- сделать общий обзор построения современных локальных сетей;
- рассмотреть основные причины и преимущества создания виртуальных локальных сетей;
- проанализировать основные функции и назначения VLAN;
- изучить типы и протоколы VLAN;
- рассмотреть примеры организации VLAN и произвести распределение трафика в данной сети.

Первые две задачи я выполнила в первой главе моей работы. Резюмируя, их можно сказать следующее.

Как уже было сказано ранее, VLAN (англ. Virtual Local Area Network, Виртуальная Локальная Сеть) – это группа устройств, которая взаимодействует напрямую на канальном уровне, несмотря на то, что на физическом уровне все эти устройства подключены к разным коммутаторам. К достоинствам виртуальной локальной сети по сравнению с другими LAN можно отнести:

- гибкое разделение устройств на группы: то есть, одному VLAN соответствует одна подсеть. Компьютеры, которые располагаются в разных VLAN, будут изолированы друг от друга.
- сокращение широковещательного трафика в сети: каждый VLAN определяет отдельный широковещательный домен. Широковещательный трафик не будет транслироваться между разными VLAN.
- сокращение числа оборудования и сетевого кабеля: при создании новой виртуальной локальной сети нет необходимости покупать и устанавливать коммутатор и прокладку сетевого кабеля.

2 Анализ виртуальных локальных сетей

2.1 Функции и назначение VLAN

Основным назначением технологии VLAN является облегчение процесса изолирования сетей, которые впоследствии будут связаны маршрутизаторами, реализующими один из протоколов сетевого уровня, например, IP. Данный вид организации сети позволяет обеспечивать достаточно мощные барьеры на пути ошибочного трафика, при его передаче из одной сети в другую. На данный момент можно считать, что каждая большая сеть обязана иметь маршрутизаторы, так как в противном случае потоки ошибочных кадров, например, широковещательных, могут время от времени «затапливать» всю сеть через коммутаторы, тем самым приводя сеть в неработоспособное состояние. Технология виртуальных сетей позволяет организовать основу для построения крупной сети, которая связана маршрутизаторами, так как коммутаторы дают возможность создавать полностью изолированные сегменты программным путем, то есть без использования физической коммутации. До изобретения технологии VLAN в целях создания отдельной сети применялись сегменты коаксиального кабеля, которые были физически изолированы друг от друга или сегменты, который строились на повторителях и мостах и не были связаны друг с другом. После чего данные сети соединялись маршрутизаторами в единую составную сеть.

Под изменением состава сегментов (например, переход пользователя из одной сети в другую или разделение более крупных сегментов) в данном случае понимается физическая перекоммутация разъемов, находящихся на передних панелях повторителей или в кроссовых панелях, а это в свою очередь не практично в крупных сетях, так как подразумевает большое количество физической работы и достаточно высокую вероятность ошибки. По этой причине, чтобы исключить физическую перекоммутацию разъемов, начали использовать многосегментные концентраторы, это, в свою очередь, позволило программировать состав разделяемого сегмента без физической перекоммутации. Тем не менее, использование концентраторов для изменения состава сегментов создает значительные ограничения для структуры сети — число сегментов такого повторителя достаточно мало, из-за чего невозможно предоставить каждому узлу свой сегмент, как это происходит при использовании коммутатора. Помимо этого, в данном случае всем процессом передачи данных между сегментами будут управлять маршрутизаторы, а коммутаторы, имея высокую производительность, будут “бездельничать”. По этой причине сети, которые построены с помощью повторителей с конфигурационной коммутацией, все еще работают на основе дробления среды передачи данных между большим числом узлов и имеют значительно меньшую производительность по сравнению с сетями, которые построены на основе

коммутаторов. Применение технологии виртуальных сетей в коммутаторах позволяет решить две задачи:

- повышение производительности в каждой из виртуальных сетей, так как коммутатор передает кадры в подобной сети только узлу назначения;
- изоляция сетей друг от друга для управления правами доступа пользователей и создания защитных барьеров на пути широковещательных штормов [4].

Для соединения виртуальных сетей в единую общую сеть необходимо использование сетевого уровня. Сетевой уровень может быть реализован в отдельном маршрутизаторе, а также имеет возможность работать в составе программного обеспечения коммутатора, который в таком случае является комбинированным устройством — так называемым коммутатором 3-го уровня. Технология образования и работы виртуальных сетей с использованием коммутаторов достаточное количество времени не была стандартизирована, несмотря на то, что была реализована в очень широком спектре моделей коммутаторов различных производителей. Но ситуация изменилась после принятия в 1998 году стандарта IEEE 802.1Q, который имеет возможность определять основные правила построения виртуальных локальных сетей, которые не зависят от протокола канального уровня, который поддерживается коммутатором. Из-за позднего появления стандарта на VLAN крупные производители коммутаторов создали свои технологии виртуальных сетей, которые были несовместимы с технологиями других производителей. По этой причине, несмотря на появление стандарта, очень часто можно наблюдать такую ситуацию, когда виртуальные сети, которые созданы на коммутаторах одного производителя, не распознаются и не поддерживаются коммутаторами другого производителя.

2.2 Создание VLAN на основе одного коммутатора

Для создания виртуальных сетей на основе одного коммутатора чаще всего применяется способ группирования в сети портов коммутатора, при котором каждый порт причисляется определенной виртуальной сети. Широковещательный кадр, поступивший от порта, который относится, например, к виртуальной сети 1, никогда не будет отправлен порту, который не находится в данной виртуальной сети. Порт также можно отнести к нескольким виртуальным сетям, но на практике данный способ используется редко, так как исчезает эффект полной изоляции сетей.

Наиболее логичным и распространенным способом создания VLAN является группирование портов для одного коммутатора, так как виртуальных сетей, построенных на основе одного коммутатора, не может быть больше, чем портов. В случаях, когда к одному порту подсоединен сегмент, который создан на основе повторителя, нецелесообразно подключать узлы данного сегмента к

разным виртуальным сетям, так как в любом случае трафик этих узлов останется общим. Для образования виртуальных сетей на основе группирования портов достаточно причислить каждый порт к одной из нескольких уже названных виртуальных сетей, то есть от пользователя не требуется большого объема ручной работы. Чаще всего данный процесс производится с использованием специальной программы, которая прилагается к коммутатору. Администратор образует виртуальные сети с помощью перемещения мышью графических символов портов на графические символы сетей.

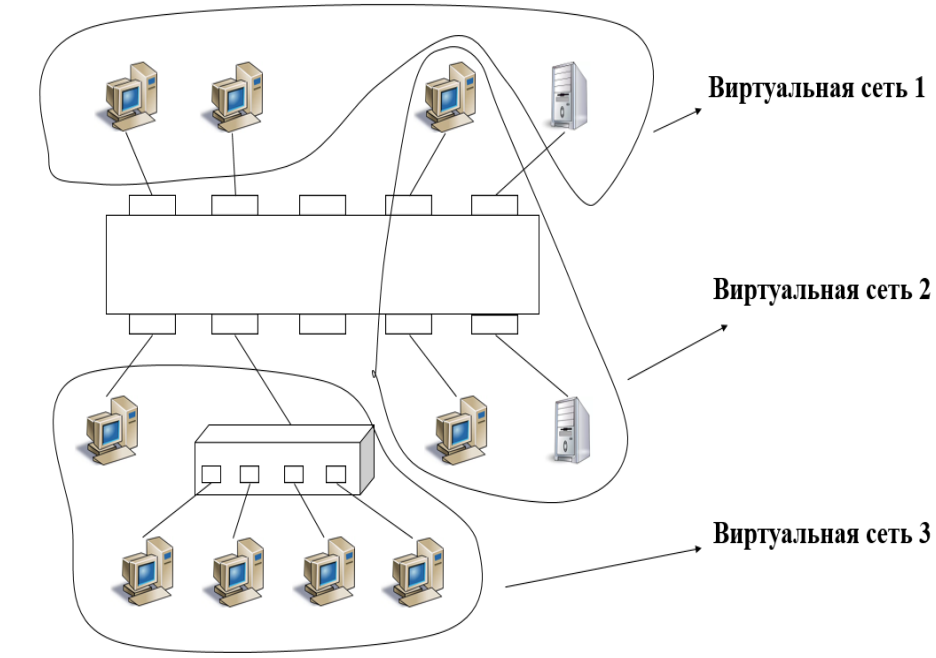

Рисунок 2.1 - Построение VLAN на основе одного коммутатора способом группировки портов

Следующим способом создания виртуальных сетей после группировки портов является группирование MAC-адресов. Каждый MAC-адрес, принятый коммутатором, причисляется какой-либо виртуальной сети. В случаях, когда в сети существует большое количество узлов, данный способ требует выполнения множества ручной работы от администратора. Но при образовании виртуальных сетей на основе нескольких коммутаторов данный способ является более удобным, чем способ группирования портов.

2.2.1 Создание VLAN на основе нескольких коммутаторов

Создание сети VLAN на основе одного коммутатора не требует многого: достаточно настроить каждый порт таким образом, чтобы задать ему номер VLAN, в которой он находится. В случаях, когда присутствует более одного

коммутатора необходимо брать во внимание и другие дополнительные способы перенаправления трафика между ними.

При использовании сети VLAN в сетях с некоторым количеством связанных между собой коммутаторов, на каналах связи, которые находятся между ними, используется магистральное соединение VLAN (англ. VLAN trunking). Магистральное соединение VLAN предполагает применение коммутаторами процесса назначения тегов VLAN (англ. VLAN tagging), при котором перед началом передачи фрейма через магистральный канал коммутатор дополняет данный фрейм другим заголовком. Данный дополнительный заголовок состоит из поля идентификатора VLAN (англ. VLAN ID), который дает возможность передающему коммутатору сопоставлять фрейм с определенной сетью VLAN, а принимающему коммутатору определить, к какой конкретно VLAN относится этот фрейм [5].

На рисунке 2.2 можно увидеть пример двух сетей VLAN с несколькими коммутаторами, однако, без использования магистрального соединения. В данном случае применяются две сети VLAN: VLAN 10 и VLAN 20. Каждой из сетей VLAN принадлежит по два порта на каждом коммутаторе, следовательно, каждая сеть VLAN присутствует в обоих коммутаторах. Для перенаправления трафика сети VLAN 10 между двумя коммутаторами, к которым она принадлежит, данная схема предполагает присутствие канала связи между ними, который в полном объеме располагается в сети VLAN 10. Точно также, для обеспечения трафика сети VLAN 20 между коммутаторами находится второй канал связи, уже полностью находящийся в сети VLAN 20.

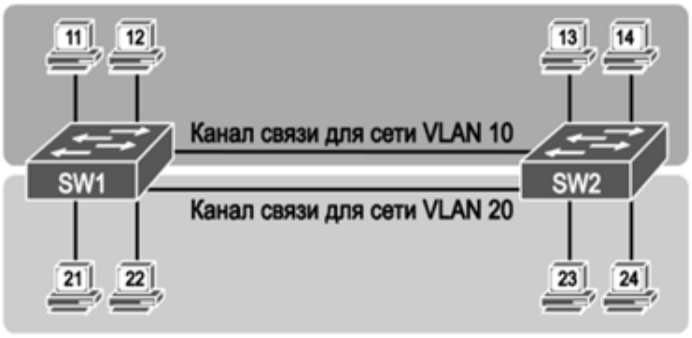

Рисунок 2.2 - Сети VLAN при присутствии нескольких коммутаторов, однако без магистрального соединения

Компьютер ПК11 (находящийся в сети VLAN 10) в полной мере имеет возможность передать фрейм компьютеру ПК14. Фрейм направится на коммутатор SW1, после чего через канал связи (предназначенный для VLAN 10) направится на коммутатор SW2. Однако, несмотря на то, что данная схема работает, ее масштабирование является нелегкой задачей. Для работы каждой сети VLAN необходим отдельный физический канал связи между коммутаторами. Например, при необходимости наличия 10 или 20 сетей VLAN,

необходимо расположить между коммутаторами 10 или 20 каналов связи и применить для них 10 или 20 портов на каждом коммутаторе.

2.2.2 Концепции назначения тегов

Магистральное соединение VLAN образует между коммутаторами один канал связи, который может поддерживать такое количество сетей VLAN, которое необходимо. Для коммутаторов данный магистральный канал будет являтся частью всех VLAN. Но несмотря на это, трафик в магистральном канале VLAN будет раздельным, и фреймы VLAN 10 никак не смогут попасть на устройства VLAN 20 (и наоборот), так как, проходя через магистральный канал, каждый фрейм обозначен номером VLAN. На рисунке 2.3 можно увидеть схему сети с одним физическим каналом связи между двумя коммутаторами.

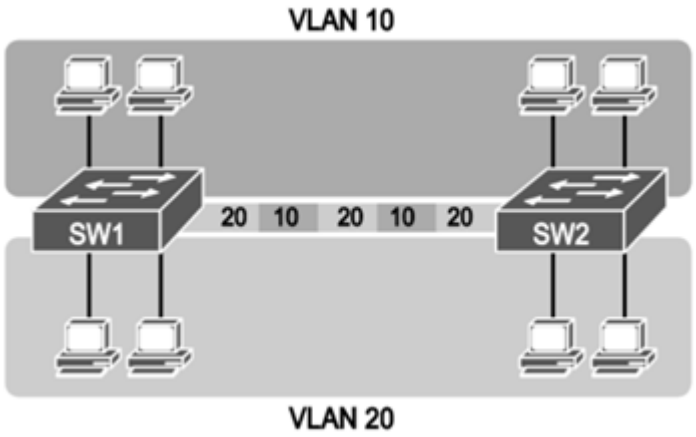

Рисунок 2.3 - Сети VLAN с несколькими коммутаторами и магистральным соединением

Магистральное соединение дает возможность коммутаторам переслать фреймы некоторого количества сетей VLAN по одному физическому каналу благодаря дополняет фрейм Ethernet небольшим заголовком. Пример, который можно увидеть на рисунке 2.4 показывает пересылку компьютером ПК11 широковещательного фрейма на интерфейсе Fa0/1 (этап 1). Для осуществления лавинной рассылки коммутатору SW1 необходимо перенаправить широковещательный фрейм на коммутатор SW2. Но при этом коммутатор SW1 обязан каким-нибудь способом сообщить коммутатору SW2, что данный фрейм принадлежит сети VLAN 10, для того, чтобы после его принятия произвести лавинную рассылку только в сети VLAN 10, а не VLAN 20. Как можно увидеть на этапе 2, перед пересылкой фрейма коммутатор SW1 дополнил исходный фрейм Ethernet заголовком VLAN, в котором указывается информация о том, к какой VLAN принадлежит данный фрейм (в данном случае VLAN 10).

Рисунок 2.4 - Магистральное соединение VLAN между двумя коммутаторами

После получения коммутатором SW2 данного фрейма, он получает информация о том, что фрейм относится к сети VLAN 10. После чего коммутатор SW2 убирает заголовок VLAN и пересылает первоначальный фрейм по интерфейсу к VLAN 10 (этап 3). В качестве другого примера можно рассмотреть случай, когда компьютер ПК21 (находящийся в сети VLAN 20) передает широковещательный фрейм. Коммутатор SW1 передает данный фрейм через порт Fa0/4 (так как этот порт принадлежит сети VLAN 20) и порт Gi0/1 (так как это магистральный канал, что означает, что он поддерживает несколько разных сетей VLAN).

Коммутатор SW1 дополняет фрейм заголовком магистрали, который состоит из идентификатора VLAN 20. Определив, что фрейм принадлежит сети VLAN 20, коммутатор SW2 убирает магистральный заголовок и пересылает его только на порты Fa0/3 и Fa0/4, так как они принадлежат сети VLAN 20, но не на порты Fa0/1 и Fa0/2, так как они принадлежат сети VLAN 10.

2.3 Протоколы VLAN

2.3.1 Протокол VLAN Trunking - VTP

В случаях, когда в сети имеется немалое число коммутаторов, настройка всех имеющихся VLAN на каждом из коммутаторов является достаточно нелегкой. Именно поэтому был создан магистральный (транкинговый) протокол виртуальных сетей VTP (VLAN Trunking Protocol). Протокол VTP представляет собой протокол локальной вычислительной сети, который предназначен для обмена данными о VLAN.

Протокол создания магистральных каналов виртуальной локальной сети (VTP) подразумевает удобное дополнение к средствам управления виртуальными локальными сетями. Он дает возможность в автоматическом

режиме устанавливать виртуальные локальные сети сразу некоторому числу коммутаторов в сети [2].

Для того, чтобы можно было рассмотреть удобство применения данного протокола, нужно представить себя на месте сетевого администратора в большой неоднородной сети. Допустим, что в данной сети содержится 500 коммутаторов и больше 100 виртуальных локальных сетей. Чтобы виртуальные локальные сети могли обмениваться информацией по магистральным каналам в соответствии с их определениями, необходимо, чтобы номера виртуальных локальных сетей были одинаковыми во всех коммутаторах, которые принимают участие в формировании данных сетей на предприятии. Также, нужно помнить для чего предназначены определенные виртуальные локальные сети, например, "данная сеть — предназначена для высшего руководства, данная — для обычных служащих" и т.д. Даже такие типичные характеристики дают возможность понять, какие сложности могут возникнуть при настройке конфигурации виртуальных локальных сетей в такой большой сети. Например, представьте себе, что может произойти если пользовательский порт будет помещен не в ту виртуальную локальную сеть, в какую требуется, из-за того, что кто-то по ошибке ввел параметр VLAN 151 вместо VLAN 115?

С целью решения данной проблемы программное обеспечение протокола VTP позволяет в автоматическом режиме привести в действие определения виртуальных локальных сетей от имени сетевого администратора, это, в свою очередь, дает возможность установить на одном коммутаторе имена и номера виртуальных локальных сетей, после чего, распространить эти данные по всему предприятию. Важно помнить, что программное обеспечение VTP не распространяет по всем коммутаторам данные о том, к какой виртуальной локальной сети относится определенное устройство (так как, в большинстве сетей эти действия могут привести к разрушительным последствиям); на другие коммутаторы передаются только определения (имя, номер и другие основные данные).

Чтобы достичь данной цели программное обеспечение VTP в первую очередь (после ввода протокола VTP в действие) анонсирует данные о конфигурации виртуальной локальной сети через все магистральные порты. Следовательно, находящиеся рядом коммутаторы получают информацию о наличии в топологии виртуальных локальных сетей и об их конфигурации. После этого, данные коммутаторы распространяют данные о виртуальных локальных сетях по подключенным к ним коммутаторам и т.д.

Программное обеспечение VTP работает в коммутаторе в трех режимах: клиентском, серверном и прозрачном.

Клиентский режим. В данном режиме коммутатор осуществляет прием и передачу анонсов VTP, относящихся к его домену управления. После чего, коммутатор дополняет свою конфигурацию виртуальной локальной сети изменениями. В то время, как коммутатор находится в клиентском режиме, какие-либо изменения в конфигурацию виртуальной локальной сети не могут быть внесены. По этой причине, изменения в конфигурацию виртуальной

локальной сети коммутатора, который находится в клиентском режиме, можно внести с использованием протокола VTP.

Серверный режим. В данном режиме коммутатор тоже производит прием и передачу анонсов VTP, но помимо этого также создает новые анонсы. Данный режим дает возможность производить модификацию данных виртуальной локальной сети непосредственно в самом коммутаторе, а также может осуществлять добавление и удаление виртуальных локальных сетей из домена управления. Модификация конфигурации MEP домена управления способствует обновлению номера версии конфигурации (а также номера версии базы данных VTP). Подобное обновление заставляет все находящиеся в домене управления коммутаторы обновить свои конфигурации VTP с учетом новых данных. Следует отметить, что в каждом домене управления необходимо наличие одного-двух серверов VTP; помимо этого, нужно внимательно контролировать соблюдение прав на модификацию конфигурации данных коммутаторов. Иначе, могут возникнуть ошибки, которые впоследствии будут распространятся по всему домену управления.

Прозрачный режим. Данный режим позволяет перенаправлять данные, но информация о конфигурации виртуальных локальных сетей, которая находится в данных анонсах, игнорируются. В данном режиме позволяется осуществлять изменения конфигурации виртуальных локальных сетей в коммутаторе, но подобные изменения в конфигурации будут относиться только к данному локальному коммутатору [6].

2.3.2 Протокол Spanning-Tree - STP

Одним из распространенных способов защиты сети от обрыва кабеля является образование резервных соединений. Но, при резервировании соединений возникает коммутационная петля, показанная на рисунке 2.3. В результате образования петли, пересылаемые по сети пакеты будут зацикливаться. По этой причине в современные коммутаторы уже встроена защита от зацикливания пакетов, блокирующая пересылку информации по резервным линиям до того момента, пока основные линии связи являются работоспособными.

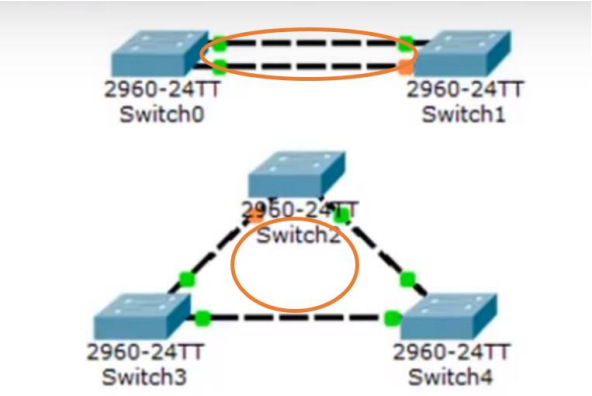

Рисунок 2.3 – Коммутационные петли

Образование коммутационных петель приводит к образованию следующих проблем, которые, в свою очередь, могут привести к неработоспособности всей сети:

1) широковещательные штормы,
2) множественные копии кадров,
3) множественные петли.

С целью предотвращения возникновения данных петель коммутаторы применяют протокол основного дерева (англ. Spanning Tree Protocol - STP) – сетевой протокол, который работает на втором уровне OSI.

Главное задачей протокола STP является приведение сети Ethernet с множественными связями к древовидной топологии. Это осуществляется с помощью автоматического блокирования избыточных связей. Время сходимости (т.е. переключение на резервный канал) составляет 30-50 секунд. Но это считается довольно большим числом, по этой причине, помимо протокола STP, существуют альтернативные протоколы: RSTP, MSTP (время сходимости которых составляет менее секунды).

Принцип действия протокола состоит из 3 этапов:

1) В сети выбирается один корневой коммутатор (англ. Root Bridge).

Порты корневого коммутатора становятся назначенными и переходят в состояние передачи, т.е. они имеют возможность принимать и передавать пакеты. (рис. 2.4)

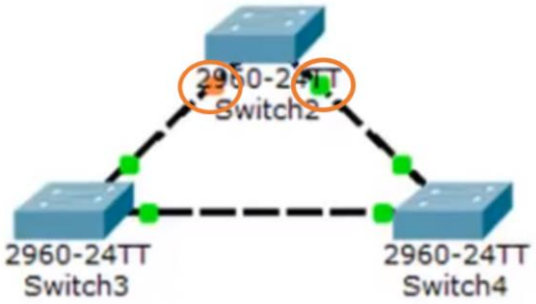

Рисунок 2.4 – Назначенные порты корневого коммутатора

2) После этого, происходит выбор корневого порта на некорневом коммутаторе. В этом случае, корневой порт выбирается в зависимости от стоимости пути от некорневого коммутатора до корневого. Стоимость пути можно рассчитать, используя пропускную способность канала. То есть, чем больше пропускная способность, тем меньше стоимость.

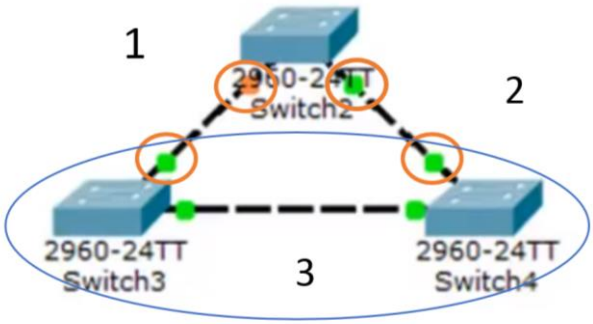

Рисунок 2.5 – Корневые порты некорневых коммутаторов

Например, при пропускной способности каналов под номерами 2 и 3 были 100 Мбит/с, а канала под номером 1 – 10 Мбит/с, то для Switch3 корневым портом являлся бы второй порт, потому, что его пропускная способность больше пропускной способности других портов.

3) Далее, выбирается назначенный порт. В каждом сегменте (т.е. пролет между коммутаторами) протокол STP образует один порт, который предназначен для связи с этим сегментом. Назначенный порт выбирается на Switch-е, имеющем самую малую стоимость пути до корневого коммутатора. Назначенный порт переходит в состояние передачи. В нашем случае – это порт на Switch4 (рис.2.6)

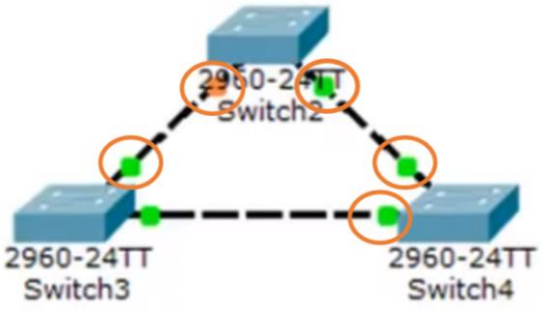

Рисунок 2.6 – Назначенный порт

Выбор корневого коммутатора происходит следующим образом. Протокол STP основывается на числе BID (англ. Bridge ID). Данный параметр представляет собой объединение приоритета коммутатора и его MAC-адреса. Т.к. на всех коммутаторах приоритет одинаковый, то корневым коммутатором автоматически станет коммутатор с наименьшим MAC-адресом. Таким же образом осуществляется выбор назначенного порта, если у двух коммутаторов одинаковые стоимости пути до корневого.

Состояния портов могут быть следующие:
- блокировка (blocking),
- прослушивание (listening),
- обучение (learning)
- передача (forwarding).

1. Blocking - это состояние всех портов по умолчанию, при котором фреймы не пересылаются портами. После включения коммутатора, все порты находятся в данном состоянии.

2. Listening - это состояние, которое идет после состояния blocking. В данном случае порт коммутатора также не передает фреймы, но принимает участие в процессе spanning-tree для решения, есть ли необходимость продолжения для передачи фреймов.

3. Learning - это состояние, следующее за состоянием listening. В этом случае, порт коммутатора не передает фреймы, а готовится к переходу в следующее - состояние forwarding.

4. Forwarding - это состояние после состояния learning. В данном случае, порт коммутатора может передавать фреймы и продолжать принимать участие в процессе spanning-tree. Это состояние необходимо для нормального функционирования устройств.

2.3.3 VLAN на базе меток – стандарт IEEE 802.1Q

В случаях, когда применяется дополнительное поле с информацией о номере виртуальной сети, оно применяется только в случаях, когда кадр пересылается от коммутатора к коммутатору, а при пересылке кадра конечному узлу оно удаляется. Совместно с этим трансформируется протокол взаимодействия "коммутатор-коммутатор", а программное и аппаратное обеспечение конечных узлов не изменяется. Существует большое количество примеров подобных фирменных протоколов, но их общим недостатком является то, что другие производители не поддерживают данные протоколы.

Компания Cisco предложила идею применения заголовка протокола 802.10 как типовое дополнение к кадрам любых протоколов локальных сетей. Данный заголовок протокола используется для поддержания функций безопасности вычислительных сетей. Сама компания Cisco применяет данную технологию в тех случаях, когда коммутаторы связываются друг с другом с помощью протокола FDDI. Но, несмотря на это, данная инициатива не получила поддержку других ведущих производителей коммутаторов.

Новый стандарт IEEE 802.1Q предназначен для установления каких-либо изменений в структуре кадра Ethernet, которые дают возможность пересылать данные о VLAN по сети. Стандарт IEEE 802.1p определяет способ установления приоритета кадра, который работает на основе применения новых

полей, определенных в стандарте IEEE 802.1Q. Кадр Ethernet дополняется двумя байтами.

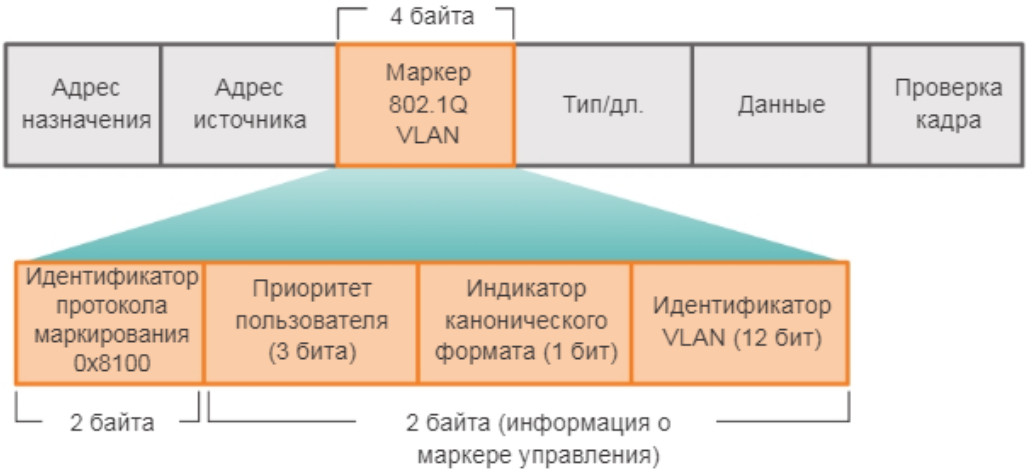

Рисунок 2.7 - Дополнительные 4 байта позволяют использовать технологии QoS и VLAN

Данные 16 бит содержат данные о том, к какой VLAN принадлежит кадр Ethernet и о его приоритете. Говоря конкретнее, три бита позволяют кодировать до восьми уровней приоритета, 12 бит дают возможность различать трафик до 4096 VLAN, а один бит зарезервирован для обозначения кадров сетей других типов (например, TokenRing, FDDI), которые пересылаются по магистрали Ethernet. Следует отметить, что дополнение максимального размера кадра Ethernet двумя байтами приводит к образованию недочетов в работе большого количества коммутаторов, которые предназначены для обработки кадров Ethernet аппаратно. С целью избежания таких проблем, специалисты по стандартизации подали идею уменьшить на два байта максимальный размер полезной нагрузки в кадре. Спецификация IEEE 802.1p, которая образуется в рамках процесса стандартизации 802.1Q, устанавливает способ пересылки данных о приоритете сетевого трафика [4].

Стандарт 802.1p предназначен для спецификации алгоритма изменения порядка позиционирования пакетов в очередях, с использованием которого можно обеспечить доставку чувствительного к временным задержкам трафика в необходимое время. Помимо установления приоритетов, стандарт 802.1p также предназначен для ввода значимого протокола GARP (англ. Generic Attributes Registration Protocol) с двумя специальными его реализациями. Первой специализацией является протокол GMRP (англ. GARP Multicast Registration Protocol), которые дает возможность рабочим станциям осуществлять запрос на присоединение к домену групповой рассылки сообщений. Концепция, которая поддерживает данный протокол имеет название подсоединения, которое инициируется "листьями". Протокол GMRP дает возможность пересылать трафик только в те порты, из которых поступил запрос на групповой трафик. Вторая реализация GARP имеет название -

протокол GVRP (англ. GARP VLAN Registration Protocol), который схож с протоколом GMRP. Но, несмотря на это, при работе по данному протоколу, рабочая станция вместо запроса на присоединение к домену групповой рассылки сообщений отправляет запрос на доступ к одной из имеющихся VLAN [1].

С целью согласования работы устройств, которые поддерживают формат кадра 802.1 Q, с теми устройствами, которые не поддерживают данный формат, создатели стандарта порекомендовали разделить весь трафик в сети на следующие типы:

– трафик входного порта;
– внутренний трафик;
– трафик выходного порта.

Трафик входного порта (англ. Ingress Port). Каждый кадр, который поступает в коммутируемую сеть и направляется от маршрутизатора или от рабочей станции, имеет определенный порт-источник. С помощью его номера коммутатор должен решить принять (или отбросить) данный кадра и передавать ли его в определенную VLAN. Данное решение, которое принимается в определенной логической точке сети, обеспечивает сосуществование совершенно разных видов VLAN. Получив кадр, коммутатор добавляет ему "ярлык" (англ. tag) VLAN. После того, как кадр с добавленным "ярлыком" VLAN попадает в сеть, он становится частью проходящего (англ. Progress), или внутреннего трафика.

Внутренний трафик (англ. ProgressTraffic). Кадр с добавленным "ярлыком" коммутируется тем же способом, что и кадр без "ярлыка". Решения о том, к какой VLAN принадлежит данный кадр принимаются в пограничных элементах сети и остальные сетевые устройства относятся “нейтрально” к тому, каким способом данный кадр оказался в сети. В результате того, что максимальный размер кадра Ethernet не изменился, пакеты всех VLAN способны быть обработаны традиционными коммутаторами и маршрутизаторами внутренней части сети.

Трафик выходного порта (англ. EgressPort). При необходимости оказаться в межсетевом маршрутизаторе или в оконечной рабочей станции, кадру необходимо попасть за границы коммутируемой сети. Выходное устройство сети принимает решение о том, какому порту (или портам) необходимо переслать пакет и нужно ли удалять из него служебные данные, которые предусмотрены стандартом 802.1Q. Суть заключается в том, что типовые рабочие станции не всегда “признают” данные о VLAN по стандарту 802.1Q, но серверу, который обслуживает некоторое количество подсетей используя единственный интерфейс, необходимо использовать эти данные [6].

Условное деление трафика на внутренний, а также входного и выходного портов дает возможность поставщикам нестандартных реализаций VLAN образовывать шлюзы для их стыковки с VLAN, которые соответствуют стандарту 802.1Q.

2.3.4 Использование сетевого протокола

При применении данного метода коммутаторам для создания виртуальной сети необходимо поддерживать какой-либо сетевой протокол. Подобные коммутаторы имеют название коммутаторов 3-го уровня, по причине того, что данные коммутаторы содержат в себе как функции коммутации, так и маршрутизации.

Объединение коммутации и маршрутизации является удобным для создания виртуальных сетей в результате того, что в данном случае нет необходимости в введении дополнительных полей в кадры, плюс к этому администратору нет необходимости повторять одну и ту же операция на канальном и сетевом уровнях, так как он может установить сети только один раз. К какой виртуальной сети принадлежит определенный конечный узел, определяется стандартным методом установления сетевого адреса.

Но, несмотря на это, применение сетевого протокола для создания виртуальных сетей не позволяет применять его обычными коммутаторами, за исключением коммутаторов 3-го уровня. Это является значительным минусом.
Поэтому, самым удобным и гибким способом считается создание виртуальных локальных сетей с использованием стандартов 802.1 Q/p с последующим их отображением на "традиционные сети" в коммутаторах 3-го уровня или маршрутизаторах.

3 Моделирование виртуальных локальных сетей для предприятия

3.1 Пример разделения локальной сети предприятия с использованием программы Cisco Packet Tracer

В сетях, которые основаны на широковещательном трафике, с увеличением числа пиров растет и число широковещательного трафика (который потенциально имеет возможность почти полностью вытеснить собой полезную нагрузку на сеть).

VLAN-ы же дают возможность уменьшить сетевой трафик с помощью создания нескольких широковещательных доменов, разделяя крупную сеть на несколько меньших независимых сегментов с небольшим числом широковещательных запросов, передаваемых каждому устройству всей сети в целом.

Данные преимущества являются причиной широкого применения виртуальных локальных сетей предприятиями и организациями. Пример разделения офиса на несколько независимых виртуальных сетей с применением одного коммутатора можно рассмотреть, используя программу моделирования сетей – Cisco Packet Tracer (CPT).

В качестве примера я использовала компанию “Adil Group”, в которой имеется несколько отделов: отдел кадров, производственный, высшее руководство, технический отдел. Каждый отдел имеет серверы, доступ к которым нужно ограничить сотрудникам из других отделов.

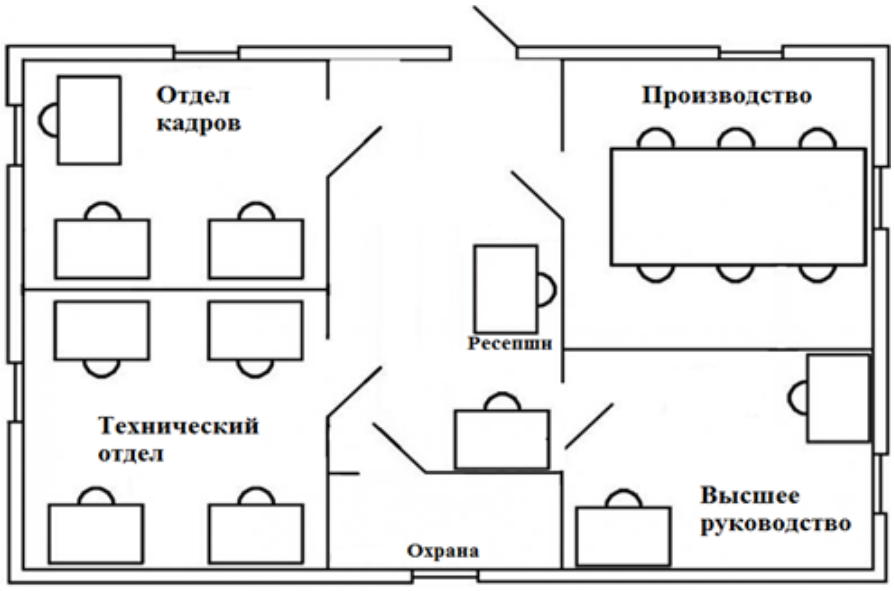

Рисунок 3.1 - Схема расположения отделов компании “AdilGroup”

На первый взгляд, теоретически осуществить это не так уж сложно. Так как можно разработать сетевую инфраструктуру каждой сети по отдельности. С другой точки зрения загвоздка заключается в том, что подобную сеть нелегко

разработать. Помимо этого, может возникнуть потребность в изменении самой конфигурации сети.

По этой причине, намного легче разработать общую физическую сеть с дальнейшим логическим разделением определенных частей сети. Этот метод дает возможность произвести более гибкое планирование и управление сетью, к тому же позволяет повысить безопасность сети.

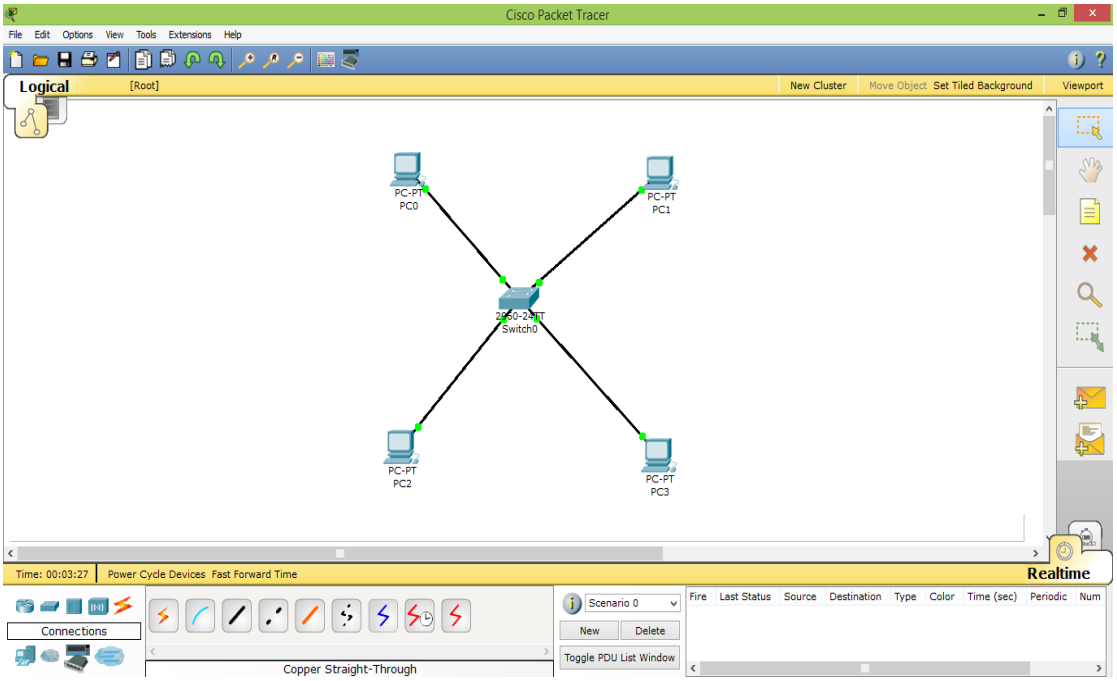

Рисунок 3.2

На рисунке 3.2 можно увидеть схему, состоящую из 4 ПК и одного коммутатора, которые соединены прямым кабелем. ПК0 принадлежат сегменту отдела кадров, ПК1 сегменту высшего руководства, ПК3 сегменту технического отдела и ПК4 сегменту производства. Нам необходимо объединить компьютеры отдела кадров и высшего руководства в одну виртуальную сеть, а компьютеры отдела кадров и сегмента производства в другую (рис.3.3).

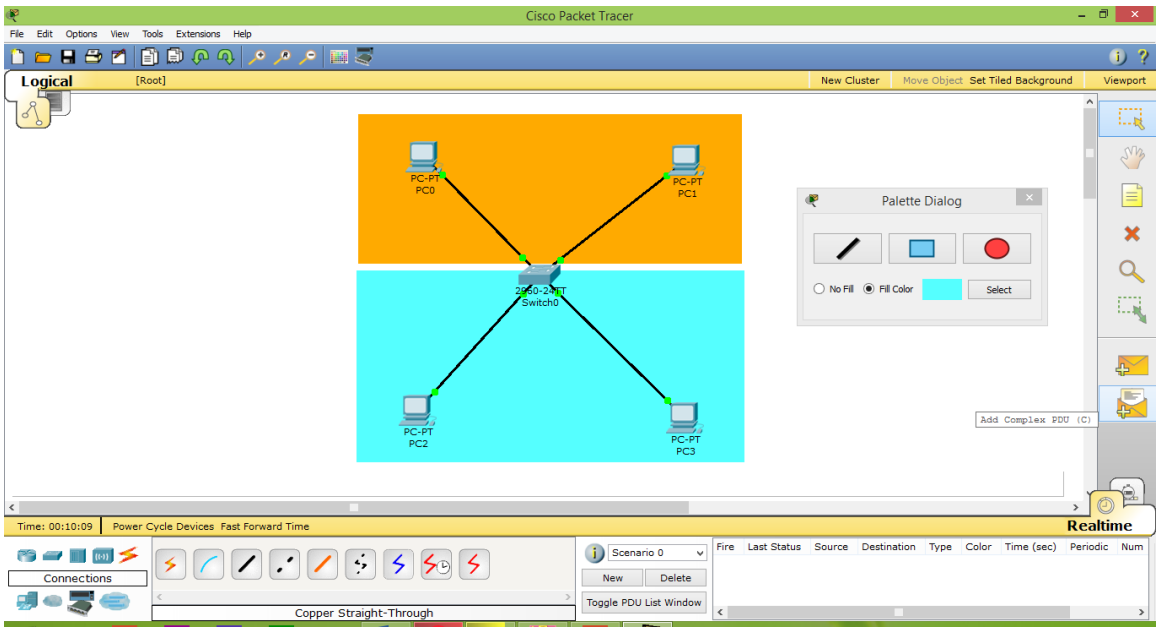

Рисунок 3.3 – Сегментирование на VLAN-ы с помощью одного коммутатора

Для того, чтобы разделить трафики разных сегментов необходимо зайти в консоль (CLI), который находится в настройках коммутатора и определяем VLAN, в котором будут находиться данные пользователи. В изначальной схеме все порты коммутатора находятся в Vlan1. Нам необходимо создать VLAN2 и определить порты в соответствующие сети.

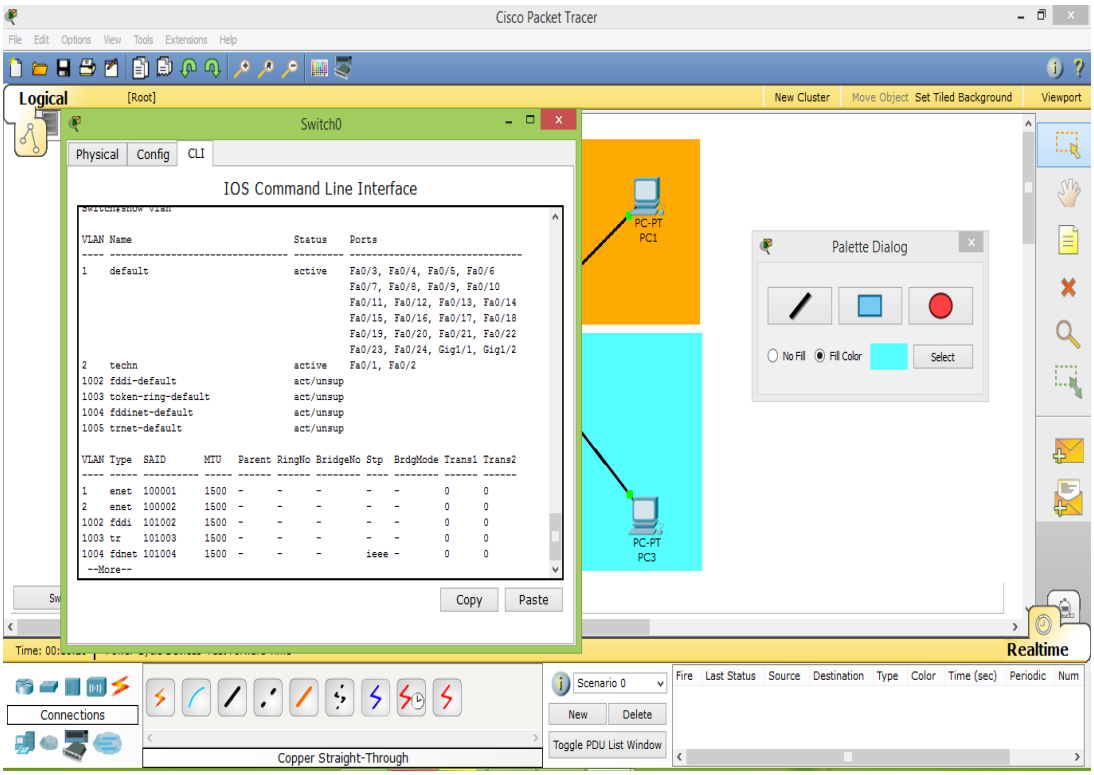

Рисунок 3.4 – Настройка коммутатора для разделения трафика разных сегментов

Проверку проделанной работы можно увидеть на рисунке 3.4, на котором показано, что первый дефолтный (default) vlan, который существует на всех коммутаторах, выставлен на всех портах, кроме fastEthernet 0/1 и 0/2, которые мы только что определили в vlan2.

Далее, мы производим настройку ПК и присваиваем каждому компьютеру соответствующий IP-адрес. В результате чего, мы видим, что компьютеры одного сегмента “видят” друг друга, но не могут обнаружить компьютеры другого сегмента (рис.3.5).

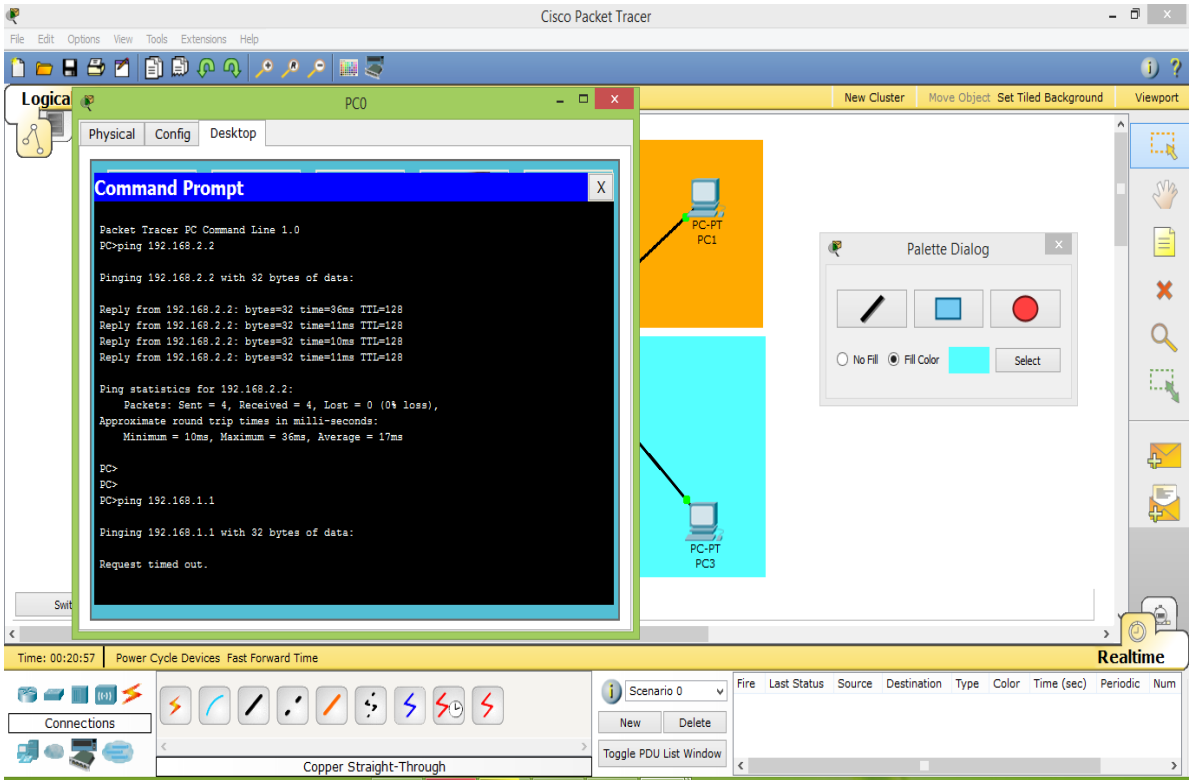

Рисунок - 3.5 – Проверка работы VLAN при работе с одним коммутатором

Также, следует рассмотреть способ сегментирования данной сети с использованием нескольких коммутаторов, в нашем случае двух. Для этого необходимо создать копию существующей схемы, соединить коммутаторы одного уровня модели OSI кросс-кабелем и включить их портом Gigabit Ethernet 0/1 – самым производительным портом (рис.3.6).

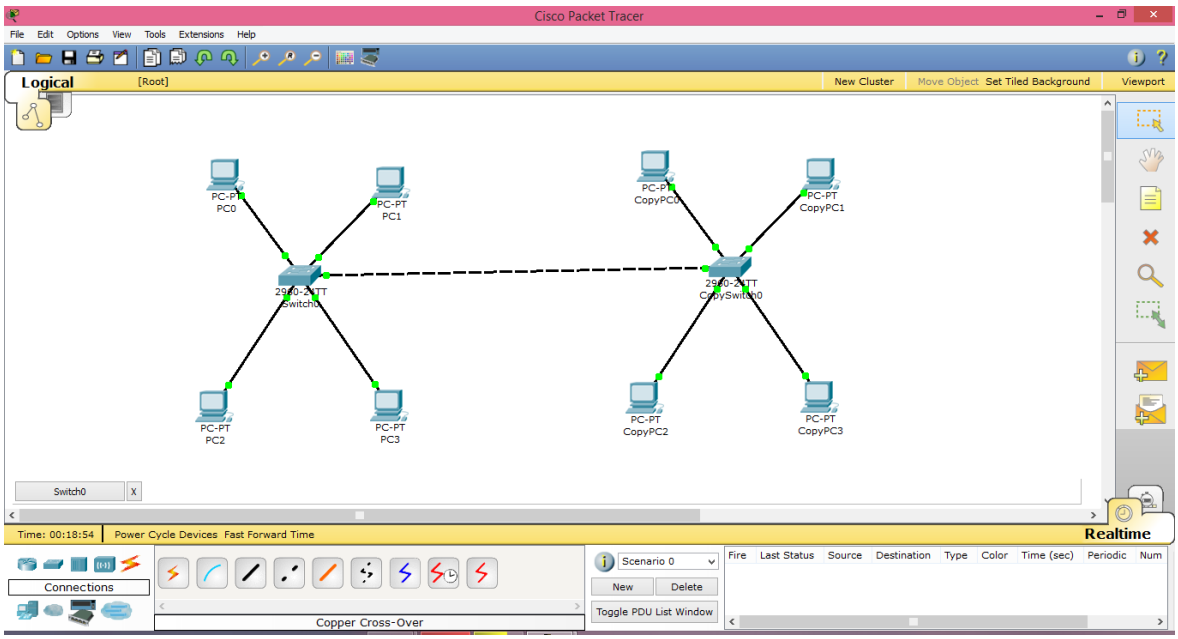

Рисунок 3.6

После изменения IP-адресов новых компьютеров, мы объединяем и в сегменты. Коммутаторы не требуют дополнительной настройки, так как все настройки уже скопированы (рисунок 3.7)

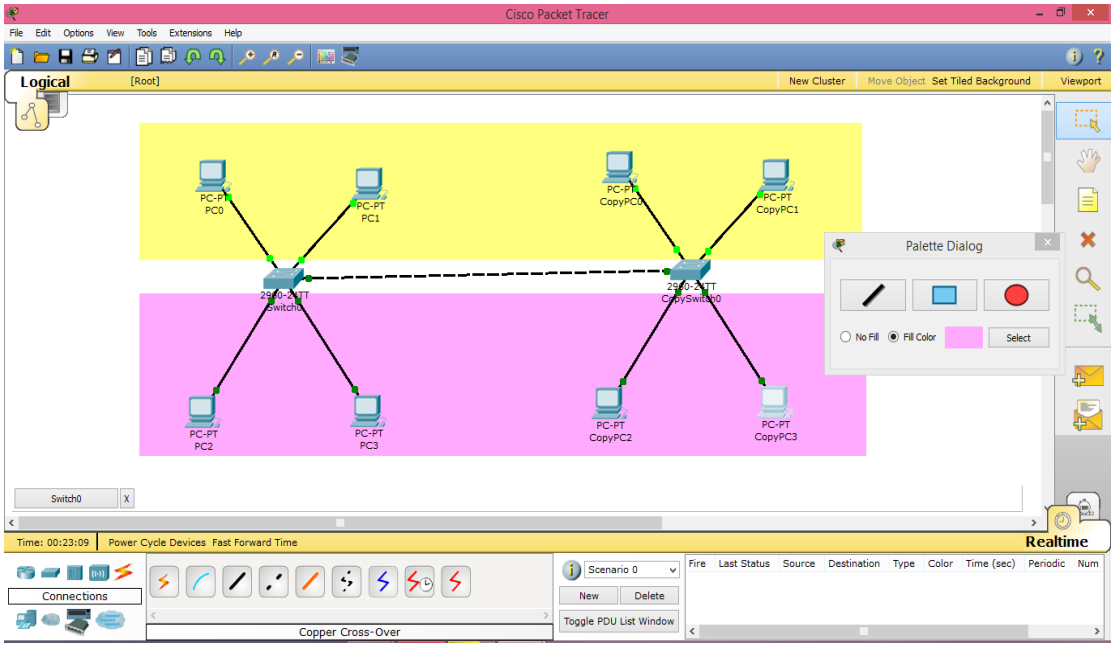

Рисунок 3.7 –Сегментирование на VLAN-ы с помощью двух коммутаторов

Далее, необходимо создать Trunkport. Физический кабель можно представить в виде трубы, а внутри нее можно прокладывать дополнительные трубочки для передачи трафика. Это и есть vlan-ы. т.е. trunkport позволяет логически разбить физическое соединение на несколько сегментов. Для этого

необходимо произвести настройку коммутаторов, в которой мы определяем сети, которые будем передавать через физическое соединение.

Для проверки проделанной работы используем команду ping. На рисунке 3.8 можно увидеть, что компьютеры одного сегмента могут обнаружить друг друга, при этом они не «видят» компьютеры другого сегмента.

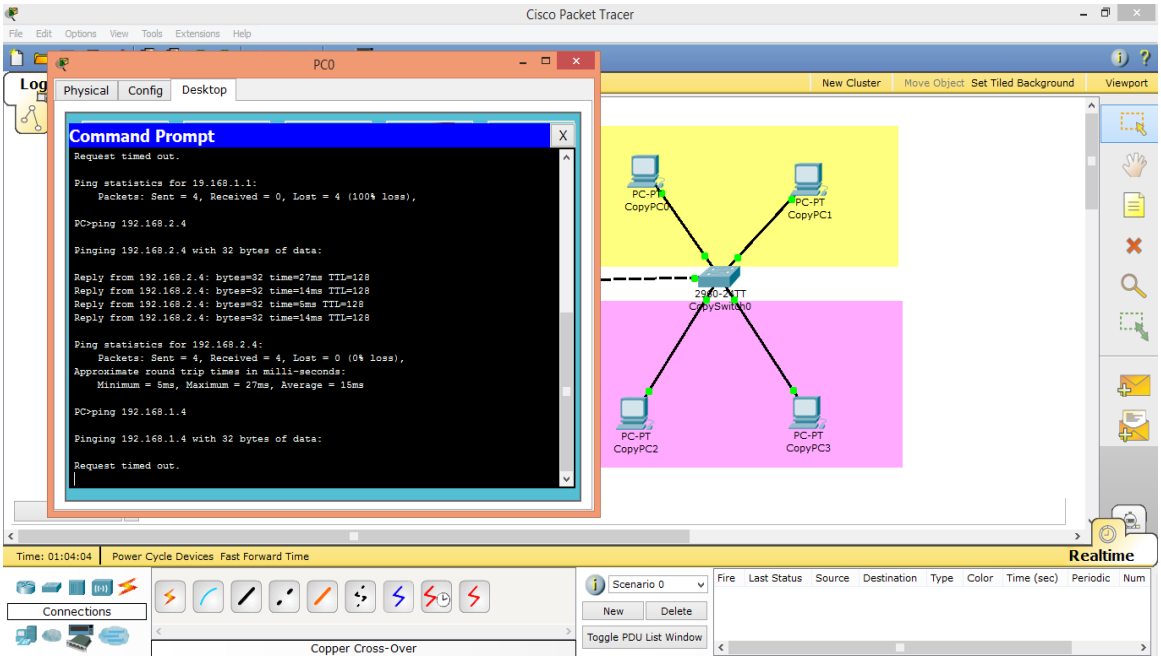

Рисунок 3.8 – Проверка работы VLAN-ов при использовании двух коммутаторов

При создании большой сети, ее необходимо разделить на части, подключить каждую часть к определенному коммутатору, а коммутаторы, в свою очередь, соединять друг с другом с помощью высокоскоростных линий связи.

В больших сетях для соединения коммутаторов применяются многоуровневые структуры с древовидной топологией связей: на нижнем уровне располагаются дешевые коммутаторы с низкой пропускной способностью, к которым подсоединяются ПК-ы, а для объединения данных коммутаторов в единую сеть применяются мощные дорогие устройства, которые имеют высокую пропускную способность и могут работать на третьем уровне модели OSI (т.е. коммутаторы 3-его уровня).

Коммутаторы 3-го уровня модели OSI (L3) позволяют осуществить следующие функции:

- IP маршрутизация, т.е. они не только разделяют сеть на отдельные VLAN-ы, но и маршрутизируют трафик между данными сегментами,
- агрегирование коммутаторов уровня доступа,
- применяются в качестве коммутаторов уровня распределения. При отсутствии коммутатора L3, нужно было бы осуществить немалое количество соединений между коммутаторами L2 [4].

Рассмотрим пример построения сети компании «Adil Group» с использованием коммутатора 3-го уровня.

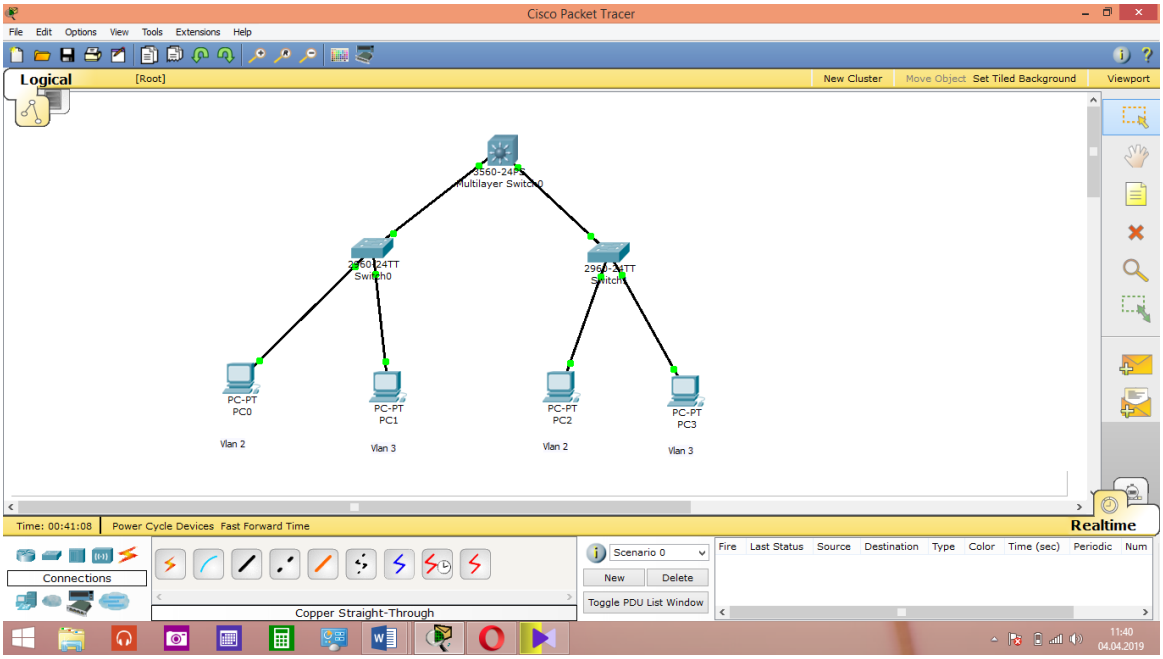

Рисунок 3.9

На рисунке 3.9 мы видим три уровня. Коммутатор Switch0 находится на 1 этаже офиса, а Switch1 – на 2 этаже. Коммутатор 3-его уровня расположен в серверной. Нам необходимо объединить компьютеры отдела кадров и высшего руководства в одну виртуальную сеть (т.е. ПК0 и ПК2), а компьютеры отдела кадров и сегмента производства в другую (т.е. ПК1 и ПК3).

В первую очередь, необходимо настроить коммутаторы уровня доступа. Для этого, мы настраиваем access-порты и trunk -порты для коммутаторов Switch 0 и Switch1 до центрального коммутатора (рис.3.10).

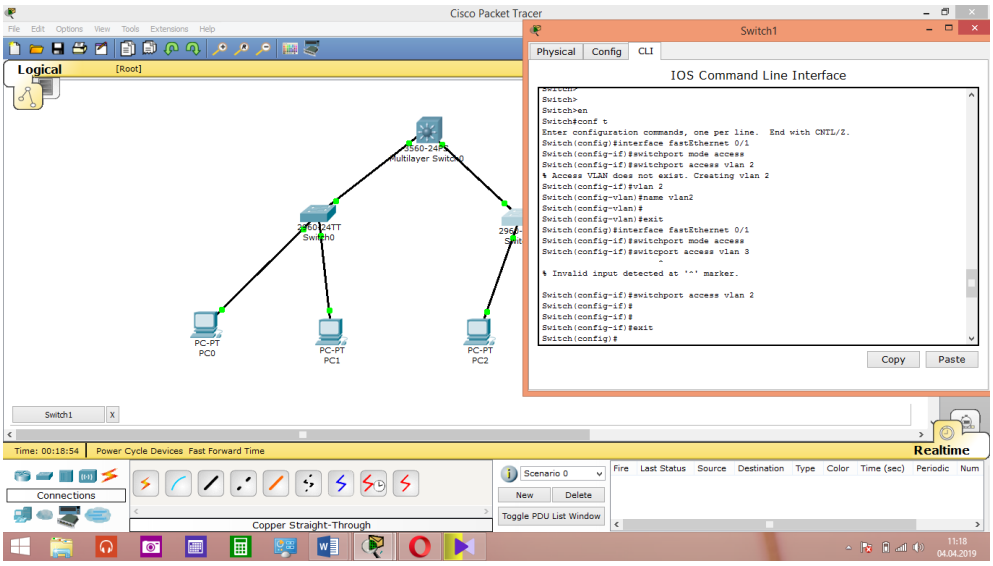

Рисунок 3.10

Далее необходимо произвести настройку коммутатора третьего уровня (L3). Так как L3 коммутатор соединяет коммутаторы Switch 0 и Switch1, мы настраиваем данные порты в транке. После чего, устанавливаем IP-адреса на созданные виртуальные интерфейсы (рис.3.11).

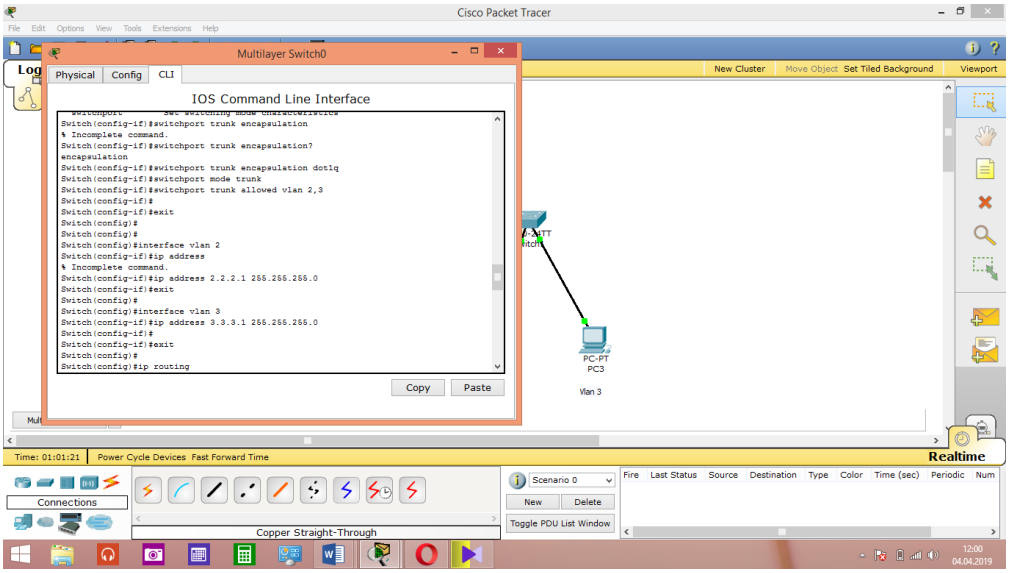

Рисунок 3.11 - Настройка портов в транке

После настройки самих компьютеров, проверить работу системы и взаимодействие между компьютерами, которые находятся в одной vlan, но подсоединенные к разным L2 коммутаторам, можно «пингованием». На рисунке 3.12 можно увидеть, что компьютеры одной сети могут обнаружить друг друга, несмотря на подключение к разным коммутаторам.

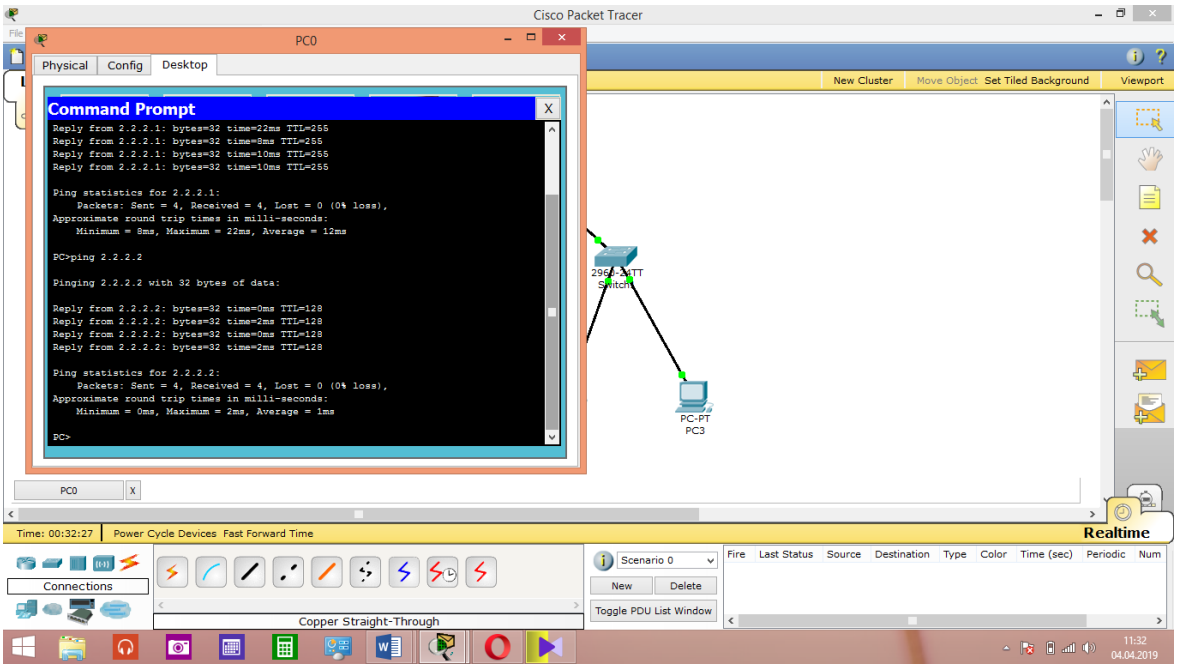

Рисунок 3.12 – Компьютеры одной сети могут обнаружить друг друга, несмотря на подключение к разным коммутаторам

В результате, мы настроили два сегмента, которые через транк-порт идут на центральный коммутатор L3, на котором прописан IP- адрес на каждый из vlan-ов.

Таким образом, используя программу моделирования сетей – Cisco Packet Tracer (CPT), я разделила большую сеть компании “Adil Group” на две меньших независимых сегментов тремя разными способами. В результате чего кадр, поступивший от порта, который относится, например, к vlan1, никогда не будет переслан порту, не принадлежащему этой виртуальной сети. Такое сегментирование сети позволяет повысить производительность каждой виртуальной сети, благодаря тому, что коммутатор пересылает кадры в подобной сети только узлу назначения; а также осуществить изолирование сетей друг от друга с целью управления правами доступа пользователей и образования защитных барьеров на пути широковещательных штормов и т.д.

3.2 Способ оптимизации прохождения трафика при заданной топологии сети на уровне доступа

На данный момент актуальной проблемой является планирование сети доступа в интернет предприятий малого и среднего масштаба. При планировании сети основной целью является обеспечение бесперебойного доступа к Интернет ресурсам на высоких скоростях при небольшой стоимости строительства и эксплуатации оборудования ЛВС. В своем исследовании я рассмотрела способ оптимизации прохождения трафика при заданной топологии сети на уровне доступа.

На рисунке 3.6 можно увидеть топологию сети компании “Adil Group”.

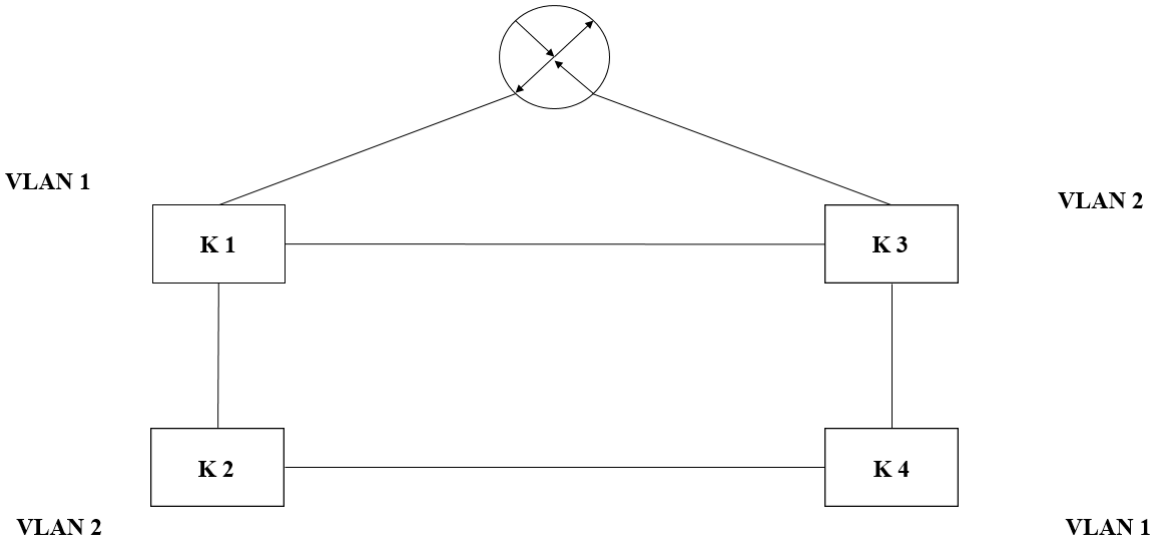

Рисунок 3.6 - Топология сети компании “Adil Group”

В этой топологии имеется 4 коммутатора, которые подключены по простой схеме организации связи в кольцо, и после этого в маршрутизатор. Пользователи, которые подключены в каждый из коммутаторов функционируют в своей, заранее сконфигурированной Vlan. Следовательно, пользователи коммутатора 1 и коммутатора 4 работают в Vlan 1, пользователи коммутатора 2 и коммутатора 3 в Vlan 2.

Как уже было сказано ранее, в рассматриваемом предприятии имеется 4 отдела, которые в разной степени пользуются информационными технологиями, кто-то больше, а кто-то меньше. Из-за чего необходимо грамотно прогнозировать, планировать и распределять трафик в такой сети. Коммутатор 1 открывает выход в интернет сотрудникам отдела кадров. Коммутатор 2 для высшего руководства. Коммутатор 3 для сотрудников технического отдела. Коммутатор 4 используется сотрудниками производства. В таблице 1 можно увидеть планируемую нагрузку, которая создается каждой группой работников.

Таблица 1 - Нагрузка, создаваемая работниками

Подразделения предприятия	Интенсивность создаваемой нагрузки λ, (Мбит/с)
Отдел кадров	150
Технический отдел	650
Отдел производства	150
Высшее руководство	30

Из таблицы 1 можно заметить, что наибольшую долю нагрузки составляют каналы для технического отдела и отдела производства. Причиной высоких цифр является использование в компании высокоскоростных почтовых и WEB-серверов.

Для того, чтобы избежать петель в данной топологии удобно использовать протокол STP (стандарт IEEE 802.1d). При использовании этого протокола алгоритм STP в автоматическом режиме построит новую топологию, выберет корневой коммутатор (устройство, которое является для STP точкой отсчета, центром сети, все дерево STP сходится к нему). Но это может привести к тому, что алгоритм в автоматическом режиме выберет корневым первый коммутатор в цепи, и разорвёт топологию так, что более 80% трафика будет передаваться только по одной стороне кольца. Для оптимального распределения нагрузки в каналах целесообразно осуществить ручную конфигурацию протокола MSTP (стандарт IEEE 802.1s). Этот стандарт дает возможность осуществить балансировку нагрузки с помощью распределения трафика для разных Vlan на одних и тех же каналах. Для того, чтобы

рассмотреть преимущества этого способа, необходимо произвести расчёт необходимой пропускной способности каналов для обоих вариантов.

Чтобы рассчитать пропускную способность нужно составить математическую модель сети, которая является совокупностью систем массового обслуживания (СМО) M/M/1. Каждый канал является совокупностью двух систем M/M/1, в которой каждая система представляет выходной интерфейс коммутатора или маршрутизатора. В результате того, что пропускная способность рассчитывается в двух направлениях для каждой линии, за конечную пропускную способность принимается наибольшая. Для системы M/M/1 интенсивность обслуживания определяется с помощью формулы среднего времени задержки.

$$t = \frac{1/\mu}{1 - 1/\mu}, \quad (1)$$

где t – среднее время задержки;

λ – интенсивность поступающей нагрузки;

μ – интенсивность обслуживания, которая в нашем случае является пропускной способностью.

После преобразования формулу (1) мы получаем конечную формулу для расчёта пропускной способности:

$$\mu = \frac{1}{t} + \lambda \quad (2)$$

Далее необходимо определить среднее время задержки в СМО. Допустим, что время сквозной задержки не должно превышать 1000 мс. С условием, что 0,9 мс секунды затрачивается на создание датаграммы, 10 мс на задержку пакетизации и 1,8 на задержку в джиттер-буфере, время, которое остается на сквозную задержку равно 987,3 мс. При применении протокола STP максимальное число СМО на пути передвижения пакета равно 3, из чего следует, что задержка на одну СМО равна 329,1 мс. В другом случае, при применении протокола MSTP максимальное число СМО на пути прохождения пакета равно 5, из чего следует, задержка на одну СМО равна 197,46 мс.

Для выполнения расчёта топология сети представлена в виде графа, рисунок 3.7.

В данной топологии номера каналов между устройствами изображены римскими цифрами. При ручной настройке протокола MSTP, представляется большое число вариантов прохождения трафика для разных Vlan. Штрих пунктирными линиями обозначены направления прохождения трафика для разных Vlan.

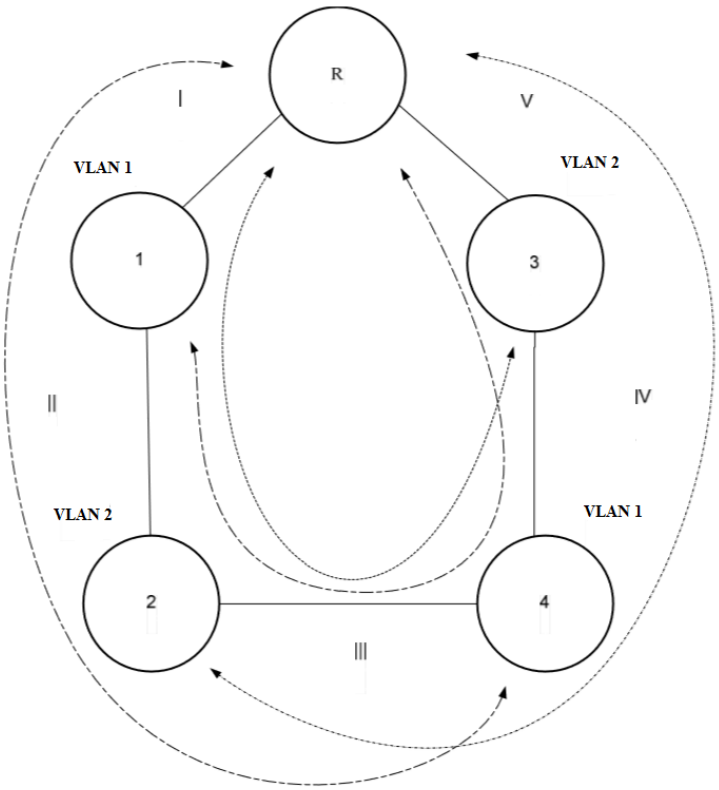

Рисунок 3.7 – Граф топологии сети

Результаты вычисления пропускных способностей для разных направлений представлены в таблице 2.

Таблица 2 – Пропускные способности каналов

Номер канала	Требуемая пропускная способность для протокола STP, (Мбит/с)	Требуемая пропускная способность для протокола MSTP					
		Vlan 1, (Мбит/с)	Vlan 2, (Мбит/с)	Резерв Vlan 1, (Мбит/с)	Резерв Vlan 2, (Мбит/с)	Общее значение Vlan, (Мбит/с)	Общее значение резерв Vlan, (Мбит/с)
I	850,012154	180,02	0	0	670,02025	180,01	670,0202
II	820,009115	150,01	0	30,00506	670,01519	150,01	700,0202
III	170,006077	150,01	650,01	30,01012	20,010128	800,01	50,02025
IV	150,003038	0	650,01	180,0151	20,005064	650,01	200,0202
V	0	0	670,01	180,0202	0	670,01	180,0202

В таблице можно рассмотреть результаты расчётов для протокола STP и каждой Vlan при применении MSTP. Из таблицы 2 можно увидеть, что при использовании STP, максимальное значение требуемой ширины канала достигает 850,012 Мбит/с. При использовании же протокола MSTP, максимальное значение требуемой ширины канала равно 700,02 Мбит/с. Следовательно, для оптимальной балансировки нагрузки в этой ситуации выгоднее производить ручную конфигурацию протокола MSTP.

ЗАКЛЮЧЕНИЕ

Подводя итоги выполненной дипломной работы, в качестве главных результатов следует выделить следующие.

В этой работе были рассмотрены предпосылки внедрения технологии виртуальных локальных сетей, протоколы и методы реализации виртуальных локальных сетей. Технология виртуальных локальных сетей является очень востребованной, благодаря ряду преимуществ:

1) VLAN помогает структурировать сеть;

2) VLAN используется для обеспечения безопасности;

3) VLAN используется для объединения пользователей на канальном уровне;

4) VLAN уменьшает количество широковещательного трафика.

С помощью программы Cisco Packet Tracer был показан процесс создания виртуальной локальной сети на примере предприятия. В результате использования этой технологии загруженность сетевого оборудования значительно уменьшилась, а также образовались перспективы масштабирования пользовательских сервисов.

Суммируя вышесказанное, можно отметить, что все поставленные задачи, а также основная цель дипломной работы - провести анализ работы виртуальных локальных сетей, выполнены. Оптимизация работы сети проведена успешно, был получены значительные возможности для внедрения и развития современных сервисов на сети.

Перечень принятых сокращений, терминов

VLAN – Virtual Local Area Network (виртуальная локальная сеть);
LAN (Local Area Network) – локальная вычислительная сеть;
MAC (Media Access Control) — управление доступом к среде;
ПК – персональный компьютер;
SW (switch) – коммутатор;
IP - протокол межсетевого взаимодействия;
CSMA/CD (Carrier Sense Multiple Access With Collision Detection) - множественный доступ с контролем несущей и обнаружением коллизий;
VTP (VLAN Trunking Protocol) - протокол виртуальных сетей;
STP (Spanning Tree Protocol) - канальный протокол;
MSTP (Multiple Spanning Tree Protocol) - расширение протокола STP;
RIF (Routing Information Field) – поле маршрутной информации;
BPDU (Bridge Protocol DataUnit) - фрейм (единица данных) протокола управления сетевыми мостами;
FDDI (Fiber Distributed Data Interface) -волоконно-оптический распределенный интерфейс передачи данных;
GMRP (Multicast Registration Protocol) - для регистрации членства в широковещательных посылках;
GARP (Generic Attribute Registration Protocol) - базовый протокол регистрации атрибутов;
GVRP (GARP VLAN Registration Protocol) – сетевой протокол канального уровня модели OSI/ISO;
CPT(Cisco Packet Tracer) - программа моделирования сетей;
CLI (Command Line Interface)- интерфейс командной строки;
OSI (Open Systems Interconnection Basic Reference Model) — базовая эталонная модель взаимодействия открытых систем;
СМО – система массового обслуживания;

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Олифер В.Г., Олифер Н.А. "Базовые технологии локальных сетей." [Электронный ресурс] СПб.: Питер, 2006г - Режим доступа: http://citforum.ru/nets/protocols2/index.shtml

2. Гергель А.В. Компьютерные сети и сетевые технологии.Нижний Новгород, 2007, 107 с.

3. Амато Вито. Основы организации сетей Cisco, том 1. М.: Издательский дом "Вильяме", 2004. – 512с.

4. Максим Кульгин «Технологии корпоративных сетей. Энциклопедия» - СПб: Питер, 2000 г.

5. Учебное пособие: Коммутаторы локальных сетей D-Link.

6. Джесси Рассел. «Виртуальные локальные сети» - М.: ЭКСМО, 2011г. – 672с.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
СӘТБАЕВ УНИВЕРСИТЕТІ

РЕЦЕНЗИЯ

на дипломную работу

Махамбетовой Ботагоз Сериковны

5В071900 – Радиотехника, электроника и телекоммуникации

На тему: Анализ виртуальных локальных сетей

Выполнено:
а) графическая часть на 17 листах
б) пояснительная записка на 47 страницах

ЗАМЕЧАНИЯ К РАБОТЕ

В современное время в число важнейших стратегических направлений почти всех крупнейших производителей сетевого оборудования входят виртуальные сети - VLAN. VLAN представляет собой логическое комбинирование некоторого числа конечных станций в одном сегменте на канальном уровне. Изолирование трафика группы узлов от остальной сети является актуальной проблемой.

Дипломная работа Махамбетовой Б. посвящена анализу виртуальных локальных сетей. В первой главе рассматриваются общие вопросы, связанные с принципами построения современных локальных сетей, с основными понятиями о виртуальных локальных сетях, преимуществами и недостатками использования технологии VLAN для эффективной организации работы предприятий.

Во второй главе дается анализ виртуальных локальных сетей, функции и назначение VLAN, способы построения сетей, а также протоколы, используемые в виртуальных локальных сетях: VTP, STP и IEEE 802.1Q.

Третья глава посвящена моделированию организации виртуальных локальных сетей на примере разделения локальной сети предприятия с помощью программы Cisco Packet Tracer.

Оценка работы

Считаю, что дипломная работа выполнена на 95/А/«отлично», а дипломант, Махамбетова Ботагоз Сериковна, заслуживает присвоения академической степени бакалавра техники и технологии по специальности 5В071900-Радиотехника, электроника и телекоммуникации.

Рецензент
канд.техн. наук, профессор АУЭС
_____ А.С. Байкенов
“ _____ 2019г.

Ф КазНИТУ 706-17. Рецензия

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
СӘТБАЕВ УНИВЕРСИТЕТІ

ОТЗЫВ

НАУЧНОГО РУКОВОДИТЕЛЯ

на дипломную работу

Махамбетовой Ботагоз Сериковны

5В071900 – Радиотехника, электроника и телекоммуникации

Тема: Анализ виртуальных локальных сетей

В данной дипломной работе рассматриваются вопросы сегментирования локальной сети, которые всегда будут актуальными в связи с тем, что данная технология позволяет уменьшить сетевой трафик.

Первая глава посвящена общим вопросам, связанным с появлением локальных вычислительных сетей, принципам их построения, методам коммутации, а также преимуществам и недостаткам использования технологии VLAN для эффективной организации работы предприятий.

Вторая глава непосредственно дает анализ виртуальным локальным сетям, методам их построения и протоколам.

В третьей главе в программе Cisco Packet Tracer показана модель разделения локальной сети предприятия, где в качестве примера рассматриваются три распространенных метода построения сети, а также показан способ оптимизации прохождения трафика.

Считаю, что дипломная работа выполнена на 95/А/«отлично», а дипломант, Махамбетова Ботагоз Сериковна, заслуживает присвоения академической степени бакалавра техники и технологии по специальности 5В071900-Радиотехника, электроника и телекоммуникации.

Научный руководитель
маг-р техн. наук, лектор
_____Г.М. Байкенова
"13" 05 _____2019г.

Ф КазНИТУ 706-16. Отзыв научного руководителя

Протокол анализа Отчета подобия

заведующего кафедрой / начальника структурного подразделения

Заведующий кафедрой / начальник структурного подразделения заявляет, что ознакомился(-ась) с Полным отчетом подобия, который был сгенерирован Системой выявления и предотвращения плагиата в отношении работы:

Автор: Махамбетова Ботагоз Серіковна

Название: Анализ виртуальных локальных сетей

Координатор: Гулжан Байкенова

Коэффициент подобия 1:21,7

Коэффициент подобия 2:0,6

Тревога:0

После анализа отчета подобия заведующий кафедрой / начальник структурного подразделения констатирует следующее:

☐ обнаруженные в работе заимствования являются добросовестными и не обладают признаками плагиата. В связи с чем, работа признается самостоятельной и допускается к защите;
☐ обнаруженные в работе заимствования не обладают признаками плагиата, но их чрезмерное количество вызывает сомнения в отношении ценности работы по существу и отсутствием самостоятельности ее автора. В связи с чем, работа должна быть вновь отредактирована с целью ограничения заимствований;
☐ обнаруженные в работе заимствования являются недобросовестными и обладают признаками плагиата, или в ней содержатся преднамеренные искажения текста, указывающие на попытки сокрытия недобросовестных заимствований. В связи с чем, работа не допускается к защите.

Обоснование:

.....
.....
.....
.....
.....

03.05.2019 .....

Дата

Подпись заведующего кафедрой /

начальника структурного подразделения

Протокол анализа Отчета подобия Научным руководителем

Заявляю, что я ознакомился(-ась) с Полным отчетом подобия, который был сгенерирован Системой выявления и предотвращения плагиата в отношении работы:

Автор: Маканбетова Багагоз Сериковна

Название: Анализ виртуальных локальных сетей

Координатор: Гулжан Байкенова

Коэффициент подобия 1: 21,7

Коэффициент подобия 2: 0,6

Тревога: 0

После анализа Отчета подобия констатирую следующее:

☑ обнаруженные в работе заимствования являются добросовестными и не обладают признаками плагиата. В связи с чем, признаю работу самостоятельной и допускаю ее к защите;

☐ обнаруженные в работе заимствования не обладают признаками плагиата, но их чрезмерное количество вызывает сомнения в отношении ценности работы по существу и отсутствием самостоятельности ее автора. В связи с чем, работа должна быть вновь отредактирована с целью ограничения заимствований;

☐ обнаруженные в работе заимствования являются недобросовестными и обладают признаками плагиата, или в ней содержатся преднамеренные искажения текста, указывающие на попытки сокрытия недобросовестных заимствований. В связи с чем, не допускаю работу к защите.