АННОТАЦИЯ

В данной работе описывается процесс управление доступом с применением технологии VLAN на базе стандарта IEEE 802.1Q для Тверского колледжа им. А. Н. Коняева. Для разработки управление доступа в колледже было сделано исследование самый оптимальных методов управление несанкционированный доступ (НСД) и пришли к выводу что VLAN является самый лучше вариант из-за следующий достоинств:

- повышение безопасности каждой виртуальной сети. Работники одного отдела офиса не смогут отслеживать трафик отделов, не входящих в их VLAN, и не получат доступ к их ресурсам;
- сокращение числа широковещательных запросов, которые снижают пропускную способность сети;
- создать новую виртуальную сеть можно без прокладки кабеля и покупки коммутатора;
- позволяет объединить в одну сеть компьютеры, подключенные к разным коммутаторам;
- возможность разделять или объединять отделы или пользователей, территориально удаленных друг от друга. Это позволяет привлекать к рабочему процессу специалистов, не находящихся в здании офиса.
- VLAN более быстрее и гибкий метод защита доступа, потому что оно работает на операционной системе, а не на программной системе

ОГЛАВЛЕНИЕ

Введение

Актуальность темы исследования. Целью, данной диссертация является управление доступа с применением технологии VLAN на базе стандарта IEEE 802.1Q. Система управления предприятием, компанией, как правило, имеет сложную структуру, в которую входят отдельные, но взаимосвязанные между собой, подсистемы. Подсистемы управления функциональными подразделениями должны обеспечивать эффективное управление этими подразделениями, но, обязательно с учетом достижения оптимального значения показателя эффективности (целевой функции) всего предприятия. Это обстоятельство приводит к необходимости создания информационной системы всего предприятия, которая реализуется на базе вычислительной сети.

Каждое подразделение (отдел) может иметь серверы, доступ к которым нужно ограничить сотрудникам из других отделов. В таком случае целесообразно создать общую физическую сеть с последующим логическим сегментированием определенных частей сети. Такой подход позволяет более гибко планировать работу сети и ее управление, а также повышает безопасность сети. Этот подход может быть реализован с использованием VLAN-сети в соответствии со стандартом IEEE 802.1Q

Рис. 1.0 Виртуальной локальной сетью *(Virtual Local Area Network, VLAN)*

Глава 1. Анализ предметной области и постановка задач диссертации.

1.1 Состояние предметной области и ее особенности

В соответствии с определением управление несанкционированный доступ является одним из видов утечки информации. Как уже было сказано выше, несанкционированным доступом к информации, является доступ к информации, нарушающий установленные правила разграничения доступа. НСД может носить случайный или преднамеренный характер. В результате НСД чаще всего реализуется угроза конфиденциальности информации, однако целью злоумышленника может быть и реализация других видов угроз (целостности информации, раскрытия параметров системы). Выделяют следующие этапы управления доступом:

- идентификация
- аутентификация;
- авторизация (представление объекту полномочий).

Объектами идентификации и аутентификации могут быть человек (должностное лицо, пользователь, оператор), техническое средство (ПК, консоль, терминал), документы. Для преднамеренного несанкционированный доступ используются как общедоступные, так и скрытые способы и средства. Такими способами являются:

- инициативное сотрудничество (предательство);
- склонение к сотрудничеству (подкуп, шантаж);
- подслушивание переговоров самыми различными путями;
- негласное ознакомление со сведениями, составляющими тайну;
- хищение, копирование, подделка, уничтожение;
- незаконное подключение к каналам и линиям связи и передачи данных;
- перехват (акустический или радиоперехват, в том числе и за счет побочных электромагнитных излучений и наводок);

Постановка цели и задач

Целью, данной диссертация является управление доступа с применением технологии VLAN на базе стандарта IEEE 802.1Q. Для достижения цели имеется ряд задач, которые надо разрешить:

1. провести анализ предметной области
2. необходимо создать структуру компьютерной сети в колледже
3. разработка структуры VLAN с стандартом 802.1Q
4. провести моделирование сети в среде Cisco Packet Tracer
5. провести необходимые результаты моделирования и математическую модель впроцедуре расчёта нагрузки в сети

Рассмотрим типичные примеры проектирования виртуальных сетей на основе коммутаторов, поддерживающих стандарт IEEE 802.1Q. Если имеется всего один коммутатор, к портам которого подключаются компьютеры конечных пользователей, то для создания полностью изолированных друг от друга виртуальных сетей все порты должны быть объявлены как Untagget Ports для обеспечения совместимости с сетевыми Ethernet-контроллерами клиентов. Принадлежность узлов сети к той или иной VLAN определяется заданиемидентификатора порта PVID.

Возьмем восьмипортовый коммутатор, на базе которого создаются три изолированные виртуальные сети VLAN#1, VLAN#2 и VLAN#3. Первому и второму портам коммутатора присваивается идентификатор PVID=1. Поскольку идентификаторы этих портов совпадают с идентификатором первой виртуальной сети (PVID=VID), то данные порты образуют виртуальную сеть VLAN#1. Если портам 3, 5 и 6 присвоить PVID=2 (совпадает с идентификатором VID VLAN#2), то вторая виртуальная сеть будет образована портами 3, 4 и 8. Аналогично формируется и VLAN#3 на базе портов 5, 6 и 7. Для обеспечения совместимости с конечным оборудованием (предполагается, что к портам коммутатора

подключаются ПК клиентов сети, сетевые карты которых не совместимы со стандартом IEEE 802.1Q) все порты необходимо сконфигурировать как Untagged.

Если инфраструктура сети включает несколько коммутаторов, поддерживающих стандарт IEEE 802.1Q, то для связи коммутаторов друг с другом необходимо использовать несколько иной принцип конфигурирования. Рассмотрим два шестипортовых коммутатора, которые поддерживают стандарт IEEE 802.1Q и на основе которых необходимо сконфигурировать три изолированные друг от друга виртуальные сети VLAN#1, VLAN#2 и VLAN#3. Пусть к первой виртуальной сети относятся клиенты, подключенные к портам 1 и 2 первого коммутатора и к портам 5 и 6 второго коммутатора. К сети VLAN#2 относятся клиенты, подключенные кпорту 3 первого коммутатора и порту 1 второго коммутатора, а к сети VLAN#3 относятся клиенты, подключенные к портам 4 и 5 первого коммутатора и портам 2 и3 второго коммутатора. Порт 6 первого коммутатора и порт 4 второго коммутатора используются для связи коммутаторов друг с другом.

Чтобы сконфигурировать указанные виртуальные сети, необходимо прежде всего определить на каждом из коммутаторов по три виртуальные сети VLAN#1, VLAN#2 и VLAN#3, задав их идентификаторы (VID=1 для VLAN#1, VID=2 для VLAN#2 и VID=3 для VLAN#3). На первом коммутаторе порты 1 и 2 должны входить в состав VLAN#1, для чего этим портам присваивается PVID=1. Порт 2 первого коммутатора необходимо приписать к VLAN#2, для чего идентификатору порта присваивается значение PVID=2. Аналогично, для портов 5 и 6 первого коммутатора устанавливаются идентификаторы PVID=3, так как эти порты относятсяк VLAN#3.

Все указанные порты первого коммутатора должны быть сконфигурированы как Untagged Port для обеспечения совместимости с сетевыми картами клиентов.Порт 4 первого коммутатора используется для связи со вторым коммутатором и должен передавать кадры всех трех виртуальных сетей без изменения второму коммутатору. Поэтому его необходимо сконфигурировать как Tagged Port и включить в состав всех трех виртуальных сетей (ассоциировать с VID=1, VID=2 и VID=3). При этом идентификатор порта не имеет значения и может быть любым (в

нашем случае PVID=4). Для обмена сообщениями, использующими магистральные фреймы 2-го уровня, для управления добавлением, удалением и переименованием VLAN-сетей в одном домене используется протокол VTP (VLAN Trunk Protocol). Кроме того, протокол VTP позволяет осуществлять централизованные изменения в сети, о которых сообщается всем другим коммутаторам в сети.

1.2 Методы управление доступа

Можно выделить несколько обобщенных категорий методов управление от Несанкционированный доступ, в частности:

- организационные (в т. ч. административные);
- технологические (или инженерно-технические);
- правовые;
- финансовые;
- морально-этические (или социально-психологические).

К первой категории относятся меры и мероприятия, регламентируемые внутренними инструкциями организации, эксплуатирующей информационную систему. Пример такой защиты – присвоение грифов секретности документам и материалам, хранящимся в отдельном помещении, и контроль доступа к ним сотрудников. Вторую категорию составляют механизмы защиты, реализуемые на базе программно-аппаратных средств, например систем идентификации и аутентификации или охранной сигнализации. Третья категория включает меры контроля за исполнением нормативных актов общегосударственного значения, механизмы разработки и совершенствования нормативной базы, регулирующей вопросы защиты информации. Финансовые методы защиты предполагают введение специальных доплат при работе с защищаемой информацией, а также систему вычетов и штрафов за нарушение режимных требований. Морально-этические методы не носят обязательного характера, однако являются достаточно эффективными при борьбе с внутренними нарушителями. Реализуемые на практике методы, как правило, сочетают в себе элементы нескольких из перечисленных категорий. Так, управление доступом в помещения может

представлять собой взаимосвязь организационных (выдача допусков и ключей) и технологических (установку замков и систем сигнализации) способов защиты.

1.2.1 Организационные методы управление доступа

Эффективная управление доступа возможна при обязательном выполнении ряда условий, как-то:

- единство в решении производственных, коммерческих, финансовых и режимных вопросов;
- координация мер безопасности между всеми заинтересованными подразделениями предприятия;
- научная оценка информации и объектов, подлежащих классификации (защите);
- разработка режимных мер до начала проведения режимных работ;
- персональная ответственность (в том числе и материальная) руководителейвсех уровней, исполнителей, участвующих в закрытых работах, за обеспечение сохранности тайны и поддержание на должном уровне режима охраны проводимых работ;
- включение основных обязанностей рабочих, специалистов и администрации по соблюдению конкретных требований режима в коллективный договор, контракт, трудовое соглашение, правила трудового распорядка;
- организация специального делопроизводства, порядка хранения, перевозки носителей коммерческой тайны; введение соответствующей маркировки документов и других носителей закрытых сведений;
- формирование списка лиц, уполномоченных руководителем предприятия классифицировать информацию и объекты, содержащие конфиденциальные сведения;
- оптимальное ограничение числа лиц, допускаемых к КИ;
- наличие единого порядка доступа и оформления пропусков;
- выполнение требований по обеспечению сохранения КИ при проектировании и размещении специальных помещений, в процессе опытно-конструкторской

разработки, испытаний и производства изделий, сбыта, рекламы, подписания контрактов, при проведении особо важных совещаний, в ходе использования технических средств обработки, хранения и передачи информации и т. п.;

- наличие охраны, пропускного и внутриобъектового режимов;
- плановость разработки и осуществления мер по защите КИ, систематический контроль за эффективностью принимаемых мер;
- создание системы обучения исполнителей правилам обеспечения сохранности КИ.

1.3 Анализ Парольные системы

Для рассмотрения принципов построения парольных систем сформулируем несколько основных определений.

Пароль пользователя – некоторая информация, известная только пользователю и парольной системе, которая может быть запомнена пользователем и предъявляется для прохождения процедуры аутентификации. Одноразовый пароль дает возможность пользователю однократно пройти аутентификацию. Многоразовый пароль может быть использован для проверки подлинности повторно. Учетная запись пользователя – совокупность его идентификатора и пароля. Под парольной системой будем понимать программно-аппаратный комплекс, реализующий системы идентификации и аутентификации пользователей. Основными компонентами парольной системы являются:

- интерфейс пользователя;
- интерфейс администратора;
- модуль сопряжения с другими подсистемами безопасности;
- база данных учетных записей.

Наиболее распространенные методы аутентификации основаны на применении многоразовых или одноразовых паролей. Эти методы включают следующие разновидности способов аутентификации:

- по хранимой копии пароля или его свертке (хэш-коду);
- по некоторому проверочному значению;

- без непосредственной передачи информации о пароле проверяющей стороне;
- без непосредственной передачи информации о пароле проверяющей стороне;
- с использованием пароля для получения криптографического ключа.

В первую разновидность способов входят системы аутентификации,предполагающие наличие у обеих сторон копии пароля или его свертки (хэш-кода).Свертка – некоторая последовательность символов, полученная из исходного пароля путем алгебраических преобразований. Часто результат этих преобразований – хэш- функция. Хэш-функция – некоторая функция двух аргументов – ключа и текста, причем восстановить аргумент-текст по значению функции без знания ключа невозможно.

1.4 Хранение паролей

Стойкость парольной системы зависит от способа хранения паролей в базе данных учетных записей. Возможны следующие варианты хранения паролей:

- ❑ в открытом виде;
- ❑ в виде сверток (хэширование);
- ❑ зашифрованными на некотором ключе.

Наиболее безопасное хранение паролей обеспечивается при их хэшировании и последующем шифровании полученных сверток, т. е. при комбинации второго и третьего способов. Стойкость парольной системы определяется ее способностью противостоять атаке злоумышленника, завладевшего базой данных учетных записей и пытающегося восстановить пароли, и зависит от скорости максимально быстрой реализации используемого алгоритма хэширования. При хранении паролей в виде сверток стойкость парольной системы зависит от криптографических свойств алгоритма шифрования или хэширования паролей. Если потенциальный злоумышленник имеет возможность перехватывать передаваемые по сети преобразованные значения паролей, при выборе алгоритма необходимо обеспечить невозможность (с заданной вероятностью) восстановить пароль при наличии достаточного количества перехваченной информации.

Проиллюстрируем приведенные рассуждения на конкретном примере. Для шифрования паролей в системах UNIX до середины 1970-х гг. использовался алгоритм, эмулирующий шифратор М-209 американской армии времен

Второй мировой войны. Это был надежный алгоритм, но он имел очень быструю для тех лет реализацию. На компьютере PDP-11/70 можно было зашифровать 800 паролей в секунду, и словарь из 250000 слов мог быть проверен менее чем за 5 минут. С конца 1970-х для этих целей стал применяться алгоритм шифрования DES. Реализации алгоритма DES работали значительно медленнее. На компьютере jiVAX-П (более быстром, чем PDP-11/70) можно было сделать в среднем 4 операции шифрования в секунду. Проверка словаря из 250000 слов длилась бы 19 часов, а проверка паролей для 50 пользователей – 40 дней. В последнее время в некоторых UNIX-системах используется алгоритм MD5, еще более медленный по сравнению с DES. Однако современные реализации криптографических алгоритмов позволяют производить сотни тысяч итераций алгоритма в секунду. Учитывая недостаточную стойкость часто выбираемых пользователями паролей, можно сделать вывод о том, что получение базы данных учетных записей или перехват переданного по сети значения свертки пароля представляют серьезную угрозу безопасности парольной системы.

1.5 Передача пароля по сети

В большинстве случаев аутентификация происходит в распределенных системах и связана с передачей по сети информации о параметрах учетных записей пользователей. Если передаваемая по сети в процессе аутентификации информация не защищена надлежащим образом, возникает угроза ее перехвата злоумышленником и использования для нарушения защиты парольной системы. Известно, что многие компьютерные системы позволяют переключать сетевой адаптер в режим прослушивания адресованного другим получателям сетевого трафика в сети, основанной на широковещательной передаче пакетов данных.

Следовательно, необходима защита сетевого трафика: физическая защита сети, оконечное шифрование, шифрование пакетов.

Распространены следующие способы передачи по сети паролей:

- в открытом виде;
- зашифрованными;

- в виде сверток;
- без непосредственной передачи информации о пароле («доказательство с нулевым разглашением»).

Первый способ применяется и сегодня во многих популярных приложениях (например, TELNET. FTP и др.). В защищенной системе его можно применять только в сочетании сосредствами защиты сетевого трафика.

Основные типы угроз парольной системе

Парольная система представляет собой «передний край обороны» всей системы безопасности. Некоторые ее элементы (в частности, реализующие интерфейс пользователя) могут быть расположены в местах, открытых для доступа потенциальному злоумышленнику. Поэтому парольная система становится одним из первых объектов атаки при вторжении злоумышленника в защищенную систему. Основные типы угроз безопасности парольным системам, следующие:

1. Разглашение параметров учетной записи:

- через подбор в интерактивном режиме;
- подсматривание;
- преднамеренную передачу пароля его владельцем другому лицу;
- захват базы данных парольной системы (если пароли не хранятся в базе в открытом виде, для их восстановления может потребоваться подбор или дешифрование);
- перехват переданной по сети информации о пароле;
- хранение пароля в доступном месте.

2. Вмешательство в функционирование компонентов парольной системы:

- через внедрение программных закладок;
- обнаружение и использование ошибок, допущенных на стадии разработки;
- выведение из строя парольной системы.

Некоторые из перечисленных типовугроз связаны с наличием так называемого человеческого фактора, проявляющегося в том, что пользователь может:

- выбрать пароль, который легко запомнить и так же легко подобрать;
- записать пароль, который сложно запомнить, и положить запись в доступномместе;
- ввести пароль так, что его смогут увидеть посторонние;
- передать пароль другому лицу намеренно или под влиянием заблуждения.

Существует также «парадокс человеческого фактора», заключающийся в том, что пользователь нередко стремится выступать скорее противником, чем сторонником парольной системы (впрочем, как и любой системы безопасности, функционирование которой влияет на его рабочие условия).

Таким образом, основные факторы, влияющие на безопасность парольной системы, следующие:

- корректное поведение пользователей (пользователи сохраняют свои пароли в тайне отдругих сотрудников и посторонних лиц);
- стойкость процедур генерирования паролей по отношению к атакам подбора постатистике и подбора по словарю;
- реализация в компьютерной системе при коллективной работе пользователейтребований изолированной программной среды;
- защита канала ввода паролей доступа (от перехвата визуальными, визуально-техническими, техническими способами и устройствами).

Бреши и изъяны в парольных системах разграничения доступа в большинстве случаев обусловлены как раз несоблюдением приведенных выше условий. Тем не менее преимущества парольных систем разграничения доступа обусловливают их чрезвычайноширокое применение в телекоммуникационных системах.

Выбор паролей

В большинстве систем пользователи имеют возможность самостоятельно

выбирать пароли или получают их от системных администраторов. При этом для уменьшения деструктивного влияния описанного выше человеческого фактора необходимореализовать ряд рекомендаций по выбору и использованию паролей.

Требование к выбору пароля	Получаемый эффект
1	2
Установление минимальной длины пароля	Усложняет задачу злоумышленника при попытке подсмотреть пароль или подобрать пароль методом «тотального опробования»
Использование в пароле различных групп символов	Усложняет задачу злоумышленника при попытке подобрать пароль методом «тотального опробования»
Проверка и отбраковка пароля по словарю	Усложняет задачу злоумышленника при попытке подобрать пароль по словарю
Установление максимального срока действия пароля	Усложняет задачу злоумышленника по подбору паролей методом «тотального опробования», в том числе без непосредственного обращения к системе защиты (режим *off-line*)
Установление минимального срока действия пароля	Препятствует попыткам пользователя заменить пароль на старый после его смены по предыдущему требованию
Ведение журнала истории паролей	Обеспечивает дополнительную степень защиты по предыдущему требованию
Ограничение числа попыток ввода пароля	Препятствует интерактивному подбору паролей злоумышленником

Таблица1.0 Рекомендации по выбору и использованию паролей

Еще одним способом повышения стойкости паролей при передаче по сети является применение одноразовых (one-time) паролей. Общий подход к применению одноразовых паролей основан на последовательном использовании хэш-функциидля вычисления очередного одноразового пароля на основе предыдущего. Вначале пользователь получает упорядоченный список одноразовых паролей, последний из которых сохраняется в системе аутентификации. При каждой регистрации пользователь вводит очередной пароль, а система вычисляет его свертку и сравнивает с хранимым у себя эталоном. В случае совпадения пользователь успешно проходит аутентификацию, а введенный им пароль сохраняется для

использования в качестве эталона при следующей регистрации. Защита от сетевого перехвата в такой схеме основана на свойстве необратимости хэш-функции. Выбирая тот или иной протокол аутентификации, необходимо определить, какая именно аутентификация требуется – односторонняя или взаимная, нужно ли использовать доверенное третье лицо и если да, то какая из сторон – претендент иливерификатор – будет с ним взаимодействовать. Протоколы без диалоговой аутентификации часто осуществляют еще и контроль целостности данных.

1.6 Основные направления и цели использования криптографических методов

При построении защищенных АС роль криптографических методов для решения различных задач информационной безопасности трудно переоценить. Криптографические методы в настоящее время являются базовыми для обеспечения надежной аутентификации сторон информационного обмена, защиты информации в транспортной подсистеме АС, подтверждения целостности объектов АС и т. д.

Проблемой защиты информации путем ее преобразования занимается криптология (kryptos – тайный, logos – наука). Криптология разделяется на два направления – криптографию и криптоанализ. Цели этих направлений прямо противоположны.

Криптография занимается поиском и исследованием математических методов преобразования информации. Криптография дает возможность преобразовать информацию таким образом, что ее прочтение (восстановление) возможно только при знании ключа.

Сфера интересов криптоанализа – исследование возможности расшифровывания информации без знания ключей.

Основные направления и цели использования криптографических методов:

- передача конфиденциальной информации по каналам связи (например, электронная почта);
- обеспечение достоверности и целостности информации;
- установление подлинности передаваемых сообщений;
- хранение информации (документов, баз данных) на носителях в зашифрованномвиде;

- выработка информации, используемой для идентификации и аутентификациисубъектов, пользователей и устройств;
- выработка информации, используемой для защиты аутентифицирующих элементов защищенной ТКС.

В качестве информации, подлежащей шифрованию и дешифрованию, будут рассматриваться тексты, построенные на некотором алфавите.

Алфавит – конечное множество используемых для кодирования информации знаков.

Текст – упорядоченный набор из элементов алфавита.

В качестве примеров алфавитов, используемых в современных ТКС, можно привести следующие:

• алфавит Z33 – 32 буквы русского алфавита и пробел;
• алфавит Z256 – символы, входящие в стандартные коды ASCII и КОИ-8;
• бинарный алфавит – Z2 = {0,1};
• восьмеричный алфавит или шестнадцатеричный алфавит;

Шифрование – преобразовательный процесс: исходный текст, который носит также название открытого текста, заменяется шифрованным текстом (рис. 2).
Дешифрование – обратный шифрованию процесс. На основе ключа шифрованный текстпреобразуется в исходный (рис. 3).
Ключ – информация, необходимая для беспрепятственного шифрования и дешифрованиятекстов. Обычно ключ представляет собой последовательный ряд букв алфавита.
Криптосистемы разделяются на симметричные и ассиметричные (с открытым ключом).

В *симметричных криптосистемах* и для шифрования, и для дешифрования используется один и тот же ключ: источник зашифровывает открытый текст на секретном ключе К, а приемник расшифровывает шифр текст на секретном ключе К*. Обычно К = К*.

В *ассиметричных системах (системах с открытым ключом)* используются два ключа – открытый и закрытый, которые математически связаны друг с другом. Информация шифруется с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения, или наоборот. *Криптостойкостью* называется характеристика шифра, определяющая его стойкость к дешифрованию без знания ключа (т. е. криптоанализу).

В зависимости от исхода криптоанализа все алгоритмы шифрования можно разделить на три группы. К первой группе относятся совершенные шифры, заведомо не поддающиеся дешифрованию (при правильном использовании). Примером такого шифра является шифр гаммирования случайной равновероятной гаммой.

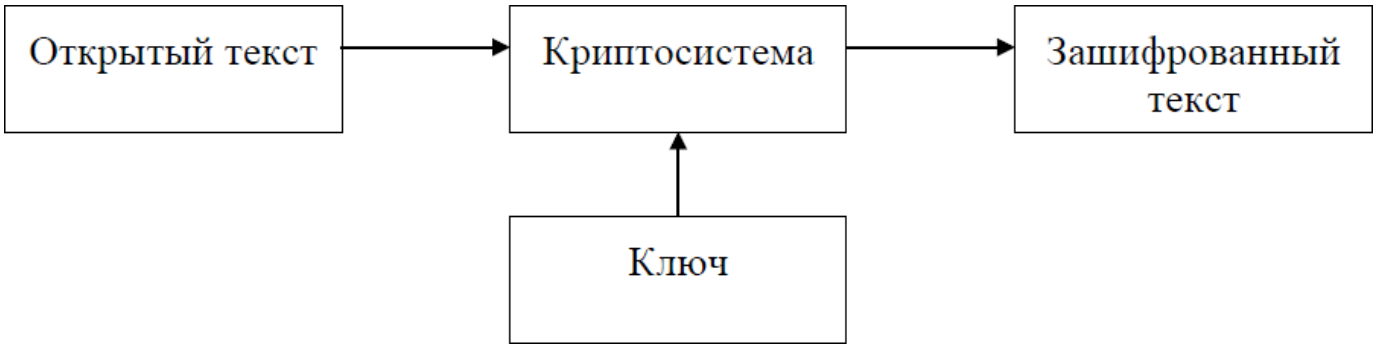


Рис. 2. Шифрование

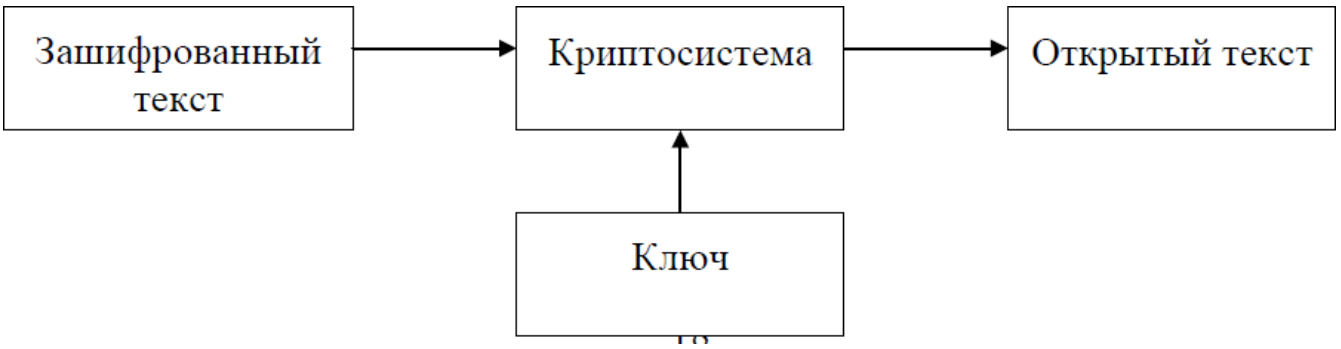


Рис. 1.2 Дешифрование

Во вторую группу входят шифры, допускающие неоднозначное дешифрование. Например, такая ситуация возникает, если зашифровать с помощью шифра простой замены очень короткое сообщение.

Основная масса используемых шифров относится к третьей группе и может быть в принципе однозначно дешифрована. Сложность дешифрования шифра из этой группы будет определяться трудоемкостью используемого алгоритма дешифрования. Следовательно, для оценки стойкости такого шифра необходимо рассмотреть все известные алгоритмы дешифрования и выбрать из них имеющий минимальную трудоемкость, т. е. тот, который работает в данном случае быстрее всех остальных. Трудоемкость этого алгоритма и будет характеризовать стойкость исследуемого шифра. Удобнее всего измерять трудоемкость алгоритма дешифрования в элементарных операциях, но более наглядным параметром является время, необходимое для вскрытия шифра (при этом необходимо указывать технические средства, которые доступны криптоаналитику). Не следует забывать,что вполне возможно существование неизвестного на данный момент алгоритма, который может значительно снизить вычисленную нами стойкость шифра.К большому сожалению разработчиков шифросистем, строго доказать с помощью математических методов невозможность существования простых алгоритмов дешифрования удается чрезвычайно редко. Очень хорошим результатом в криптографии является доказательство того, что сложность решения задачи дешифрования исследуемого шифра эквивалентна сложности решения какой-нибудь известной математической задачи. Такой вывод хотя и не дает 100 % гарантии, но позволяет надеяться, что существенно понизить оценку стойкости шифра в этом случае будет очень непросто.

1.7 Симметричные криптоалгоритмы

Все многообразие существующих криптографических методов можно свести к следующим классам преобразований:

1. Моно- и многоалфавитные подстановки.

Наиболее простой вид преобразований, заключающийся в замене символов исходного текста на другие (того же алфавита) по более или менее сложному правилу. Для

обеспечения высокой криптостойкости требуется использование больших ключей.

2. Перестановки.

Также несложный метод криптографического преобразования. Используется, как правило, в сочетании с другими методами. Подстановка задает перемешивание, перестановка – рассеивание. При перестановке изменяется порядок последовательности битов открытого текста, причем конкретный вид перестановки определяется секретным ключом (ГОСТ 28147–89) или является неизменным (DES). При подстановке совокупность нескольких битов (обычно 4 или 8) открытого текста заменяется совокупностью такого же числа битов, а конкретный вид подстановки определяется секретным ключом. Иногда используется фиксированный набор подстановок и перестановок, как, например, в DES.

3. Гаммирование.

Этот метод заключается в наложении на исходный текст некоторой псевдослучайной последовательности, генерируемой на основе ключа. Гаммирование также является широко применяемым криптографическим преобразованием. Принцип шифрования гаммированием заключается в генерации гаммы шифра с помощью датчика псевдослучайных чисел и наложении полученной гаммы на открытые данные обратимым образом (например, используя сложение по модулю 2).

Процесс дешифрования данных сводится к повторной генерации гаммы шифра при известном ключе и наложению такой гаммы на зашифрованные данные.

Полученный зашифрованный текст является достаточно трудным для раскрытия в том случае, если гамма шифра не содержит повторяющихся битовых последовательностей. По сути дела, гамма шифра должна изменяться случайным образом для каждого шифруемого слова. Фактически же, если период гаммы превышает длину всего зашифрованного текста и не известна никакая часть исходного текста, то шифр можно раскрыть только прямым перебором. Криптостойкость в этом случае определяется размером ключа.

На практике вместо случайной гаммы используют псевдослучайную последовательность. В этом случае, если злоумышленнику становится известен

фрагмент исходного текста и соответствующая ему шифрограмма, простым вычитанием по модулю получается отрезок псевдослучайной последовательности и по нему восстанавливается вся последовательность. Злоумышленник может сделать это на основе догадок о содержании исходного текста. Так, если большинство посылаемых сообщений начинается со слов

«СОВ. СЕКРЕТНО», то криптоанализ всего текста значительно облегчается. Это следуетучитывать при создании реальных систем информационной безопасности.

4. Блочные шифры.

Представляют собой последовательность (с возможным повторением и чередованием) основных методов преобразования, применяемых к блоку (части) шифруемого текста. Блочные шифры на практике встречаются чаще, чем «чистые» преобразования того или иного класса в силу их более высокой криптостойкости. Российский и американский стандарты шифрования основаны именно на этом классе шифров.

1.8 Угрозы безопасности информации при ее обработке СКЗИ

К средствам криптографической защиты информации (СКЗИ) относятся:

- аппаратные;
- программно-аппаратные;
- программные средства.

Предполагается, что СКЗИ используются в некоторой АС (ТКС или сети связи) совместно с механизмами реализации и гарантирования политики безопасности.

Можно говорить о том, что СКЗИ производят защиту объектов на семантическом уровне. В то же время объекты-параметры криптографического преобразования являются полноценными объектами АС и могут быть объектами некоторой политики безопасности (например, ключи шифрования могут и должны быть защищены от НСД, открытыеключи для проверки цифровой подписи – от изменений и т. д.).

Перечислим особенности СКЗИ, наиболее существенно влияющие на их надежность:

- СКЗИ обменивается информацией с внешней средой, а именно: в него вводятся ключи, открытый текст при шифровании;
- СКЗИ в случае аппаратной реализации использует элементную базу ограниченной надежности (т. е. в деталях, составляющих СКЗИ, возможны неисправности или отказы);
- СКЗИ в случае программной реализации выполняется на процессоре ограниченной надежности и в программной среде, содержащей посторонние программы, которые могут повлиять на различные этапыего работы;
- СКЗИ хранится на материальном носителе (в случае программной реализации) и может быть при хранении преднамеренно или случайно искажено;
- СКЗИ взаимодействует с внешней средой косвенным образом (питается от электросети,излучает электромагнитные поля и т. д.);
- СКЗИ изготавливает или/и использует человек, могущий допустить ошибки(преднамеренные или случайные) при разработке и эксплуатации.

Основные причины нарушения безопасности информации при ее обработке СКЗИ:

2. Утечка информации по техническим каналам:
   - электромагнитному высокочастотному прямому (излучение электронно-лучевой трубки дисплея, несущее информацию о выводе на экран, высокочастотное излучение системного блока, модулированное информативным сигналом общей шины и т. д.);
   - электромагнитному низкочастотному прямому (поле с сильной магнитной составляющей от магнитных элементов типа катушек или трансформаторов);
   - электромагнитному косвенному (наводки на проводящие линии и поверхности, модуляция гетеродинов вспомогательной аппаратуры);
   - акустическому (звуки и вибрации от нажатий клавиш и работыпринтера, голоса оператора СКЗИ);
   - визуальному (просмотр или фотографирование текстов на экране,

принтере или иных устройствах отображения информации);

- акустоэлектрическому (преобразование звуковых и вибрационных сигналов в электрические с помощью вспомогательного оборудования – телефона, электрочасов, осветительных приборов и т. д.);
- сетевому (неравномерность потребляемого от сети тока, наводки на проводапитания);
- по шине заземления или по линии связи компьютер–связное оборудование (модем) (наводки сигнала от СКЗИ в линии связи или заземления).
- посредством анализа вспомогательных материалов (красящих лент, неисправных дискет и винчестеров и т. д.).

3. Неисправности в элементах СКЗИ.

Сбои и неисправности в элементах СКЗИ могут сказаться:

- на виде шифрующего преобразования (можно показать, что в общем случае фиксация нулевых или единичных потенциалов приведет к упрощению реализации шифрующего преобразования);протоколах взаимодействия аппаратуры или программ СКЗИ с прочим оборудованием и программами (например, ввод каждый раз фиксированного ключа);
- процедурах считывания ключа.

4. Работа совместно с другими программами.

При этом речь может идти об их непреднамеренном и преднамеренном влиянии.

Непреднамеренное влияние

Пусть программа зашифровывает файл и помещает шифртекст в тот же файл. Предположим, что в то же время работает программа запрета записи на диск. Тогда результатом шифрования будет исходный незашифрованный файл. В общем случае источником непреднамеренного взаимного влияния является, как правило, конкуренция за ресурсов вычислительной среды и некорректная обработка ошибочных ситуаций.

Преднамеренное влияние

При рассмотрении этой ситуации применяют термин «программная закладка» (некоторые авторы используют термин «криптовирус»). Речь идет о специализированном программном модуле, целенаправленно воздействующем на СКЗИ. Программная закладка может работать в следующих режимах:

- пассивном – сохранение вводимых ключей или открытых текстов без влияния на информацию;
- активном – влияние на процессы записи–считывания программ шифрования и цифровой подписи без изменения содержания информации (пример – программная закладка для системы цифровой подписи Pretty Good Privacy (PGP), выполняющая навязывание укороченных текстов для хэширования), влияние на процессы считывания и записи с изменением информации, изменение алгоритма шифрования путем редактирования исполняемого кода в файле или оперативной памяти.

3. Воздействие человека.

Разработчик преднамеренно или непреднамеренно может наделить программу некоторыми свойствами (например, возможностью переключения в отладочный режим с выводом части информации на экран или внешние носители). Эксплуатирующий программу защиты человек может решить, что программа для него «неудобна», и использовать ее неправильно (вводить короткие ключи либо повторять один и тот же ключ для шифрования разных сообщений). То же замечание относится и к аппаратным средствам защиты. В связи с этим помимо встроенного контроля за пользователем необходимо отслеживание правильности разработки и использования средств защиты с применением организационных мер.

1.9. Технические методы управление доступа . Идентификация и аутентификация

Рассмотрим подробнее такие взаимосвязанные методы управление доступа, как идентификация, аутентификация и VLAN преобразование информации. Под безопасностью (стойкостью) системы идентификации и аутентификации будем понимать гарантированность того, что злоумышленник. не способен пройти аутентификацию от имени другого пользователя. В этом смысле чем выше стойкость системы аутентификации, тем сложнее злоумышленнику решить

указанную задачу. Система идентификации и аутентификации является одним из ключевых элементов инфраструктуры защиты от НСД любой информационной системы. Различают три группы методов аутентификации, основанных на наличии у пользователей:

- индивидуального объекта заданного типа;
- индивидуальных биометрических характеристик;
- знаний некоторой известной только пользователю и проверяющей сторонеинформации.

К первой группе относятся методы аутентификации, предполагающие использование удостоверений, пропуска, магнитных карт и других носимых устройства, которые широко применяются для контроля доступа в помещения, а также входят в состав программно-аппаратных комплексов защиты от НСД к средствам вычислительной техники.

Во вторую группу входят методы аутентификации, основанные напримененении оборудования для измерения и сравнения с эталоном заданных индивидуальных характеристик пользователя: тембра голоса, отпечатков пальцев, структуры радужной
оболочки глаза и др. Такие средства позволяют с высокой точностью аутентифицировать обладателя конкретного биометрического признака, причем «подделать» биометрические параметры практически невозможно.

Последнюю группу составляют методы аутентификации, при которых используются пароли. По экономическим причинам они включаются в качестве базовых средств защиты во многие программно-аппаратные комплексы защиты информации. Все современные операционные системы и многие приложения имеют встроенные механизмы парольной защиты.

Если в процедуре аутентификации участвуют только две стороны, устанавливающие подлинность друг друга, такая процедура называется непосредственной аутентификацией. Если же в процессе аутентификации участвуют не только эти стороны, но и другие, вспомогательные, говорят об аутентификации с
участием доверенной стороны. Третью сторону называют сервером аутентификации

или арбитром.

Рассмотрим особенности различных методов аутентификации.

1) Методы аутентификации с использованием индивидуальных объектов заданного типа:а) использование ключей.

Существуют определенные требования, которым должны удовлетворять ключи, например, ключи для цилиндровых штифтовых замков должны иметь не менее 5 выемок, причем не более трех одинаковой глубины, ключи для сувальных замков должны быть двухбородочными и иметь не менее 6 сувальд

(количество ступенек бородки минус одна). Ключи используются в основном для разграничения доступа в помещение, однако могут определять и доступ к рабочему месту, терминалу. Для этих целей применяются также ключевые дискеты;

б) Использование идентификационных карточек.

Существуют различные виды идентификационных карточек, среди которых можно выделить:

- карточки с эмбоссированием (объемное изображение);
- магнитные карточки. Идентификационная информация содержится на куске магнитной пленки. Для увеличения защищенности выпускают многослойные корточки, состоящие из нескольких пленок с разными магнитными характеристиками;
- виганд-карточки, в каждую из которых вклеена тонкая проволока из виганд- сплава, обладающая уникальными магнитными свойствами, формирующимися в процессе изготовления;
- оптические карточки. Простейшие из них содержат штрих-код, более сложные выполнены с использованием лазерных технологий и представляют собой небольшой оптический диск;
- проксими-карты. Существуют активные – с источником питания и пассивные, которые нужно облучать магнитным полем, индуцируемым считывателем, после чего карточка передает свой код. Считывание кода возможно дистанционно. Система считывания может быть

закамуфлирована. При помощи таких карточек легко организовать контроль за перемещением по объекту;

- карты памяти с микрочипом. (например, телефонные);
- март-карты, которые по своим возможностям приближаются к небольшому компьютеру: в них имеется процессор, ОЗУ, ПЗУ. Такая карта служит не только средством аутентификации, но может использоваться для расчетов, обменаинформацией.

Для увеличения степени защищенности применяют комбинированные карточки, например с эмбоссированием и магнитной полосой. Наибольшей надежностью обладаютвиганд-карты и смарт-карты.

2) Методы биометрической аутентификации.

В последнее время биометрическая аутентификация получает все более широкое распространение. Основные достоинства этих методов: трудно подделать, нельзя украсть, всегда с собой. При биометрической аутентификации используются статическиеили динамические признаки:

а) формы аутентификации с использованием статических признаков.

Статические признаки более стабильны, чем динамические, поэтому такая аутентификация более надежна. Чаще всего для аутентификацииииспользуются отпечатки пальцев (дактилоскопия). В настоящее время существуют встроенные системы, выпускается мышь с дактилоскопическим датчиком. В качестве признаков для аутентификации используются также геометрическая форма ладоней рук, расположение кровеносных сосудов на сетчатке глаза, форма и размер лица, цвет и рисунок радужной оболочкиглаза, форма фигуры и масса тела. б) формы аутентификации с использованием динамических признаков.

Используется аутентификация по почерку, обычно по росписи. Используются устройства ввода графической информации. Рассматривается наличие точек, выбросов, разрывов, протяженных участков без кривизны, участков с большим количеством линий, направления линий, число и направление

переходов. Получается эталонная аппроксимация, подделать которую невозможно.

Применяется аутентификация по клавиатурному почерку. Претенденту предлагается набор ключевой фразы или набор свободного текста, например фразы «Внимание! Идет аутентификация по клавиатурному почерку». Фраза должна иметь достаточную длину, равномерное распределение по клавиатуре. Программными средствами запоминаются интервалы (или относительные интервалы) между нажатиями клавиш. Для распознавания небольшого числа претендентов достаточно оценить статистические характеристики (математическое ожидание, дисперсию). Если пользователей много, то в системе хранится образ для каждого человека. При наборе свободного текста вся клавиатура делится на несколько зон и фиксируется время перехода из одной зоны в другую. Это позволяет оперативными методами контролировать, кто пользуется клавиатурой.

Для использования системы идентификации по голосу достаточно наличия звуковой карты. В процессе обучения системы подбирается фраза или несколько фраз с достаточным количеством идентификационных признаков.

Надежность систем аутентификации по динамическим признакам в ряде случаев зависит от физического состояния человека. Кроме того, надо иметь в виду, что существуют люди, не обладающие стабильными динамическими признаками.

3) Методы аутентификации с использованием паролей.

Аутентификация с использованием пароля является в настоящее время наиболее распространенным способом подтверждения подлинности обмена в ТКС. Однако специалисты в области информационной безопасности признают, что эти методы имеют существенные недостатки. Обзор современных парольных систем приведен в гл. 8.5.

Глава 2. Методы исследования

До появления общепризнанного стандарта по организации виртуальных сетей IEEE 802.1Q каждый производитель сетевого оборудования использовал собственную технологию организации VLAN. Такой подход имел существенный недостаток — технологии одного производителя были несовместимы с

технологиями других фирм. Поэтому при построении виртуальных сетей на базе нескольких коммутаторов необходимо было использовать только оборудование от одного производителя. Принятие стандарта виртуальных сетей IEEE 802.1Q позволило преодолеть проблему несовместимости, однако до сих пор существуют коммутаторы, которые либо не поддерживают стандарт IEEE 802.1Q, либо, кроме возможности организации виртуальных сетей по стандарту IEEE 802.1Q, предусматривают и иные технологии.

Существует несколько способов построения виртуальных сетей, но сегодня в коммутаторах главным образом реализуется технология группировки портов или используется спецификация IEEE 802.1Q.

2.1 Создание виртуальные сети на основе группировки портов

При создании виртуальных сетей на основе одного коммутатора обычно используется механизм группирования портов коммутатора (рис. 3). При этом каждый порт приписывается той или иной виртуальной сети. Кадр, пришедший от порта, принадлежащего, например, виртуальной сети 1, никогда не будет передан порту, который не принадлежит этой виртуальной сети.

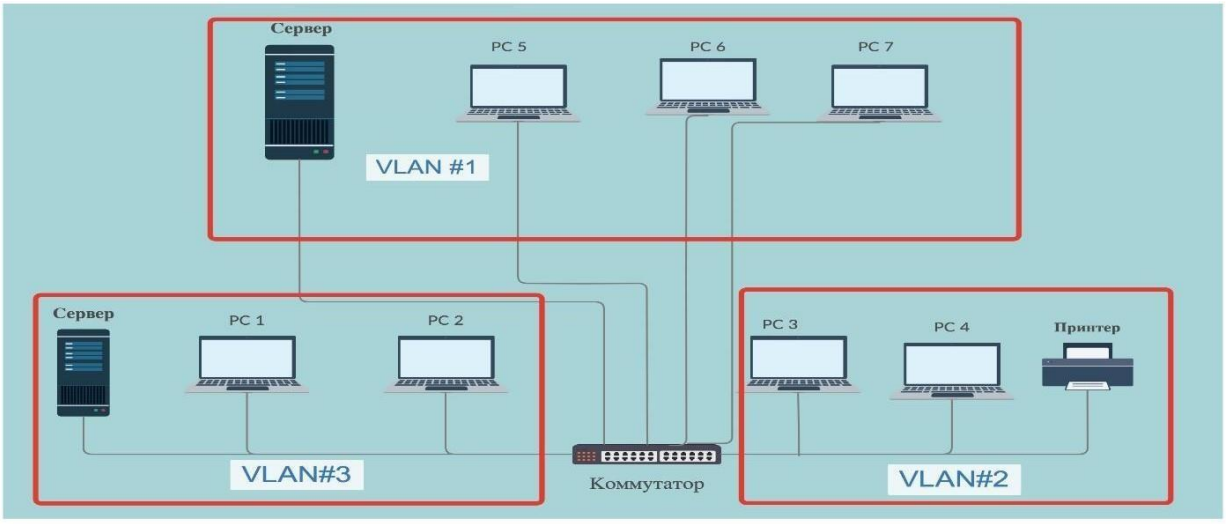


Рис 1.3 Виртуальные сети построенные на одном коммутатор

Созданиевиртуальных сетей путем группирования портов не требует от администратора большого объема ручной работы — достаточно каждый порт приписать к одной из нескольких заранее поименованных виртуальных сетей. Обычно такая операция выполняется с помощью специальной программы, прилагаемой к коммутатору. Второй способ образования виртуальных сетей основан на группировании MAC- адресов. Каждый MAC-адрес, который изучен коммутатором, приписывается той или иной виртуальной сети. При существовании в сети множества узлов этот способ требуетот администратора большого объема ручной работы. Однако при построении виртуальных сетей на основе нескольких коммутаторов он оказывается более гибким, чем группирование портов.

2.2 Создание виртуальные сети на основе стандарта IEEE 802.1Q

Анализ IEEE 802.1 q

Механизм тегирования IEEE 802.1q кажется довольно простым и эффективным благодаря своим 4-байтовым накладным расходам, зажатым между исходным адресом и полем Типа/длины нашего фрейма Ethernet :

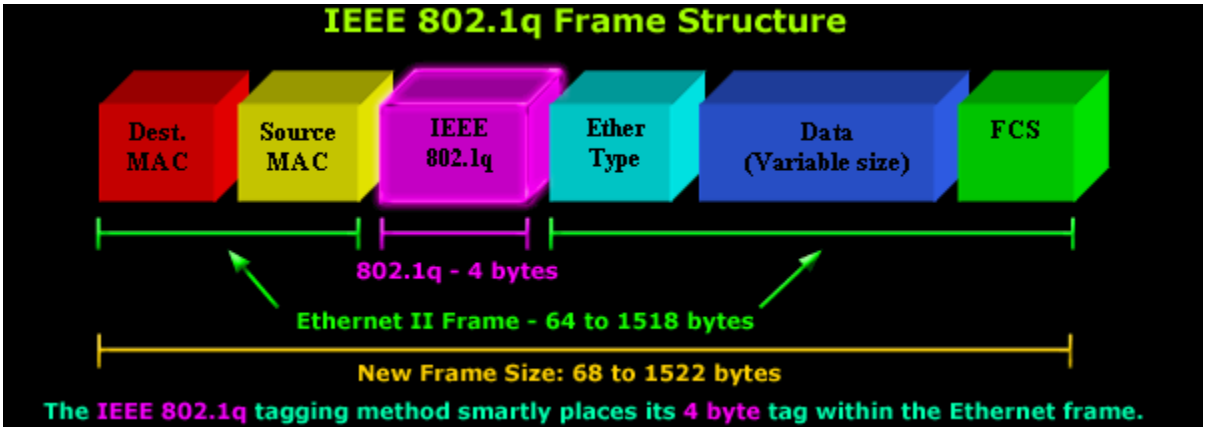


Рис 1.4 Структура помеченного кадра Ethernet

Процесс вставки тега 802.1 q в кадр Ethernet приводит к тому, что исходное поле Проверки последовательности кадров (FCS) становится недействительным, поскольку мы изменяем кадр, поэтому важно, чтобы новый FCS был пересчитан на основе нового кадра, теперь содержащего поле IEEE 802.1 q. Этот процесс

автоматически выполняется коммутатором непосредственно перед отправкой кадра по магистральной линии. Здесь мы сосредоточимся на розовом 3D-блоке, обозначенном как заголовок IEEE 802.1 q.

Заголовок IEEE 802.1 q

Как уже отмечалось, заголовок 802.1 q имеет длину всего 4 байта или 32 бита, в то время как в этом пространстве находится вся необходимая информация, необходимая для успешной идентификации VLAN кадра и обеспечения его прибытия в правильное место назначения. На приведенной ниже диаграмме анализируются все поля, содержащиеся в заголовке 802.1 q:

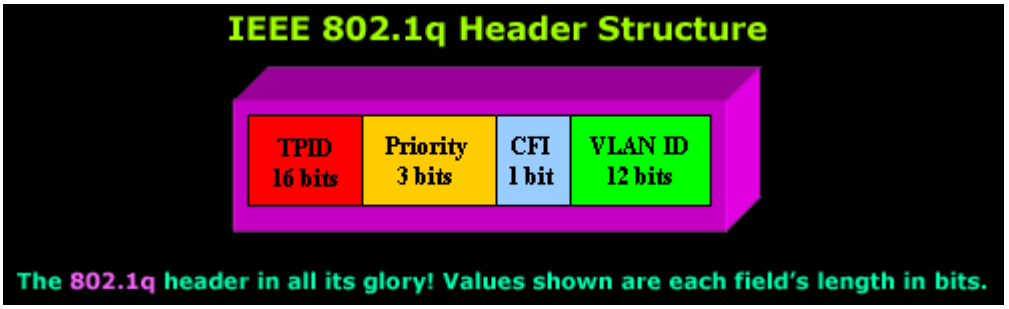


Рис. 1.5 Структура заголовка 802.1 q

Структура довольно проста, так как существует всего 4 поля. Мы продолжим анализ каждой из этих областей, чтобы выяснить, что представляет собой протокол.

TPID - Tag Protocol Identifier - Поле TPID имеет длину 16 бит. Он используется для идентификации кадра как помеченного кадра IEEE 802.1 q.

Приоритет - Поле приоритета имеет длину всего 3 бита, но используется для приоритизации данных, которые несет этот кадр.

CFI - Индикатор канонического формата - Поле CFI имеет длину всего 1 бит. Если установлено значение "1", то это означает, что MAC-адрес находится в неканоническом формате, в противном случае " 0 " означает, что это канонический формат. Для коммутаторов Ethernet это поле всегда равно нулю (0). Поле CFI в основном используется по соображениям совместимости между сетями Ethernet и Token Ring.

VLAN ID - Идентификатор виртуальной локальной сети - Поле VLAN ID является,

пожалуй, самым важным полем из всех, потому что мы можем определить, к какой VLAN принадлежит кадр, позволяя принимающему коммутатору решать, из каких портов кадру разрешено выходить в зависимости от конфигурации коммутатора.

Дополнительное поле с пометкой о номере виртуальной сети используется только тогда, когда кадр передается от коммутатора к коммутатору, а при передаче кадра конечному узлу оно обычно удаляется. При этом модифицируется протокол взаимодействия

«коммутаторкоммутатор», а программное и аппаратное обеспечение конечных узлов остается неизменным. До принятия стандарта IEEE 802.1Q существовало много фирменных протоколов этого типа, но все они имели один недостаток — оборудование различных производителей при образовании VLAN оказывалось несовместимым.

Тег виртуальной локальной сети состоит из поля TCI (Tag Control Information — управляющая информация тега) размером в 2 байта и предшествующего ему поля EtherType, которое является стандартным для кадров Ethernet и также состоит из двух байтов (рис. 4).

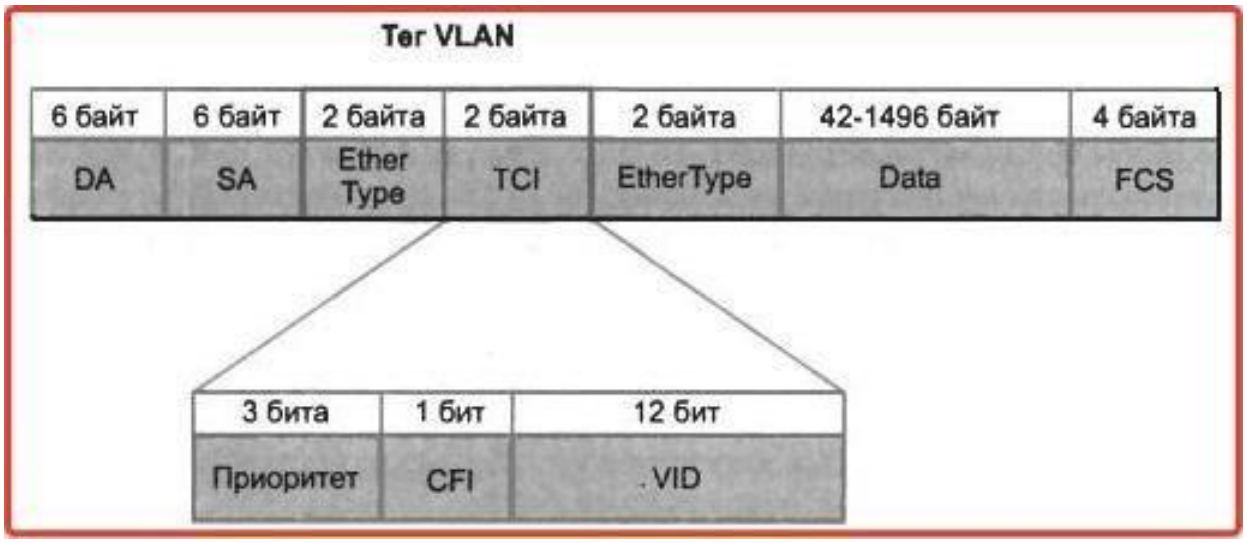


Рис. 1.6 Структура помеченного кадра Ethernet

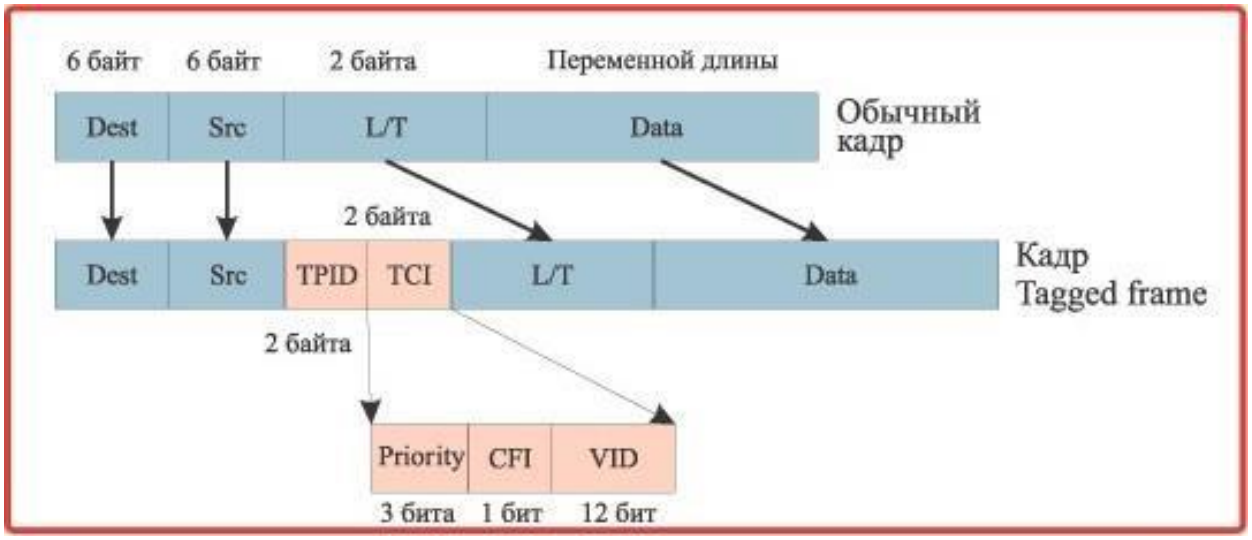


Рис. 1.7 Сравнение обычного Ethernet-кадра и кадра с меткой

Тег VLAN не является обязательным для кадров Ethernet. Кадр, у которого имеется такой заголовок, называют помеченным (tagged frame). Коммутаторы могут одновременно работать как с помеченными, так и с непомеченными кадрами. Из-за добавления тега VLAN максимальная длина поля данных уменьшилась на 4 байта. Добавляемая метка кадра включает в себя двухбайтовое поле TPID (Tag Protocol Identifier) и двухбайтовое поле TCI (Tag Control Information). Поле TCI, в свою очередь, состоит из полей Priority, CFI и VID. Поле Priotity длиной 3 бита задает восемь возможных уровней приоритета кадра. Поле VID (VLAN ID) длиной 12 бит является идентификатором виртуальной сети. Эти 12 бит позволяют определить 4096 различных виртуальных сетей, однако идентификаторы 0 и 4095 зарезервированы для специального использования, поэтому всего в стандарте 802.1Q возможно определить 4094 виртуальные сети. Поле CFI (Canonical Format Indicator) длиной 1 бит зарезервировано для обозначения кадров сетей других типов (Token Ring, FDDI), передаваемых по магистрали Ethernet, и для кадров Ethernet всегда равно 0.

Изменение формата кадра Ethernet приводит к тому, что сетевые устройства, не поддерживающие стандарт IEEE 802.1Q (такие устройства называют Tag-unaware), не могут работать с кадрами, в которые вставлены метки, а сегодня подавляющее большинство сетевых устройств (в частности, сетевые Ethernet-контроллеры конечных узлов сети) не поддерживают этот стандарт. Поэтому для обеспечения совместимости с устройствами, поддерживающими стандарт IEEE

802.1Q (Tag-aware-устройства), коммутаторы стандарта IEEE 802.1Q должны поддерживать как традиционные Ethernet- кадры, то есть кадры без меток (Untagged), так и кадры с метками (Tagged).

Входящий и исходящий трафики, в зависимости от типа источника и получателя, могут быть образованы и кадрами типа Tagged, и кадрами типа Untagged — только в этом случае можно достигнуть совместимости с внешними по отношению к коммутатору устройствами. Трафик же внутри коммутатора всегда образуется пакетами типа Tagged. Поэтому для поддержки различных типов трафиков и для того, чтобы внутренний трафик коммутатора образовывался из пакетов Tagged, на принимаемом и передающем портах коммутатора кадры должны преобразовываться в соответствии с предопределенными правилами.

Линия доступа связывает пррт коммутатора (называемый в этом случае портом доступа)с компьютером, принадлежащим некоторой виртуальной локальной сети.

Транк — это линия связи, которая соединяет между собой порты двух коммутаторов; в общем случае через транк передается трафик нескольких виртуальных сетей.

Коммутаторы, поддерживающие технику VLAN, без специального конфигурирования по умолчанию работают как стандартные коммутаторы, обеспечивая соединения всех со всеми. В сети, образованной такими коммутаторами, все конечные узлы по умолчаниюотносятся к условной сети VLAN1 с идентификатором VID, равным 1. Все порты этой сети, к которым подключены конечные узлы, по определению являются портами доступа.

2.3 Правила входящего порта (Ingress rules)

Рассмотрим более подробно процесс передачи кадра через коммутатор (рис. 6). По отношению к трафику каждый порт коммутатора может быть как входным, так и выходным. После того как кадр принят входным портом коммутатора, решение о его дальнейшей обработке принимается на основании предопределенных правил входного порта (Ingress rules). Поскольку принимаемый кадр может относиться как к типу Tagged, так и к типу Untagged, то правилами входного порта определяется, какие типы кадров должны приниматься портом, а какие отфильтровываться.

Возможны следующие варианты: прием только кадров типа Tagged, прием только кадров типа Untagged, прием кадров обоих типов. По умолчанию для всех коммутаторов правилами входного порта устанавливается возможность приема кадров обоих типов.

Рис. 1.8 Процесс продвижения кадров в коммутаторе, совместимом со стандартом IEEE 802.1Q Если правилами входного порта определено, что он может принимать кадр Tagged, в котором имеется информация о принадлежности к конкретной виртуальной сети (VID), то этот кадр передается без изменения. А если определена возможность работы с кадрами типа Untagged, в которых не содержится информации о принадлежности к виртуальной сети, то прежде всего такой кадр преобразуется входным портом коммутатора к типу Tagged (напомним, что внутри коммутатора все кадры должны иметь метки о принадлежности к виртуальной сети).

Чтобы такое преобразование стало возможным, каждому порту коммутатора присваивается уникальный PVID (Port VLAN Identifier), определяющий принадлежность порта к конкретной виртуальной сети внутри коммутатора (по умолчанию все порты коммутатора имеют одинаковый идентификатор PVID=1). Кадр типа Untagged преобразуется к типу Tagged, для чего дополняется меткой VID (рис. 6). Значение поля VID входящего Untagged-кадра устанавливается равным значению PVID входящего порта, то есть все входящие Untagged-кадры автоматически приписываются к той виртуальной сети внутри коммутатора, к которой принадлежит входящий порт.

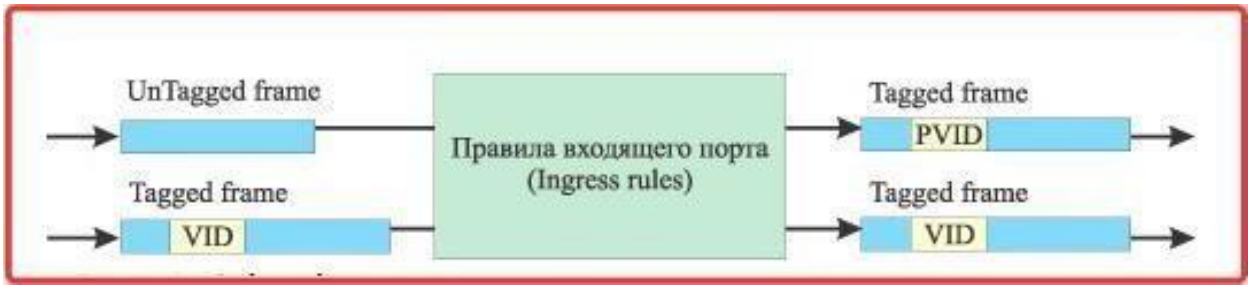


Рис. 1.9 Обработка кадров входящим портом коммутатора

2.4 Правила продвижения пакетов (Forwarding Process)

После того как все входящие кадры отфильтрованы, преобразованы или оставлены без изменения в соответствии в правилами входящего порта, решение об их передаче к выходному порту основывается на предопределенных правилах продвижения пакетов. Правило продвижения пакетов внутри коммутатора заключается в том, что пакеты могут передаваться только между портами, ассоциированными с одной виртуальной сетью.

Как уже отмечалось, каждому порту присваивается идентификатор PVID, который используется для преобразования принимаемых Untagged-кадров, а также для определения принадлежности порта к виртуальной сети внутри коммутатора с идентификатором VID=PVID. Таким образом, порты с одинаковыми идентификаторами внутри одного коммутатора ассоциируются с одной виртуальной сетью. Если виртуальная сеть строится на базе одного коммутатора, то идентификатора порта PVID, определяющего его принадлежность к виртуальной сети, вполне достаточно. Правда, создаваемые таким образом сети не могут перекрываться, поскольку каждому порту коммутатора соответствует только один идентификатор. В этом смысле создаваемые виртуальные сети не обладали бы такой гибкостью, как виртуальные сети на основе портов. Однако стандарт IEEE 802.1Q с самого начала задумывался для построения масштабируемой инфраструктуры виртуальных сетей, включающей множество коммутаторов, и в этомсостоит его главное преимущество по сравнению с технологией образования VLAN на основе портов. Но для того, чтобы расширить сеть за пределы одного коммутатора, одних идентификаторов портов недостаточно, поэтому каждый порт может быть ассоциирован с несколькими виртуальными сетями, имеющими

различные идентификаторы VID.

Если адрес назначения пакета соответствует порту коммутатора, которыйпринадлежит к той же виртуальной сети, что и сам пакет (могут совпадать VID пакетаи VID порта или VID пакета и PVID порта), то такой пакет может быть передан. Если же передаваемый кадр принадлежит к виртуальной сети, с которой выходной порт никак не связан (VID пакета не соответствует PVID/VID порта), то кадр не может быть передан и отбрасывается.

2.5 Правила выходного порта (Egress rules)

После того как кадры внутри коммутатора переданы на выходной порт, их дальнейшее преобразование зависит от правил выходного порта. Как уже говорилось, трафик внутри коммутатора создается только пакетами типа Tagged, а входящий и исходящий трафики могут быть образованы пакетами обоих типов. Соответственно правилами выходного порта (правило контроля метки — Tag Control) определяется, следует ли преобразовывать кадры Tagged к формату Untagged.

Каждый порт коммутатора может быть сконфигурирован как Tagged или Untagged Port. Если выходной порт определен как Tagged Port, то исходящий трафик будет создаваться кадрами типа Tagged с информацией о принадлежности к виртуальной сети. Следовательно, выходной порт не меняет тип кадров, оставляя их такими же, какими они были внутри коммутатора. К указанному порту может быть подсоединено только устройство, совместимое со стандартом IEEE 802.1Q, например коммутатор или сервер с сетевой картой, поддерживающей работу с виртуальными сетями данного стандарта.

Если же выходной порт коммутатора определен как Untagged Port, то все исходящие кадры преобразуются к типу Untagged, то есть из них удаляется дополнительная информация о принадлежности к виртуальной сети. К такому порту можно подключать любое сетевое устройство, в том числе коммутатор, не совместимый со стандартом IEEE 802.1Q, или ПК конечных клиентов, сетевые карты которых не поддерживают работу с виртуальными сетями этого стандарта.

Глава 3. Основные требования к сети

Сейчас невозможно представить офис без единой локальной сети. ЛВС находят широкое применение, как часть информационной системы той или иной фирмы. Локально-вычислительная сеть есть в каждом офисе, на промышленных предприятиях, в зданиях различного назначения, банках. Грамотно реализованная и отвечающая современным стандартам безопасности ЛВС работает надежно и качественно, обеспечивая в офисе стабильное информационное взаимодействие.

Основными требованиями к ЛВС, являются:

- **Открытость** — возможность подключения дополнительных компьютеров и других устройств, а также линий (каналов) связи без изменения технических и программных средств существующих компонентов сети.
- **Гибкость** — сохранение работоспособности при изменении структуры в результате выхода из строя любого компьютера или линии связи.
- **Эффективность** — обеспечение требуемого качества обслуживания пользователей при минимальных затратах.

Для того чтобы достичь наилучших результатов по открытости, гибкости, эффективности необходим модульный и иерархический подход к дизайну сети передачи данных. Такой подход позволяет наращивать сеть, оптимальным путем добавления новых блоков, не затрагивая остальные компоненты сетевой структуры, обеспечивает крайне высокий степень определённости в поведении сети, что облегчает поиск и устранение неисправностей.

Таким образом, при правильном построении компьютерной сети и грамотном администрировании легко обеспечивается доступ к необходимой информации, а также ее защита от несанкционированного доступа. Вложенные на этапе организации финансовые средства обеспечивают системе долговечность и эффективность, в дальнейшем сеть быстро окупится и потребует минимальных затрат на эксплуатацию.

3.1 Уровень ядра

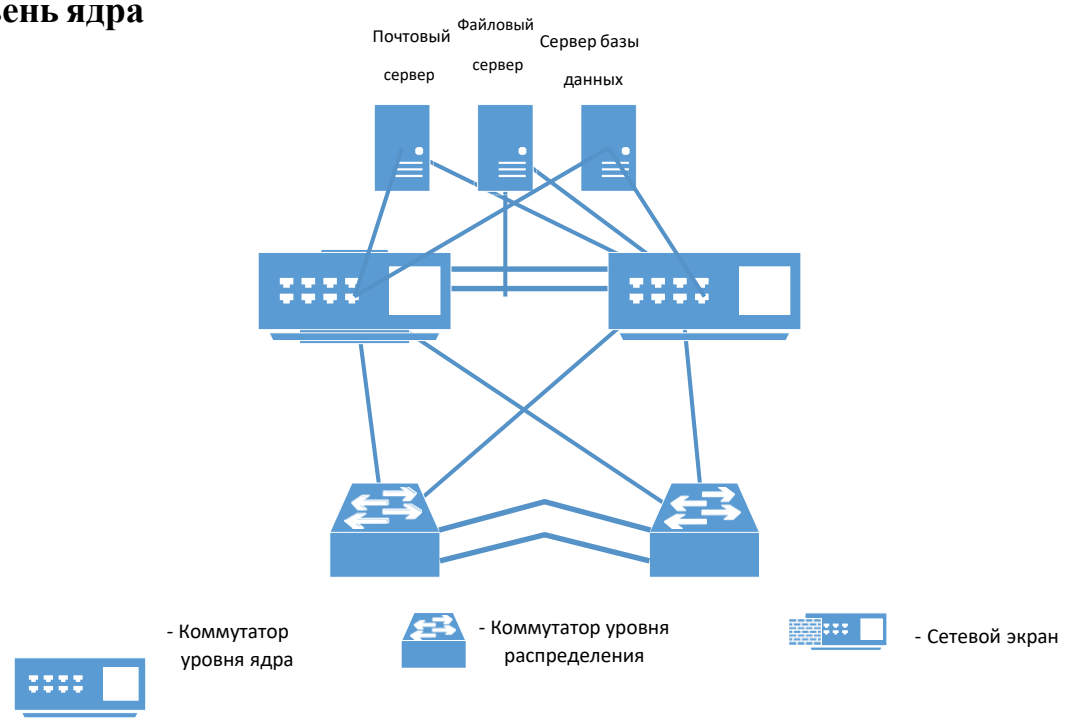


Рис. 2 Ядро сети

Этот уровень отвечает за быструю и надежную пересылку больших объемов трафика. Единственным предназначением уровня ядра является быстрая коммутация трафика. Трафик передается совместно для нескольких пользователей. Однако на уровне распределения обрабатываются пользовательские данные, чтоможет привести к дополнительным запросам к ядру сети.

Если происходит ошибка на уровне ядра, то она влияет на всех пользователей. Следовательно, весьма важно здесь обеспечить высокую надежность. На этом уровне обрабатываются большие объемы трафика, поэтому не менее важно учитывать скорость и задержки. Отметив функции данного уровня, перейдем к особенностям реализации: Ничто не должно замедлять трафик, в том числе списки доступа, маршрутизация между виртуальными локальными сетями VLAN и фильтрация пакетов.

Не следует реализовывать функции доступа для рабочей группы.

Необходимо исключить расширение уровня ядра при росте размеров объединенной сети (например, при добавлении коммутаторов).

Если на базовом уровне возникают проблемы с производительностью, лучше выбрать модернизацию, а не расширение.

Ядро сети будет предоставлять высокоскоростной доступ к информационным ресурсам сети – серверной ферме, а также, выполнять высокоскоростной транспорт данных. Для обеспечения высокой надежности и скорости коммутаторы и серверы соединим избыточными каналами связи.

Любое активное оборудование потребляет электроэнергию и передает сигналы, так и работа оборудования ядра зависит от источников питания, и в случае отсутствия электроэнергии парализуется работа всей сети в целом. Поэтому для надежной работы оборудования этого уровня требуется предусмотреть источник бесперебойного питания.

3.2 Узел резервирования

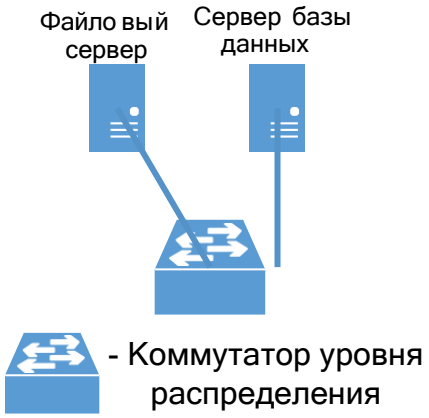


Рис. 2.1 Узел резервирования

– Бэкап сервер позволит обеспечить резервное копирование сохранить критические данные серверов в случае выхода их из строя, в случае случайной потери данных вследствие ошибок операторов и т.п.

- Во время копирования возможно сильное проседание по производительности основной системы. Поэтому создание резервных копий всегда планируют на период минимальной активности. Однако растет число систем, которые обслуживают запросы круглосуточно.

- **Сервер баз данных**. Выполняет обслуживание и управление базой данных и отвечает за целостность и сохранность данных.

- **Файловый сервер**. Предназначен для выполнения файловых операций ввода-вывода и хранения файлов любого типа.

Важное требование к серверам данной категории это большой объем дисковогопространства и высокая скорость записи и чтения данных.

3.3 Уровень распределения

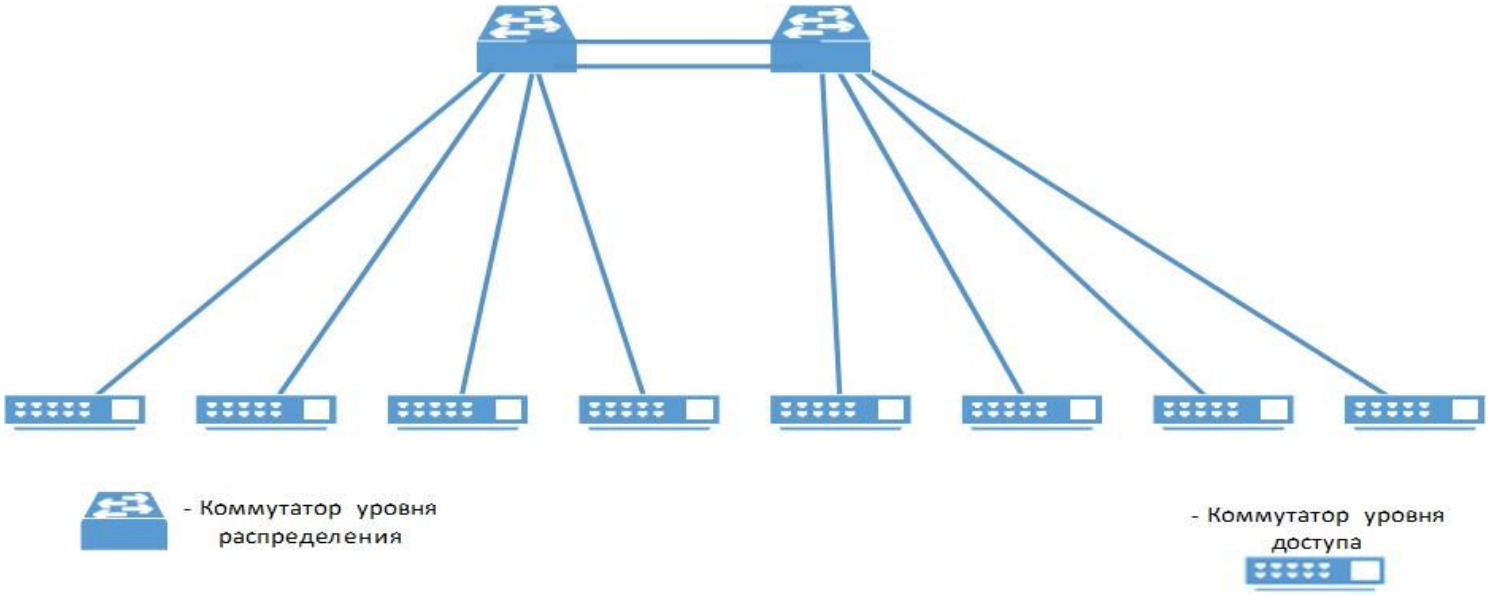


Рис. 2.3 Уровень распределения

Он расположен между базовым уровнем и уровнем доступа. Основные функции уровня распределения состоят в маршрутизации, фильтрации и доступе к региональным сетям, а также (если необходимо) в определении правил доступа пакетов к базовому уровню. Уровень распределения обязан устанавливать наиболее быстрый способ обработки запросов к службам (например, метод файлового обращения к серверу). После определения на уровне распределения наилучшегопути доступа, запрос может быть передан на уровень ядра, где реализован скоростной транспорт запроса к нужной службе. Устанавливается политика сети, а также обеспечиваются возможности гибкого описания сетевых операций.

На уровне распределения выполняется несколько функций:

- Реализация инструментов, подобных спискам доступа, фильтрации пакетов илимеханизму запросов.
- Реализация системы безопасности и сетевых политик, включая

трансляциюадресов и установку брандмауэров.

- Перераспределение между протоколами маршрутизации, включая использование статических путей. Маршрутизация между сетями VLAN и другие функции поддержки рабочихгрупп.

На уровне распределения не следует выполнять те функции, которые свойственны двум другим уровням. У нас два коммутатора уровня распределения, которые связаны с двумя коммутаторами уровня ядра избыточными каналами связи со скоростью передачи до 1 Гбит/сек, скорость передачи данных с коммутаторами уровня доступа при этом также составляет 1 Гбит/сек

3.4 Уровень доступа

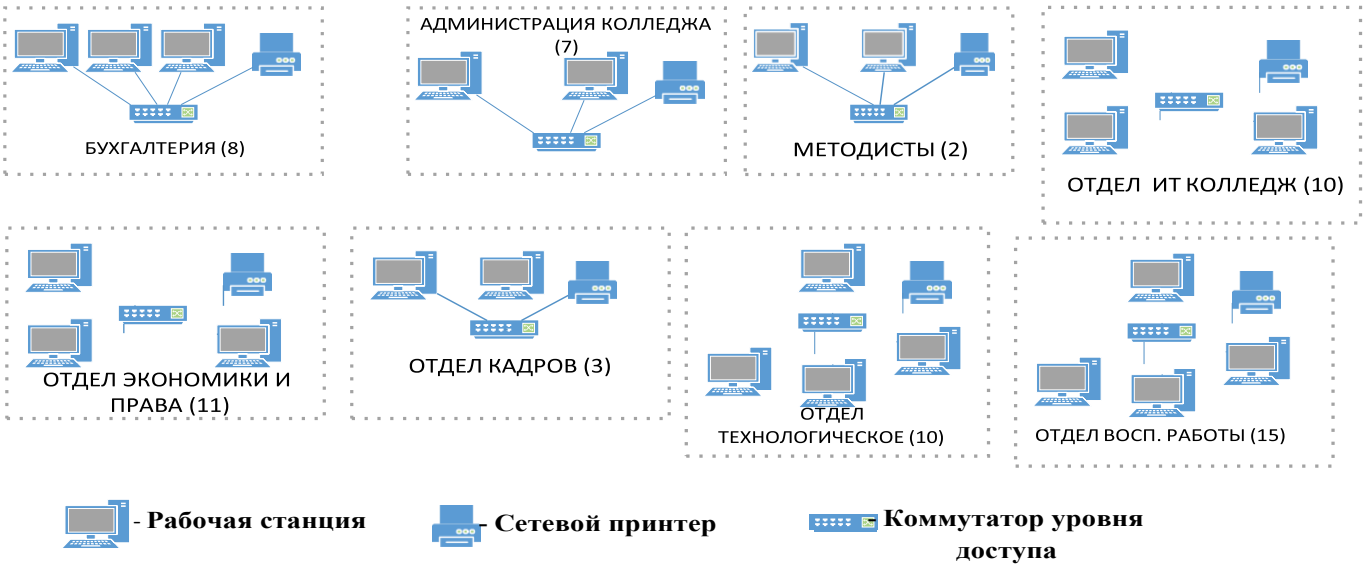


Рис. 2.4 Уровень доступа

Уровень доступа управляет доступом пользователей и рабочих групп к ресурсам объединенной сети. Основной задачей уровня доступа является создание точек входа/выхода пользователей в сеть. Уровень выполняет следующие функции:

- управление доступом пользователей и политиками сети;
- создание отдельных доменов коллизий (сегментация);
- подключение рабочих групп к уровню распределения;

- использование технологии коммутируемых локальных сетей.

На этом уровне располагаются 8 компактных коммутаторов, которые подключеныk коммутаторам уровня распределения каналами связи со скоростью до 1000 Мбит/сек. К коммутаторам уровня доступа подключены рабочие станции, скорость передачи данных100 Мбит/сек.

3.5 Подключение к сети Интернет

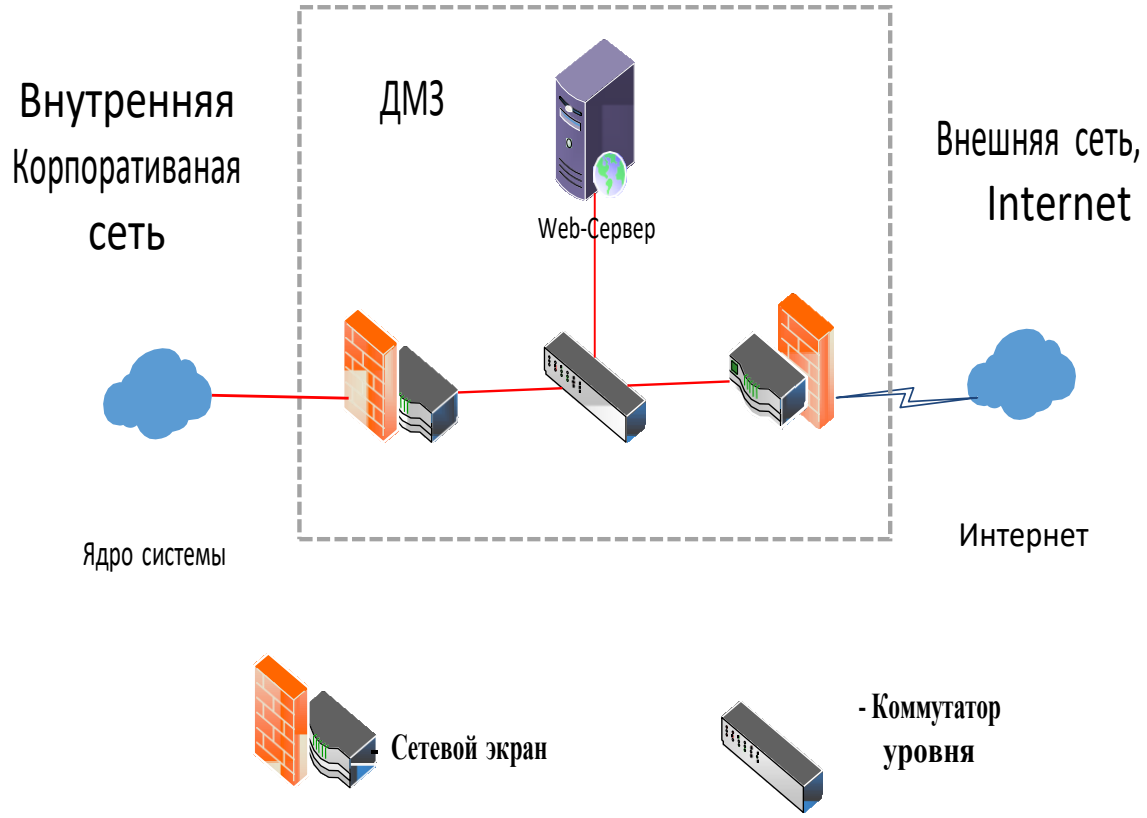


Рис. 2.5 Подключение к сети Интернет

Для связи с провайдером используется выделенная оптоволоконная линия связи. Оптоволоконная магистраль обладает такими преимуществами, как:

- высокая скорость передачи данных.
- высокая помехозащищенность.
- отсутствие методов снятия конфиденциальной информации с оптоволокна.
- высокая надежность.

3.6 Обеспечение безопасности сети. Демилитаризованная зона

Рис. 2.6 Демилитаризованная зона

-

Администрация колледжа должна определить политику информационной безопасности, которая включает ответы на следующие вопросы:

- какую информацию и от кого следует защищать;
- кому и какая информация требуется для выполнения служебных обязанностей;
- какая степень защиты требуется для каждого вида информации;
- чем грозит потеря того или иного вида информации;
- как организовать работу по защите информации.

К организационным (или процедурным) мерам обеспечения безопасности относятся конкретные правила работы сотрудников колледжа, например, строго определенный порядок работы с конфиденциальной информацией на компьютере.К средствам обеспечения информационной безопасности могут быть отнесены:

- системы контроля доступа, включающие средства аутентификации и авторизациипользователей;
- системы шифрования информации;
- системы цифровой подписи, используемые для аутентификации документов;
- средства доказательства целостности документов (использующие, например, дайджест-функции);

- системы антивирусной защиты;

Все указанные выше средства обеспечения безопасности могут быть реализованы в виде встроенных функций операционных систем, системных приложений, компьютерови сетевых коммуникационных устройств.

Под безопасностью электронной системы понимается ее свойство, выражающееся в способности противодействовать попыткам нанесения ущерба владельцам и пользователям системы при различных возмущающих (умышленных и неумышленных) воздействиях на нее.

Внешняя безопасность включает защиту от стихийных бедствий, от проникновения злоумышленника извне с целями хищения, получения доступа к носителям информации или вывода системы из строя.

Со стороны проектировщика сети важными являются следующие требования:

1) Разграничение доступа пользователей к различным ресурсам сети.

Для этого необходимо строить сегментированные сети с использованием управляемых коммутаторов и маршрутизаторов, для которых можно устанавливать права доступа того или иного пользователя к конкретной подсети.

2) Обеспечение безопасного доступа к общедоступным глобальным сетям, в частности к сети Интернет.

Необходимым является скрытие внутренней структуры сети при помощи маршрутизатора и Proxy-сервера, с межсетевым экраном, выполняющим фильтрацию проходящего через него трафика.

Межсетевой экран

Межсетевой экран или сетевой экран — комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.

Основной задачей сетевого экрана является защита компьютерных сетей или отдельных узлов от несанкционированного доступа. Также сетевые экраны часто называют фильтрами, так как их основная задача — не пропускать (фильтровать) пакеты,не подходящие под критерии, определённые в конфигурации.

Демилитаризованная зона

ДМЗ (англ. DMZ, Demilitarized Zone — демилитаризованная зона) — сегмент сети, содержащий общедоступные сервисы и отделяющий их от частных. В качестве общедоступного может выступать, например, веб-сервис: обеспечивающий его сервер, который физически размещён в локальной сети (Интранет), должен отвечать на любые запросы из внешней сети (Интернет), при этом другие локальные ресурсы (например, файловые серверы, рабочие станции) необходимо изолировать от внешнего доступа.

Цель ДМЗ — добавить дополнительный уровень безопасности в локальной сети, позволяющий минимизировать ущерб в случае атаки на один из общедоступных сервисов: внешний злоумышленник имеет прямой доступ только к оборудованию в ДМЗ.

Разделение сегментов и контроль трафика между ними, как правило, реализуются специализированными устройствами — межсетевыми экранами. Основными задачами такого устройства являются:

- контроль доступа из внешней сети в ДМЗ;
- контроль доступа из внутренней сети в ДМЗ;
- разрешение (или контроль) доступа из внутренней сети во внешнюю;
- запрет доступа из внешней сети во внутреннюю.

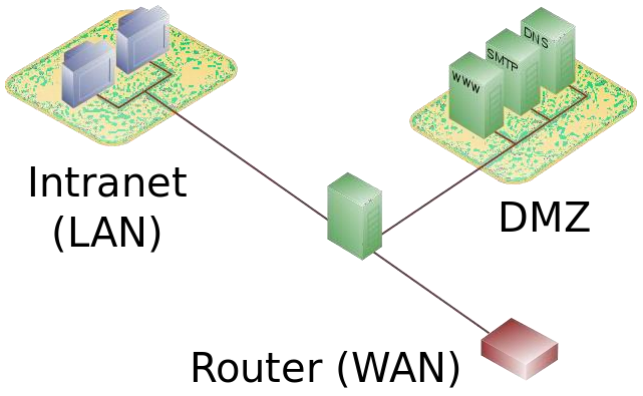


Рис. 2.7 Схема с одним межсетевым экраном

Для создания сети с ДМЗ может быть использован один межсетевой экран,

имеющий минимум три сетевых интерфейса: один — для соединения с провайдером (WAN), второй — с внутренней сетью (LAN), третий — с ДМЗ. Подобная схема проста в

реализации, однако предъявляет повышенные требования к оборудованию и администрированию: межсетевой экран должен обрабатывать весь трафик, идущий как в ДМЗ, так и во внутреннюю сеть. При этом он становится единой точкой отказа, а в случае его взлома (или ошибки в настройках) внутренняя сеть окажется уязвимой напрямую из внешней.

Вопросы безопасности сетевых ресурсов также включают защиту от вирусов, нежелательных сетевых вторжений и действий хакеров. Поэтому для защиты от внешних угроз будет использоваться комплекс антивирусных средств в нашей случае Kaspersky endpoint security.

- **Выбор оборудования**

Для проектирования VLAN в колледже я использовал следующие оборудования:

3.7.1 Коммутатор уровень ядра:

Коммутатор D-link DGS-3612

Рис. 2.8 Коммутатор D-link DGS-3612

Тип устройства - коммутатор (switch)

Стандарты и протоколы - IEEE 802.1q, IEEE 802.3af Power over Ethernet

Возможность установки в стойку - есть

Количество слотов для дополнительных интерфейсов - 4

Объем оперативной памяти - 2 Мб

Количество портов коммутатора - 8 x Ethernet 10/100/1000 Мбит/сек

Внутренняя пропускная способность - 24 Гбит/сек

Цена: 70 807 руб.

3.7.2 Коммутатор уровня доступа на 24 порта:

Коммутатор HP V1910-24G-PoE

Рис.2.9 Коммутатор HP V1910-24G-PoE

Тип устройства - коммутатор (switch)

Интерфейсы	24 порта 10/100/1000Base-TX
Поддержка PoE	Есть
Стандарты и протоколы	IEEE 802.1q 10Base-T, IEEE 802.3u 100Base-TX, IEEE 802.3af Power over Ethernet
Скорость передачи данных	• Ethernet: 10 Мбит/с (полудуплекс) / 20 Мбит/с (полный дуплекс) • Fast Ethernet: 100 Мбит/с (полудуплекс) / 200 Мбит/с (полный дуплекс) • Gigabit Ethernet: 2000 Мбит/с (полный дуплекс)

Цена: 55 250 руб.

3.7.3 Коммутатор уровня распределения на 16 портов:

Коммутатор D-link DGS-1016C

Рис. 3 Коммутатор D-link DGS-1016C

Тип устройства коммутатор - (switch)

Интерфейсы	16 портов 10/100/1000Base-T
Стандарты и протоколы	IEEE 802.1q 10Base-T, IEEE 802.3u 100Base-TX, IEEE 802.3af Power over Ethernet
Поддержка PoE	Есть
Скорость передачи данных	• Ethernet: 10 Мбит/с (полудуплекс) / 20 Мбит/с (полный дуплекс) • Fast Ethernet: 100 Мбит/с (полудуплекс) / 200 Мбит/с (полный дуплекс) • Gigabit Ethernet: 2000 Мбит/с (полный дуплекс)

Цена: 29 999 руб.

3.7.4 Рабочая станция:

Компьютер моноблок MicroXperts [M500-06] W7HB

Рис. 3.1 Моноблок MicroXperts [M500-06] W7HB

Производитель - MicroXperts

Операционная система - MS Windows 10

Pro **Чипсет материнской платы** - Intel

H81 Express**Размер LCD экрана** - 23.6"

Разрешение экрана - 1920 x 1080

Модель процессора - Intel Core i5-

4570**Частота работы процессора,**

ГГц - 3.2**Объем оперативной**

памяти - 8192 МБ**Чипсет видео** -

Intel HD Graphics

Объем жесткого диска - 1ТБ

Проводная сеть - 10/100/1000 Mbps

Цена: 49990 руб.

3.7.5 Межсетевой экран:

Межсетевой экран Ideco UTM 10/100/1000WAN, 5 10/100/1000LAN, DMZ10/100/1000Mpbs, DFL-260E/A1N

Сервер MicroXperts [ZX24-03]

Рис.3.2 Сервер MicroXperts [ZX24-03]

Характеристики:

- **Семейство процессора** - Intel® Xeon® E3
- **Количество процессоров** - Однопроцессорный
- **Чипсет** - Intel® C222 Chipset
- **Объем установленной оперативной памяти** - 16 Гб
- **Максимальный объем оперативной памяти** - 32 Гб
- **Ёмкость корзины для жестких дисков** - 4 жестких диска 3.5" fixed, интерфейс SATA
- **Сеть** - 2 x Gigabit Ethernet (RJ45)
- **Блок питания** - 300Вт
- **Процессор -** Intel Xeon E3-1220V3
- **Количество ядер** - 4
- **Материнская плата** - ASUS P9D-X/MR

Цена: 78 870 руб.

3.7.6 Принтер:

Kyocera FS-106

Устройство - принтер

Максимальный формат

- А4**Объем памяти -** 32

Мб

Процессор - ARM

Частота процессора - 390 МГц

Интерфейсы - Ethernet (RJ-45), USB 2.0

Поддержка - ОС Windows, Mac OS

Рис.3.3 Kyocera FS-106

Цена: 3600 руб.

3.7.7 Маршрутизатор:

Маршрутизатор Cisco 2911R-

V/K9Характеристики:

- 3 портов Ethernet 1 Гбит/с
- установка в стойку
- USB-порт
- IEEE 802.1q (VLAN), IEEE 802.1p (Priority tags)
- 256 МБ встроенная память, 512 МБ RAM
- размеры 438 x 89 x 305 мм, вес 9.5 кг

Цена: 136 099 ₽ руб.

Рис.3.4 Сервер Маршрутизатор Cisco 2911R-V/K9

3.8.0. Расчет стоимости

Название оборудования	Фирма	Кол-во	Цена, руб.	Итого, руб.
Коммутаторы				
DGS-3612	D-Link	2	70 807	141 614
V1910-24G-PoE	HP	1	55 250	55 250
DGS-1016C	D-Link	2	29 999	59998
2911R-V/K9	Cisco	1	136 099	136 099
Серверное оборудование				
MicroXperts [ZX24-03]	MicroXperts	1	78 870	78870
Сетевое оборудование и комплектующие				
Ideco UTM	Ideco	200	249 560	249 560
Оргтехника				
[M500-06]W7HB	MicroXperts	66	39790	2 626 140
Kyocera FS-106	Samsung	10	3600	36000
				3 383 531 руб.

Глава 4. Разработка структуры VLAN с стандартом 802.1Q

Чтобы сформировать VLAN-сеть в соответствии со стандартом IEEE 802.1Q, необходимо проделать следующие действия:

1. Задать имя виртуальной сети (например, VLAN#1) и определить ее идентификатор (VID).
2. Выбрать порты, которые будут относиться к данной виртуальной сети.
3. Задать правила входных портов виртуальной сети (возможность работы с кадрами всех типов, только с кадрами Untagged или только с кадрами Tagged).
4. Установить одинаковые идентификаторы PVID портов, входящих в виртуальную сеть.
5. Задать для каждого порта виртуальной сети правила выходного порта, сконфигурировав их как Tagged Port или Untagged Port.

В этой главе описываются обязательные и дополнительные задачи для настройки маршрутизации между VLAN с инкапсуляцией IEEE 802.1Q. Для полного описания команд в этой главе, относятся к *Cisco IOS*. Протокол IEEE 802.1Q используется для соединения нескольких коммутаторов и маршрутизаторов, а также для определения топологий VLAN. Стандарт IEEE 802.1Q чрезвычайно ограничивает немаркированные кадры. Стандарт предоставляет только решение для виртуальных локальных сетей для каждого порта для немаркированных кадров. Например, при назначении не тегированных кадров сетям VLAN учитывается только порт, с которого они были получены. У каждого порта есть параметр, называемый *постоянной виртуальной идентификацией* (Native VLAN), который указывает VLAN, назначенную для приема не тегированных кадров.

Основные характеристики IEEE 802.1Q следующие:

- Назначает кадры сетям VLAN путем фильтрации.
- Стандарт предполагает наличие одного связующего дерева и явной схемы тегирования с одноуровневым тегированием.

4.1 Список задач настройки VLAN инкапсуляции IEEE 802.1Q

Вы можете настроить маршрутизацию между любым количеством VLAN в вашей сети. В этом разделе описаны задачи настройки для каждого протокола, поддерживаемого инкапсуляцией IEEE 802.1Q. Основной процесс один и тот же, независимо от маршрутизируемого протокола. Он включает в себя следующие задачи:

- Включение протокола на роутере
- Включение протокола на интерфейсе
- Определение формата инкапсуляции как IEEE 802.1Q
- Настройка протокола в соответствии с требованиями вашей среды.

Чтобы настроить IEEE 802.1Q в нашей сети, надо выполнить задачи, описанные в следующих разделах.

- Настройка маршрутизации AppleTalk через IEEE 802.1Q
- Настройка IP-маршрутизации через IEEE 802.1Q
- Настройка маршрутизации IPX через IEEE 802.1Q

Надо выполнить задачи из следующих разделов, чтобы подключить сеть хостов через простое устройство мостового доступа к мосту концентратора удаленного доступа между виртуальными локальными сетями IEEE 802.1Q. Следующие разделы содержат задачи настройки для интегрированной маршрутизации и моста, прозрачного моста и PVST + между виртуальными локальными сетями с функцией инкапсуляции IEEE 802.1Q:

- Настройка VLAN для группы мостов с VLAN1 по умолчанию
- Настройка VLAN для группы мостов в качестве собственной VLAN

- Мониторинг и обслуживание субинтерфейсов VLAN

4.2 Настройка маршрутизации AppleTalk через IEEE 802.1Q

AppleTalk может маршрутизироваться через субинтерфейсы виртуальной LAN (VLAN) с использованием протокола инкапсуляции VLAN IEEE 802.1Q. AppleTalk Routing обеспечивает полнофункциональную поддержку AppleTalk программного обеспечения Cisco IOS для каждой виртуальной локальной сети, что позволяет настраивать стандартные возможности AppleTalk в виртуальных локальных сетях. Для маршрутизации AppleTalk через IEEE 802.1Q между виртуальными локальными сетями необходимо настроить подинтерфейс для создания среды, в которой он будет использоваться. Надо выполнить эти задачи в том порядке, в котором онипоявляются:

- Включение маршрутизации AppleTalk
- Настройка AppleTalk на субинтерфейсе
- Определение формата инкапсуляции VLAN

Включение маршрутизации AppleTalk

Чтобы включить маршрутизацию AppleTalk на интерфейсах IEEE 802.1Q, надо использовать следующую команду в режиме глобальной конфигурации:

Команда	**Цель**
Router(config)# **appletalk routing** [**eigrp** *router-number*]	Включает глобальную маршрутизацию AppleTalk

Настройка AppleTalk на субинтерфейсе

После включение AppleTalk глобально и определение формат инкапсуляции, необходимо включить его на субинтерфейсе, указав диапазон кабеля и назвав зону AppleTalk для каждого интерфейса. Чтобы включить протокол AppleTalk

на подинтерфейсе, используйте следующие команды в режиме настройки интерфейса:

	Команда	**Цель**
Шаг 1	Router(config-if)# **appletalk cable-range** *cable-range* [*network.node*]	Назначает диапазон и зону кабеля AppleTalk для субинтерфейса.
Шаг 2	Router(config-if)# **appletalk zone** *zone-name*	Назначает зону AppleTalk для подинтерфейса.

Определение формата инкапсуляции VLAN

Чтобы определить формат инкапсуляции VLAN как IEEE 802.1Q, используйте следующие команды в режиме настройки интерфейса:

	Команда	**Цель**
Шаг 1	Router(config-if)# **interface fastethernet** *slot/port subinterface-number*	Определяет субинтерфейс, который будет использовать VLAN.
Шаг 2	Router(config-if)# **encapsulation dot1q** *vlan-identifier*	Определяет формат инкапсуляции как IEEE 802.1Q(**dot1q**) и указывает идентификатор VLAN.

4.3 Настройка IP-маршрутизации через IEEE 802.1Q

IP-маршрутизация по IEEE 802.1Q расширяет возможности IP-маршрутизации, включая поддержку маршрутизации типов IP-кадров в конфигурациях VLAN с использованием инкапсуляции IEEE 802.1Q.

Для маршрутизации IP через IEEE 802.1Q между виртуальными локальными сетями необходимо настроить подинтерфейс для создания среды,

в которой он будет использоваться. Надо Выполнить задачи, описанные в следующих разделах, в порядке их появления:

- Включение IP-маршрутизации
- Определение формата инкапсуляции VLAN
- Назначение IP-адреса сетевому интерфейсу

Включение IP-маршрутизации

IP-маршрутизация автоматически включается в программном обеспечении Cisco IOS для маршрутизаторов. Чтобы повторно включить IP-маршрутизацию,если она была отключена, надо использовать следующую команду в режиме глобальной конфигурации:

Команда	**Цель**
Router(config)# **ip routing**	Включает IP-маршрутизацию на маршрутизаторе.

После включения IP-маршрутизации на маршрутизаторе можно настроить характеристики в соответствии с вашей средой.

Определение формата инкапсуляции VLAN

Чтобы определить формат инкапсуляции как IEEE 802.1Q, используйте следующие команды в режиме настройки интерфейса:

	Команда	**Цель**
Шаг 1	Router(config if)# **interface fastethernet** *slot/port.subinterface-number*	Задает подинтерфейс, на котором будетиспользоваться IEEE 802.1Q.
Шаг 2	Router(config-if)# **encapsulation dot1q** *vlanid*	Определяет формат инкапсуляции как IEEE 802.1Q (**dot1q**) и указывает

Назначение IP-адреса сетевому интерфейсу

Интерфейс может иметь один основной IP-адрес. Чтобы назначить первичный IP-адрес и сетевую маску сетевому интерфейсу, нужно использовать следующую команду в режиме настройки интерфейса:

Команда	**Цель**
Router(config-if)# **ip address** *ip-address mask*	Устанавливает основной IP-адрес для интерфейса

Маска определяет биты, которые обозначают номер сети в IP-адресе. Когда вы используете маску для подсети сети, маска тогда называется *маской подсети*.

4.3 Настройка маршрутизации IPX через IEEE 802.1Q

Маршрутизация IPX по сетям VLAN IEEE 802.1Q расширяет возможности маршрутизации Novell NetWare, включая поддержку маршрутизации типов кадров инкапсуляции Novell Ethernet_802.3 в конфигурациях VLAN. Пользователи сред Novell NetWare могут конфигурировать кадры инкапсуляции Novell Ethernet_802.3 для маршрутизации с использованием инкапсуляции IEEE 802.1Q через границы VLAN. Чтобы настроить программное обеспечение Cisco IOS на маршрутизаторе с подключенными VLAN для обмена инкапсулированными кадрами IPX Novell Ethernet_802.3, надо выполнить задачи, описанные в следующих разделах, в том порядке, в котором они появляются:

- Включение маршрутизации NetWare
- Определение формата инкапсуляции VLAN
- Настройка NetWare на субинтерфейсе

Включение маршрутизации NetWare

Чтобы включить маршрутизацию IPX на интерфейсах IEEE 802.1Q, используйте следующую команду в режиме глобальной конфигурации:

Команда	**Цель**
Router(config)# **ipx routing** [*node*]	Включает глобальную маршрутизацию IPX.

Определение формата инкапсуляции VLAN

Чтобы определить формат инкапсуляции как IEEE 802.1Q, используйте следующие команды в режиме настройки интерфейса:

	Команда	**Цель**
Шаг 1	**Router(config-if)#** interface fastethernet ***slot/port.subinterface-number***	Задает подинтерфейс, на котором будет использоваться IEEE 802.1Q.
Шаг 2	**Router(config-if)#** encapsulation dot1q ***vlan-identifier***	Определяет формат инкапсуляции как IEEE 802.1Q и указывает идентификатор VLAN.

Мониторинг и обслуживание субинтерфейсов VLAN

Чтобы указать, является ли VLAN собственной VLAN, используйте следующую команду в привилегированном режиме EXEC:

Команда	**Цель**
Router# **show vlans**	Отображает субинтерфейсы VLAN.

4.4 структуру компьютерной сети в колледже

Тверской колледж им. Коняева состоит из восьми отделов: отдел кадров 3 компьютеры, администрация колледжа 7 компьютеров, методисты 2

компьютеры, отдел ит. колледж 10 компьютеров, отдел экономики и права 11 компьютеров, отдел технологическое 10 компьютеров, отдел воспитательные работы 15 компьютеров, бухгалтерия 8 компьютеров. Все отделов находиться на четырёх этажи здание. Ниже показан структура сети в колледже.

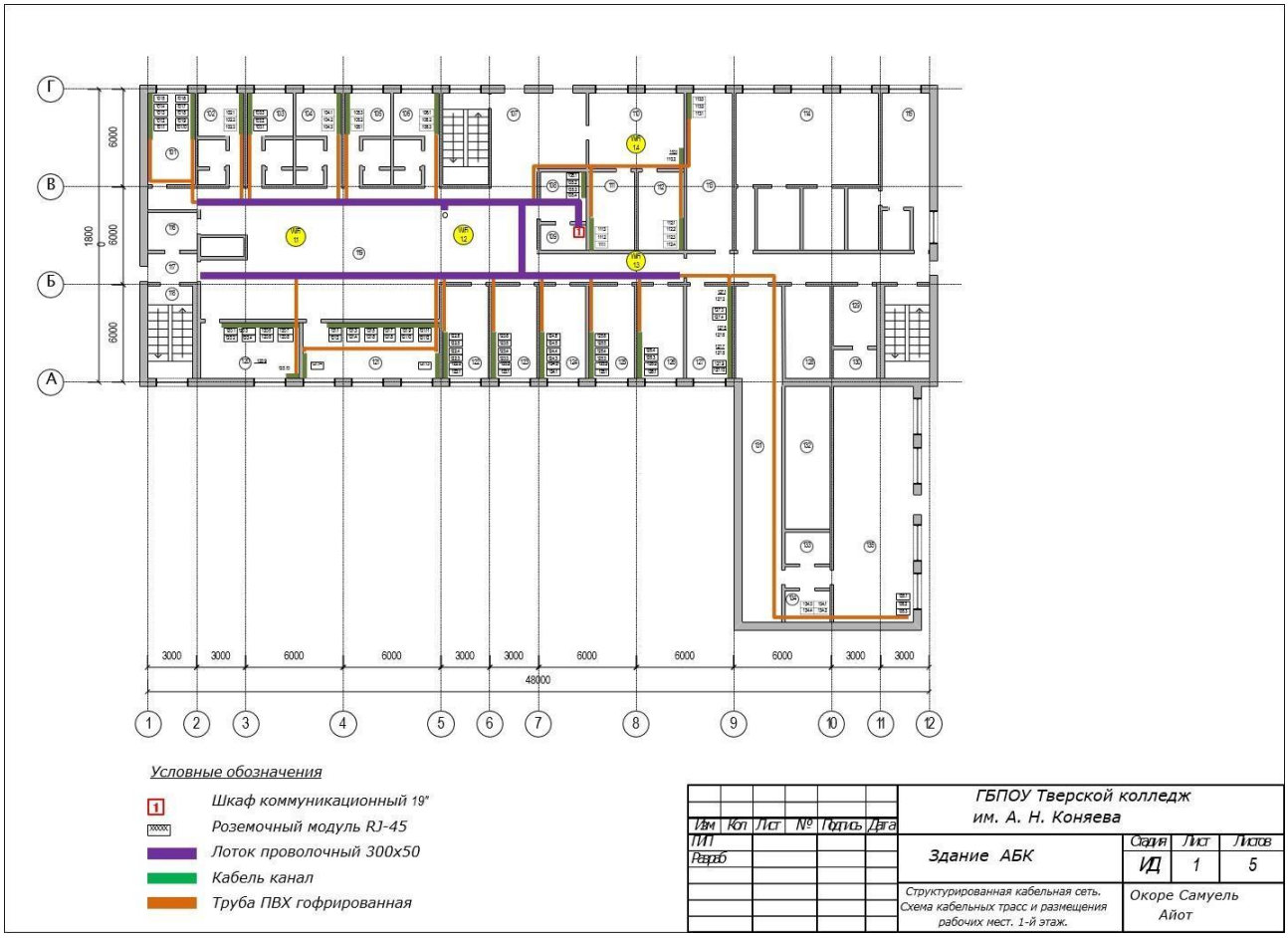


Рис. 3.5 первый этаж структура сети в колледже

На первом этаже находится администрация колледжа кабинет номер 121, отдел кадров кабинет номер 106, отдел экономики и права кабинет номер 102. Шкаф коммуникационный 19 для монтажа телекоммуникационного оборудования находится в 109 кабинет. На этом этаже установлен четыре точка доступа Wi-Fi. Так же на этом этаже настроен розеточный модуль RJ-45 предназначен для установки на симметричные кабели структурированная кабельная система (СКС) и образует интерфейс отдельных подсистем кабельной системы. В случае использования в составе стационарной линии консолидационной точки на розеточный модуль возлагаются функции внутреннего интерфейса. Лоток проволочный 300х50 для прокладки кабеля

преимущественно внутри помещений. Кабель канал для скрытой или открытой укладки проводов и кабелей. Могут использоваться как на улице, так и внутри помещений. Труба ПБХ гофрированная для защиты кабелей.

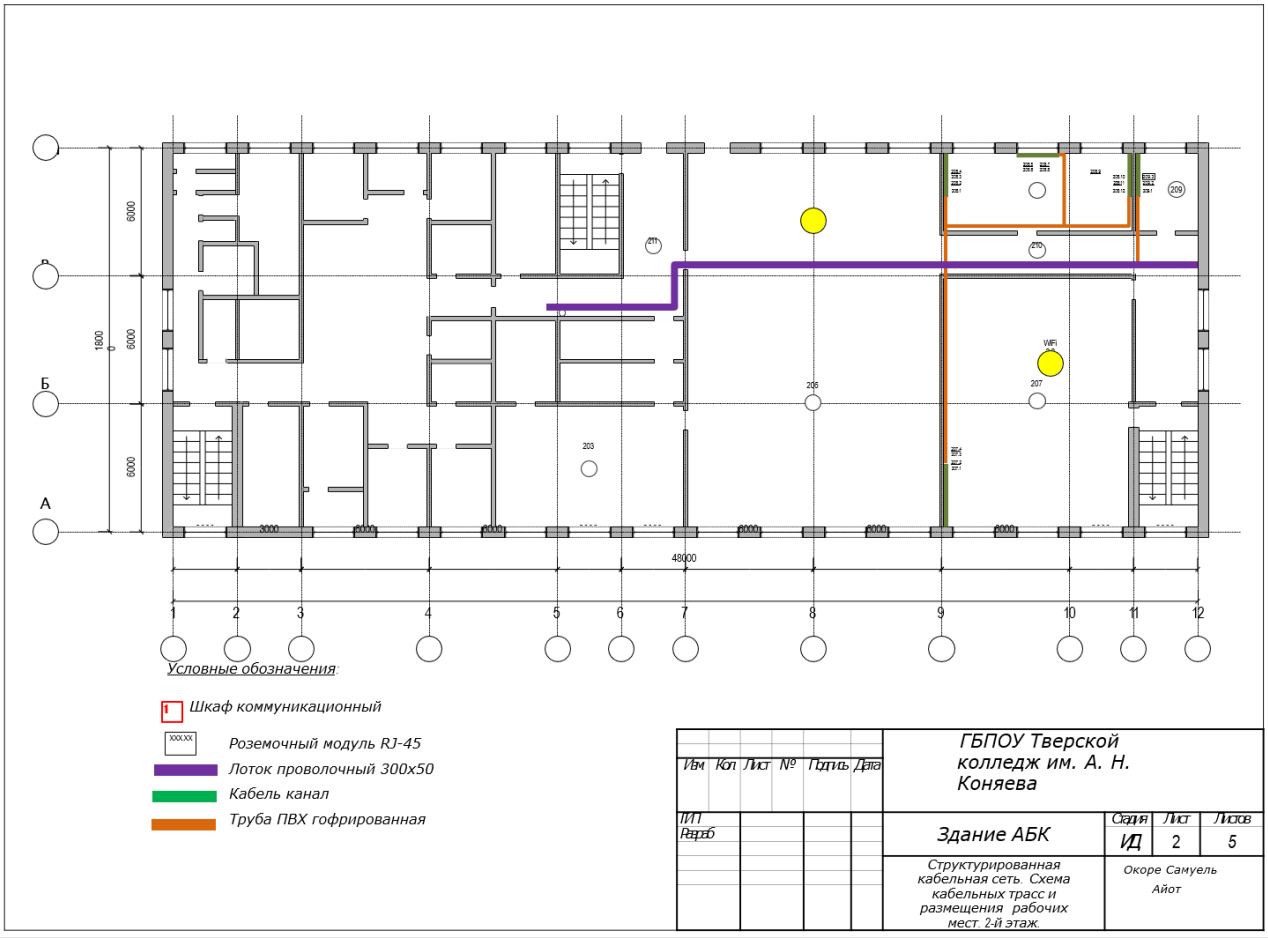


Рис. 3.6 второй этаж структура сети в колледже

На втором этаже находится методисты кабинет номер 206, отдел воспитательные работы кабинет номер 207, отдел бухгалтерия кабинет номер 209. На этом этаже установлен две точка доступа Wi-Fi. Так же на этом этаже настроен розеточный модуль RJ-45 предназначен для установки на симметричные кабели структурированная кабельная система (СКС) и образует интерфейс отдельных подсистем кабельной системы. В случае использования в составе стационарной линии консолидационной точки на розеточный модуль возлагаются функции внутреннего интерфейса. Лоток проволочный 300х50 для прокладки кабеля преимущественно внутри помещений. Кабель канал для скрытой или открытой укладки проводов и кабелей. Могут использоваться как

на улице, так и внутри помещений. Труба ПБХ гофрированная для защиты кабелей.

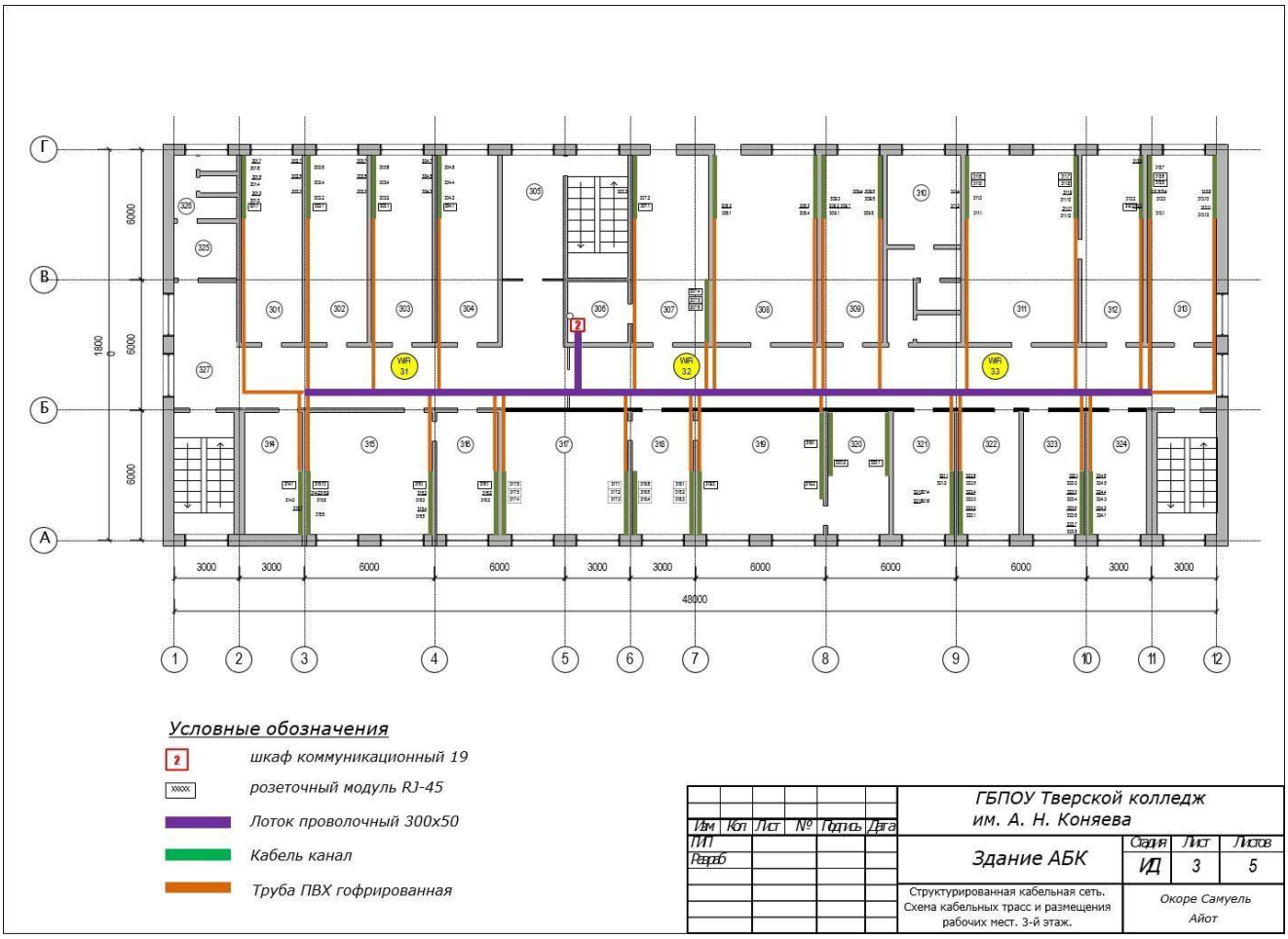


Рис. 3.7 третий этаж структура сети в колледже

На третьем этаже находится отдел ит. колледж кабинет номер 306 и отдел технологическое кабинет номер 310. Шкаф коммуникационный 19 для монтажа телекоммуникационного оборудования находится в 306 кабинет. На этом этаже установлен три точка доступа Wi-Fi. Так же на этом этаже настроен розеточный модуль RJ-45 предназначен для установки на симметричные кабели структурированная кабельная система (СКС) и образует интерфейс отдельных подсистем кабельной системы. В случае использования в составе стационарной линии консолидационной точки на розеточный модуль возлагаются функции внутреннего интерфейса. Лоток проволочный 300х50 для прокладки кабеля преимущественно внутри помещений.

на улице, так и внутри помещений. Труба ПБХ гофрированная для защиты кабелей.

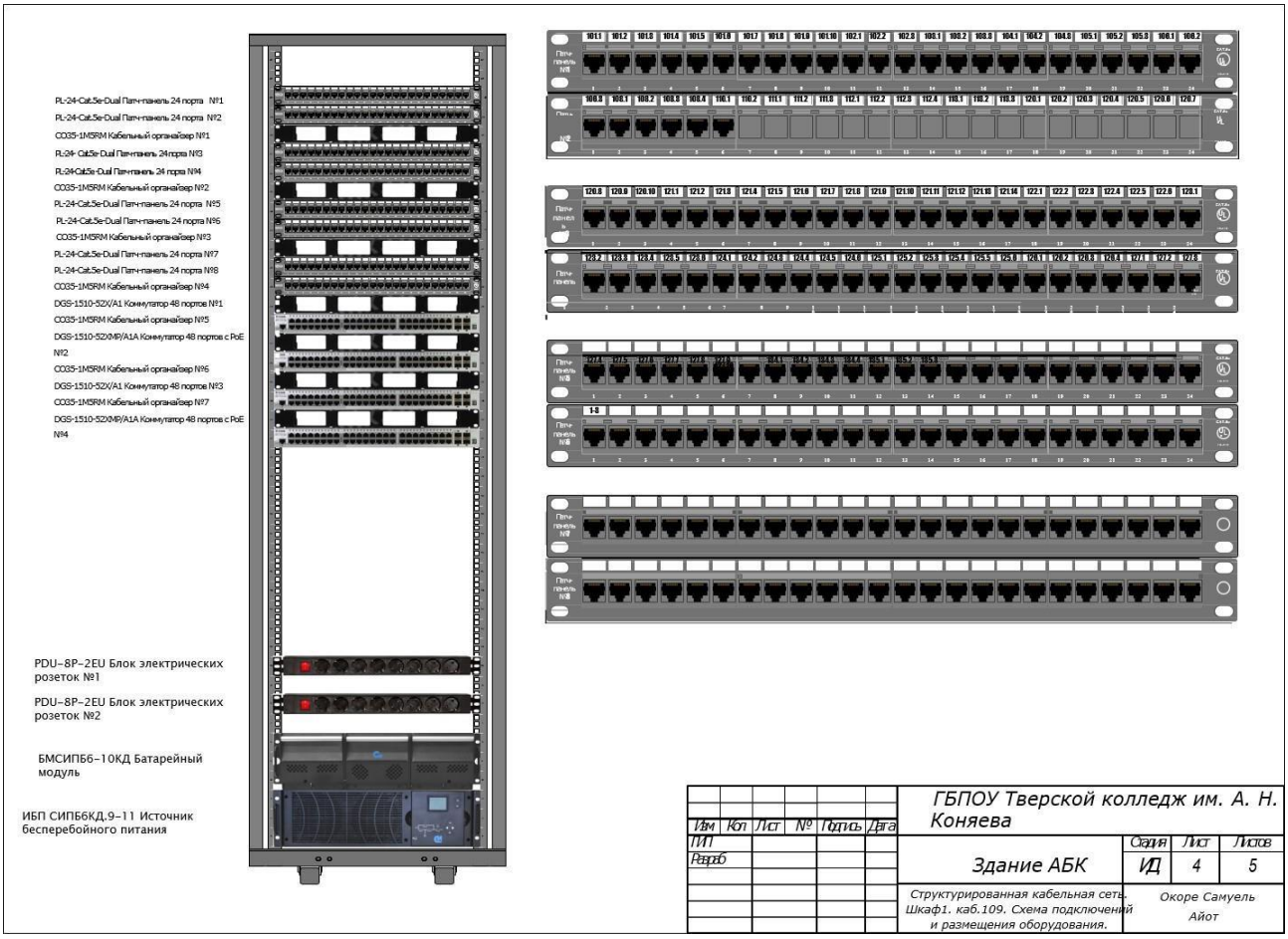


Рис.3.8 Структурированная кабельная сеть. Шкаф1. каб.109.

Структурированная кабельная сеть. Шкаф1. каб.109. Схема подключений и размещения оборудования. На нем установлен 4 коммутаторы, три серверы supermicro; сервер 1с с операционной системой windows сервер 2012 R2, веб сервер с операционной системой windows сервер 2016, прокси сервер с операционной системой windows сервер 2012 R2. Так же на нем установлен PDU-8P-2EU Блок электрических розеток, БМСИПБ6-10КД Батарейный модуль и ИБП СИПБ6КД.9-11 Источник бесперебойного питания.

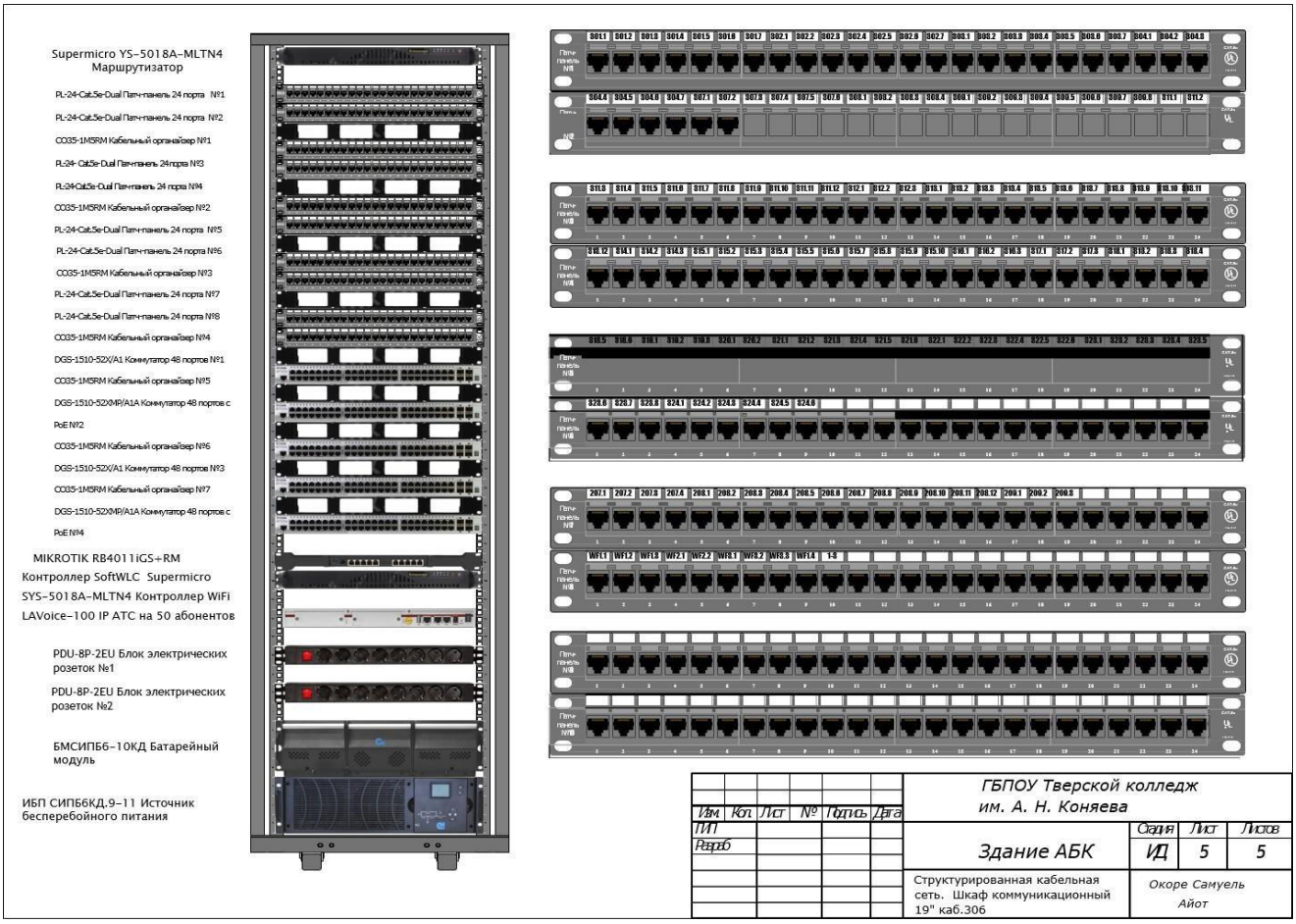


Рис. 3.9 Структурированная кабельная сеть. Шкаф 2. каб.306

Структурированная кабельная сеть. Шкаф коммуникационный 19 каб.306. Схема подключений и размещения оборудования. На нем установлен 6 коммутаторов, четыре серверы supermicro; сервер VDI с операционной системой windows сервер 2019, две серверы домен контролер сервер с операционной системой windows сервер 2019, файловый сервер с операционной системой windows сервер 2012 R2. Так же на нем установлен PDU-8P-2EU Блок электрических розеток, БМСИПБ6-10КД Батарейный модуль и ИБП СИПБ6КД.9-11 Источник бесперебойного питания, SYS-5018A- MLTN4 Контроллер WiFi для управление точка доступа, LAVoice-100 IP ATC на 50 абонентов для управление IP- телефонов.

Глава 5. Конфигураций VLAN в колледже Коняева

Важным свойством коммутатора локальной сети является способность контролировать передачу кадров между сегментами сети. По различным причинам (соблюдение прав доступа, политика безопасности и т. д.) некоторые кадры не следует передавать по адресу назначения.

Иногда нам может потребоваться разделить локальную сеть на несколько отдельных сегментов. Например, в колледже несколько отделов: Отдел кадров, Бухгалтерия, Высшее руководство, Технический отдел каждый, который находится на целый этаже здание. Каждый отдел может иметь серверы, доступ к которым нужно ограничить сотрудникам из других отделов.С одной стороны, теоретически это легко реализовать. Ведь можно создать отдельную сетевую инфраструктуру для каждой сети.

Но, с другой стороны, проблема в том, что довольно сложно планировать такую сеть. Кроме того, может потребоваться изменить и саму конфигурацию сети. Поэтому гораздо проще создать общую физическую сетьс последующим логическим сегментированием определенных частей сети. Данный подход позволяет гораздо гибче планировать и управлять сетью, а также повышает безопасность сети.

Сегментированные сети и называются виртуальными локальными сетями (VLAN- Virtual LAN) **Виртуальной локальной сетью** (Virtual Local Area Network, VLAN) называется группа узлов сети, трафик которой, в том числе широковещательный, на канальном уровне полностью изолирован от трафика других узлов сети. Это означает, что передача кадров между разными виртуальными сетями на основании адреса канального уровня невозможна независимо от типа адреса (уникального, группового или широковещательного). В то же время внутри виртуальной сети кадры передаются по технологии коммутации, то есть только на тот порт, который связан с адресом назначения кадра.

Рис. 4 Виртуальной локальной сетью (Virtual Local Area Network, VLAN)

Порты (интерфейсы) на коммутаторах могут быть назначены одной или нескольким VLAN, что позволяет разделить системы на логические группы - на основе того, с каким отделом они связаны - и установить правила о том, как системы в отдельных группах могут взаимодействовать друг с другом.

Каждая VLAN обеспечивает доступ к каналу передачи данных для всех хостов, подключенных к портам коммутатора, настроенным с тем же идентификатором VLAN. Тег VLAN - это 12-битное поле в заголовке Ethernet, которое обеспечивает поддержку до 4096 VLAN на домен коммутации. Маркировка VLAN стандартизирована в стандарте IEEE 802.1 Q и часто называется Dot1Q.

5.1 Конфигурации VLAN на Cisco 2911R-V/K9 роутер

Маршрутизаторы Cisco 2911 были разработаны с учетом различных требований к гибкости устройства. Это позволило бы снизить издержки на построение IT-инфраструктуры, а также на её дальнейшее развитие. Данная серия устройств отлично подходит для малого и среднего бизнеса с различной инфраструктурой. Множество дополнительных функций позволяет развернуть сеть под конкретные нужды, а в будущем - увеличить её, не меняя оборудование. Голосовой шлюз - один из примеров широкого

функционирования маршрутизатора за счет дополнительной гибкости устройства.

IP-телефония - ещё один бонус в копилку данных устройств, поскольку также открывает широкие возможности по обустройству офиса или компании.

Интеграция сервисов как раз и рассчитана на уменьшение расходов на построение инфраструктуры, предоставляя большие возможности для функционирования определенной сети. Высокая производительность Cisco 2911 создает комфортные условия для его использования.

Рис.4.1 Cisco 2911R-V/K9 роутер

На следующих снимках экрана отображены команды, которые были введены на коммутаторе

```
ADMIN-DEPARTMENT (config)#interface fastEthernet 0/0

ADMIN-DEPARTMENT (config-if)#no shutdown

ADMIN-DEPARTMENT (config-if)#interface fastEthernet 0/0.12

ADMIN-DEPARTMENT (config-subif)#encapsulation dot1Q 12

ADMIN-DEPARTMENT (config-subif)#ip address 192.168.12.1 255.255.255.0

METHODISTS (config)#interface fastEthernet 0/0

METHODISTS (config-if)#no shutdown

METHODISTS (config-if)#interface fastEthernet 0/0.12

METHODISTS (config-subif)#encapsulation dot1Q 12

METHODISTS (config-subif)#ip address 192.168.12.2 255.255.255.0
```

ADMIN-DEPARTMENT и METHODISTS оба настроены с подинтерфейсами и используют подсеть 192.168.12.0 /24. Все их кадры помечены как VLAN 10.

В сети поставщика услуг нам придется настроить ряд элементов. Сначала я настрою магистрали 802.1Q между ADMIN-DEPARTMENT– IT- DEPARTMENT и METHODISTS – `IT-DEPARTMENT`:

```
ADMIN-DEPARTMENT (config)#interface fastEthernet 0/19

ADMIN-DEPARTMENT (config-if)#switchport trunk encapsulation dot1q

ADMIN-DEPARTMENT (config-if)#switchport mode trunk

METHODISTS (config)#interface fastEthernet 0/21

METHODISTS (config-if)#switchport trunk encapsulation dot1q

METHODISTS (config-if)#switchport mode trunk

IT-DEPARTMENT (config)#interface fastEthernet 0/19

IT-DEPARTMENT (config-if)#switchport trunk encapsulation dot1q

IT-DEPARTMENT (config-if)#switchport mode trunk

IT-DEPARTMENT (config)#interface fastEthernet 0/21

IT-DEPARTMENT (config-if)#switchport trunk encapsulation dot1q

IT-DEPARTMENT (config-if)#switchport mode trunk
```

Следующая часть — это то, где мы настраиваем фактическое туннелирование “Q-in-Q". Поставщик услуг будет использовать VLAN 40 для передачи всего от нашего клиента. Мы настроим интерфейсы к маршрутизаторам клиентов, чтобы пометить все для VLAN 20:

```
ADMIN-DEPARTMENT (config)#interface fastEthernet 0/1

ADMIN-DEPARTMENT (config-if)#switchport access vlan 40

ADMIN-DEPARTMENT (config-if)#switchport mode dot1q-tunnel
```

```
METHODISTS (config)#interface fastEthernet 0/2

METHODISTS (config-if)#switchport access vlan 40

METHODISTS (config-if)#switchport mode dot1q-tunnel
```

Команда dot1q-tunnel режима коммутатора сообщает коммутатору, чтобы пометить трафик, и требуется команда vlan доступа к коммутатору, чтобы указать VLAN Q-in-Q 40. Убедитесь, что VLAN 40 доступна на ADMIN-DEPARTMENT, METHODISTS и IT-DEPARTMENT. Назначив интерфейсы выше этой VLAN, она была автоматически создана на ADMIN-DEPARTMENT и METHODISTS, но я также должен убедиться, что IT-DEPARTMENT имеет VLAN 40 в своей базе данных:

```
IT-DEPARTMENT (config)#vlan 40
```

Теперь все на месте, давайте проведем быстрый тест, чтобы увидеть, смогут ли ADMIN-DEPARTMENT и METHODISTS связаться друг с другом:

```
ADMIN-DEPARTMENT #ping 192.168.12.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.12.2, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Наш пинг работает! Давайте взглянем на некоторые команды, чтобы проверить нашу работу:

```
ADMIN-DEPARTMENT #show dot1q-tunnel



dot1q-tunnel mode LAN Port(s)
```

```
-----------------------------

Fa0/1

METHODISTS #show dot1q-tunnel


dot1q-tunnel mode LAN Port(s)

-----------------------------

Fa0/2
```

Команда show dot1q-tunnel не дает мне много информации. Единственное, что мы видим, — это интерфейсы, наст роенные для туннелирования dot1q. Хороший способ доказать, что коммутаторы поставщика услуг действительно туннелируют кадры от клиента, — это посмотреть на транки между ADMIN-DEPARTMENT, METHODISTS и IT-DEPARTMENT:

```
ADMIN-DEPARTMENT #show interfaces fa0/19 trunk


Port        Mode             Encapsulation Status        Native vlan

Fa0/19      on               802.1q         trunking      1


Port        Vlans allowed on trunk

Fa0/19      1-4094


Port        Vlans allowed and active in management domain

Fa0/19      10,40


Port        Vlans in spanning tree forwarding state and not pruned

Fa0/19      10,40
```

```
METHODISTS #show interfaces trunk


Port        Mode             Encapsulation Status        Native vlan

Fa0/21      on               802.1q         trunking      1


Port        Vlans allowed on trunk

Fa0/21      1-4094


Port        Vlans allowed and active in management domain

Fa0/21      10,40


Port        Vlans in spanning tree forwarding state and not pruned

Fa0/21      10,40

IT-DEPARTMENT #show interfaces trunk


Port        Mode             Encapsulation Status        Native vlan

Fa1/0/19    on               802.1q         trunking      1

Fa1/0/21    auto             n-802.1q       trunking      1


Port        Vlans allowed on trunk

Fa1/0/19    1-4094

Fa1/0/21    1-4094


Port        Vlans allowed and active in management domain

Fa1/0/19    10,40
```

```
Fa1/0/21    10,40


Port        Vlans in spanning tree forwarding state and not pruned
Fa1/0/19    10,40
Fa1/0/21    10,40
```

Как вы можете видеть выше, единственной активной VLAN (кроме VLAN 1) на этих магистральных каналах является VLAN 40. Вы не увидите здесь VLAN 10, потому что это трафик клиентов, и он инкапсулирован в VLAN 40. Еще один хороший способ доказать это-посмотреть на связующее дерево (spanning-tree):

```
ADMIN-DEPARTMENT #show spanning-tree vlan 10


Spanning tree instance(s) for vlan 12 does not exist.
METHODISTS #show spanning-tree vlan 10


Spanning tree instance(s) for vlan 12 does not exist.
IT-DEPARTMENT #show spanning-tree vlan 12


Spanning tree instance(s) for vlan 12 does not exist.
```

Наши коммутаторы не имеют топологии связующего дерева для VLAN 10, им все равно, какую VLAN использует клиент, они заботятся только о VLAN 40.

Одна из вещей, которую Туннелирование 802.1 Q может сделать, – это туннелировать некоторые протоколы уровня 2. Взгляните ниже:

```
ADMIN-DEPARTMENT (config)interface fastEthernet 0/1
ADMIN-DEPARTMENT (config-if)#l2protocol-tunnel ?
  cdp                 Cisco Discovery Protocol
  drop-threshold      Set drop threshold for protocol packets
```

```
point-to-point      point-to-point L2 Protocol

shutdown-threshold  Set shutdown threshold for protocol packets

stp                 Spanning Tree Protocol

vtp                 Vlan Trunking Protocol

<cr>
```

5.2 Протокол VTP (VLAN Trunk Protocol)

является одним из самых известных вендорских протоколов, занимающихся задачами в корпоративных сетях. Ключевое назначение протокола VTP – это решать вопрос синхронизации базы данных с информацией о VLAN'ах между коммутаторами в кампусной сетипредприятия. Протокол VTP помогает упрощать операции с VLAN'ами в организации – добавление, удаление, изменение параметров, а также оптимизирует сетевой трафик, благодаря наличию функции vtp pruning.

VTP домен – область, состоящая из одного или нескольких коммутаторов, которые, благодаря vtp, используют одну базу vlan.

На уровне взаимодействия и ролей устройств протокол VTP достаточно прост. Все коммутаторы делятся на три вида или роли:

- **VTP Server** – те, на которых можно создавать новые VLAN'ы, удалять старые, изменять существующие – в общем те, где можно полноценно изменять всю базу VLAN'ов. Устройства с Read+Write доступом к vlan базы данных.
- **VTP Client** – те коммутаторы, которые будут получать по сети анонсы от других VTP-устройств и не будут иметь возможности локально исправлять информацию (устройства с Read-only доступом).
- **VTP transparent(прозрачный)** – коммутатор может создавать, изменять и удалять VLAN-ы. В этом режиме устройство не объявляет и не обрабатывает приходящие vtp-обновления, но при этом все приходящие обновления передаются дальше.

5.2.1 VTP Pruning

Pruning - переводится как "обрезка", это технология внутри протокола VTP направленная на ограничение широковещательного трафика в домене VTP.

режим, используемый для фильтрации фреймов. При его включении, коммутатор получая фреймы для какого-то конкретного vlan-а, будет отправлять их только на те trunk-интерфейсы, которые ведут к нужному vlan-у. На все остальные фрейм отправлятся не будет. Таким образом исключается распространения широковещательного (Broadcast), многоадресного (Multicast) и прочего неведомого трафика который в немалых количествах передаются по коммутируемой сети. Для включения VTP pruning на серверном свитче

вводится команда: *Switch(config)#vtp pruning*

Задача этой функции – каждый коммутатор будет “считать” фактически используемые VLAN’ы, и в случае, когда по VTP приходит неиспользуемый VLAN, уведомлять соседа, что этот трафик не имеет смысла присылать это увеличиваеть скорость передачи. Под этот механизм будут подпадать только первые 1000 VLAN’ов, исключая самый первый (т.е. pruning работает только для VLAN’ов с номерами от 2 до 1001).

5.2.2 Настройка режима VTP

host(config)#vtp mode *режим*

Где режим – это server, client, transparent или off. Режим off получится поставить только на устройствах, поддерживающих VTPv3; на коммутаторах, которые поддерживают только VTPv1 и VTPv2 отключить протокол нельзя.

```
IT-DEPARTMENT>en
IT-DEPARTMENT#config t
Enter configuration commands, one per line.  End with CNTL/Z.
IT-DEPARTMENT(config)#vtp mode server
Device mode already VTP SERVER.
IT-DEPARTMENT(config)#exit
IT-DEPARTMENT#
%SYS-5-CONFIG_I: Configured from console by console

IT-DEPARTMENT#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 6
VTP Operating Mode              : Server
VTP Domain Name                 : TURBO-SYSTEMS
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x6B 0x97 0x85 0xAE 0xAB 0x7A 0xF1 0xE6
Configuration last modified by 0.0.0.0 at 3-1-93 00:01:50
Local updater ID is 0.0.0.0 (no valid interface found)
IT-DEPARTMENT#
```

```
HUMAN-RESOURCE-DEPARTMENT>EN
HUMAN-RESOURCE-DEPARTMENT#CONFIG T
Enter configuration commands, one per line.  End with CNTL/Z.
HUMAN-RESOURCE-DEPARTMENT(config)#VTP MODE CLIENT
Setting device to VTP CLIENT mode.
HUMAN-RESOURCE-DEPARTMENT(config)#VTP VERSION 2
Cannot modify version in VTP client mode
HUMAN-RESOURCE-DEPARTMENT(config)#VTP DOMAIN TURBO-SYSTEMS
Changing VTP domain name from NULL to TURBO-SYSTEMS
HUMAN-RESOURCE-DEPARTMENT(config)#EXIT
HUMAN-RESOURCE-DEPARTMENT#
%SYS-5-CONFIG_I: Configured from console by console

HUMAN-RESOURCE-DEPARTMENT#SHOW VTP STATUS
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 6
VTP Operating Mode              : Client
VTP Domain Name                 : TURBO-SYSTEMS
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x5D 0xB8 0xD5 0xD9 0xF2 0xD9 0xDF 0xE6
Configuration last modified by 0.0.0.0 at 3-1-93 02:22:50
HUMAN-RESOURCE-DEPARTMENT#
```

Рис. 4.2 назначение VTP режим

5.2.3 Настройка имени домена VTP

host(config)#vtp domain *имя_домена*

Стереть имя домена штатно нельзя, только сменить. Т.е. если стартово заменили дефолтное значение, которое NULL, на своё, то всё.

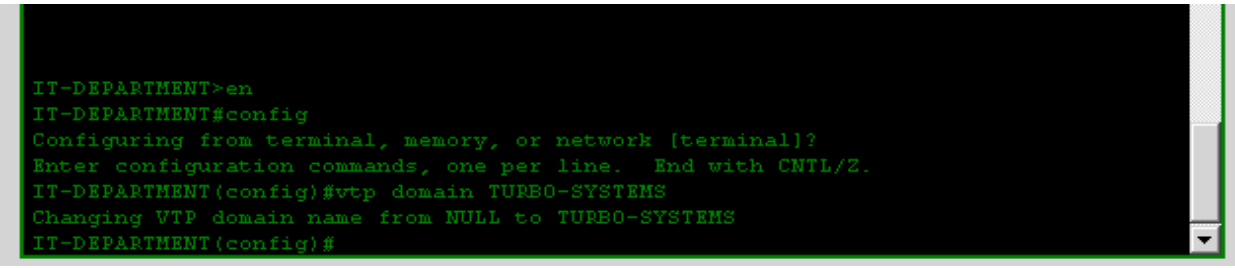


Рис. 4.3 назначение VTP домена

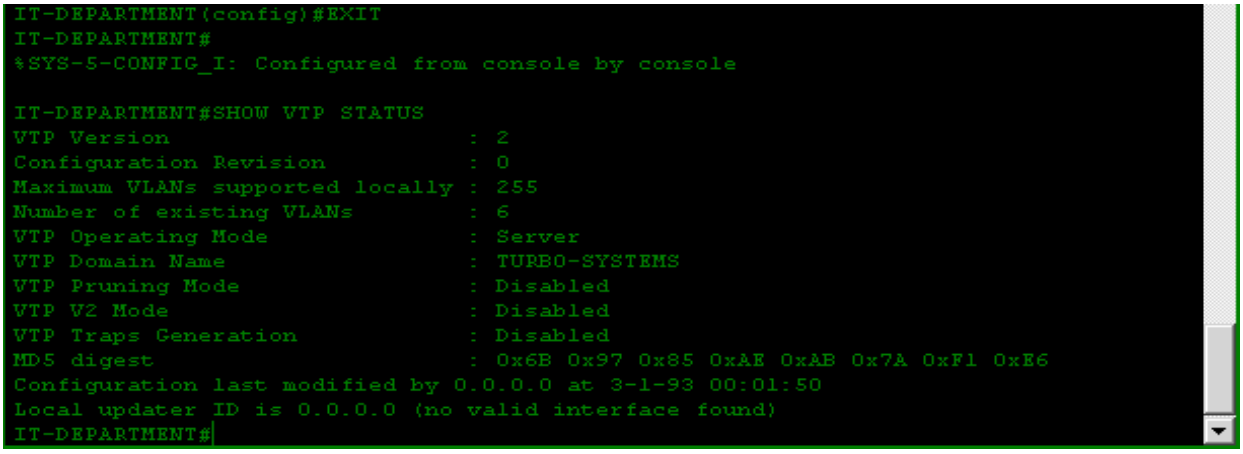


Рис. 4.4 VTP статус

5.2.4 Настройка версии VTP

host(config)#vtp version версия

На данный момент у нас есть только версия 1й до 3й.

5.2.5 Настройка пароля VTP

host(config)#vtp password пароль

При настройке пароля для VTP необходимо указать пароль на всех коммутаторах в домене VTP. На всех этих коммутаторах пароли должны совпадать. Настроенный пароль VTP преобразуется по алгоритму в 16-байтовое слово (значение MD5), которое содержится во всех пакетах сводных объявлений VTP. Это важно для безопасности сети от хакеров.

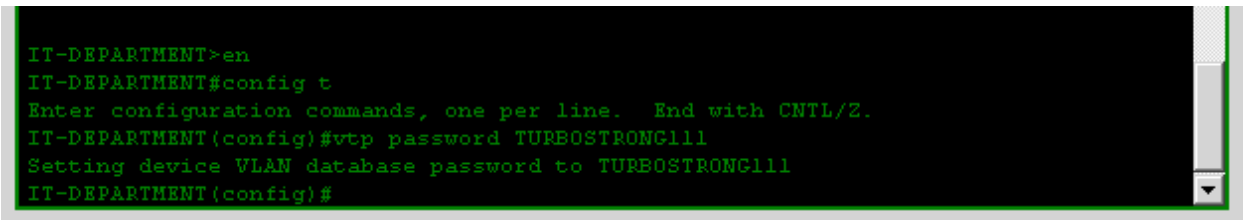


Рис. 4.5 назначение пароль

5.3 Конфигурация Vlan для Hp коммутатора

Коммутаторы HP не делают различия между портом «trunk» и портом «access». Все то же самое. Любой порт может передавать любой тегированный трафик vlan и немаркированный трафик для одного vlan. Различие заключается в том, передает ли конкретный порт тегированный или нетегированный трафик для конкретной VLAN.

Если вы хотите, чтобы порт принимал тегированный трафик на конкретном vlan, сделайте этот порт отмеченным членом этого vlan. Если вы хотите, чтобы порт принимал немаркированный трафик на конкретном vlan, сделайте этот порт нетегированным членом этого vlan. Обратите внимание, что это может быть непомеченный член только одного vlan. Итак, в ваше исходящий канал несет vlans 10,40, 6 и 1 и подключается к порту 1 коммутатора hp, вы должны использовать vlan 10

```
conf t

vlan 10

Name VLAN10_Administration

ip address 192.168.1.10 255.255.255.0

Administration

ipv6

tagged 1

untagged 2-8

qos priority 3

exit

Vlan 6

Name VLAN20_Finance

ip address 192.168.2.10 255.255.255.0

Finance
```

```
qos priority 5

tagged 1-8

exit

vlan 1

Name VLAN1_HR

qos priority 1

tagged 1-8

exit

exit

wr mem
```

Откройте программное обеспечение браузера, введите IP-адрес коммутатора и войдите в веб-интерфейс коммутатора HP Switch.

Рис. 4.6 вход через веб интерфейс

На экране приглашения введите регистрационную информацию администратора.

Информация о доступе к заводским настройкам:

• Имя пользователя: admin

• Пароль: (без пароля)

После успешного входа в систему будет отображено административное меню. Откройте меню Сеть и выберите опцию VLAN.

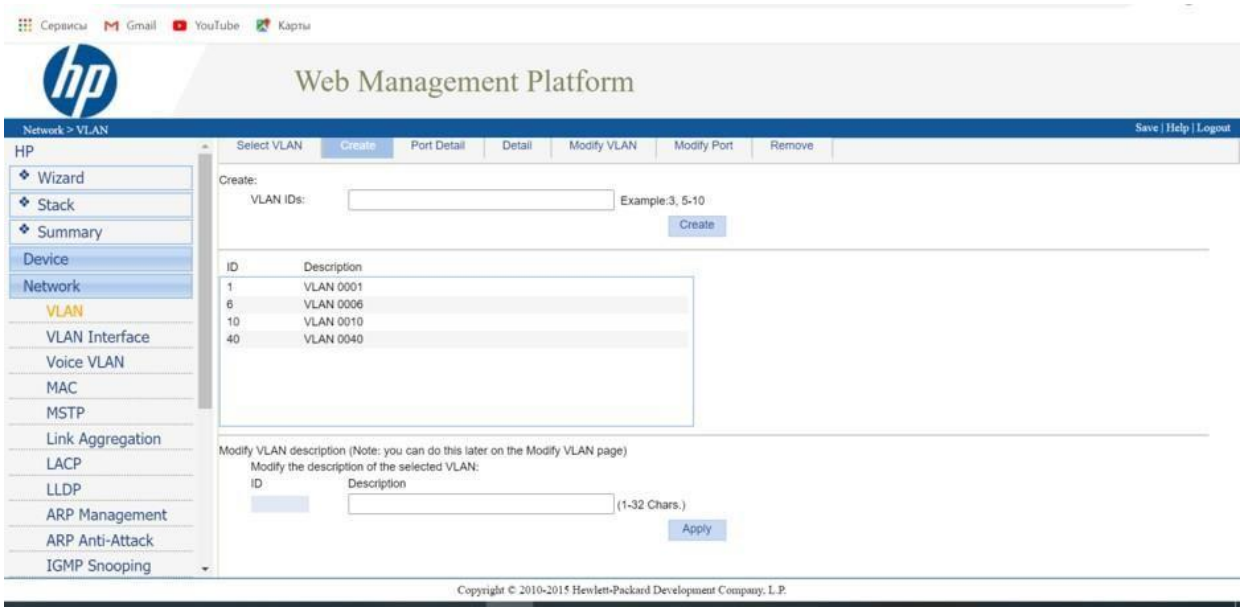


Рис. 4.7 Создание vlan в веб интерфейс

На экране VLAN выберите вкладку «Создать» в верхней части экрана. Чтобы создать новую VLAN, введите желаемый идентификационный номер и нажмите кнопку «Создать». В нашем примере были созданы следующие VLANS: 6, 40. После завершения создания Vlan вам разрешено связывать порт коммутатора с Vlan. Чтобы назначить порты vlan, я выбирал вкладку *Modify* vlan, выбираем vlan из раскрывающейся стрелки и назначаем ему порт untagged

- означает порт доступа все tagged - означает порт магистрали. Я назначил порт 1,2,6,9 в качестве untagged в vlan 10 и порт 10 в качестве tagged.

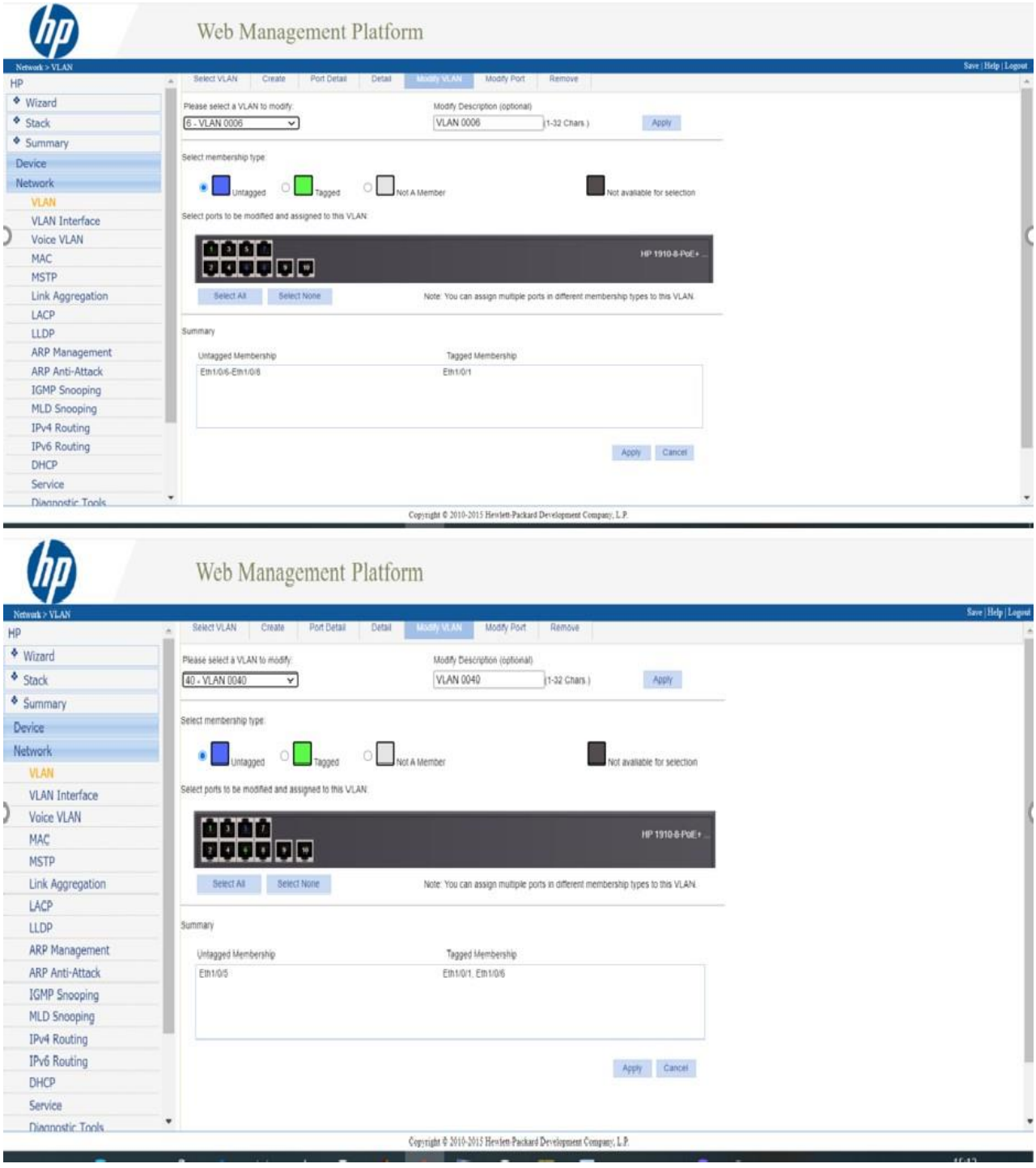


Рис. 4.8 назначение портов

Я назначил порты доступа (untagged) 6,7,8 vlan 6 и порт 1 в качестве магистрали (tagged). В vlan 40 я назначил порты доступа (untagged) 5 и 1, 6 в качестве магистральных (tagged) портов.

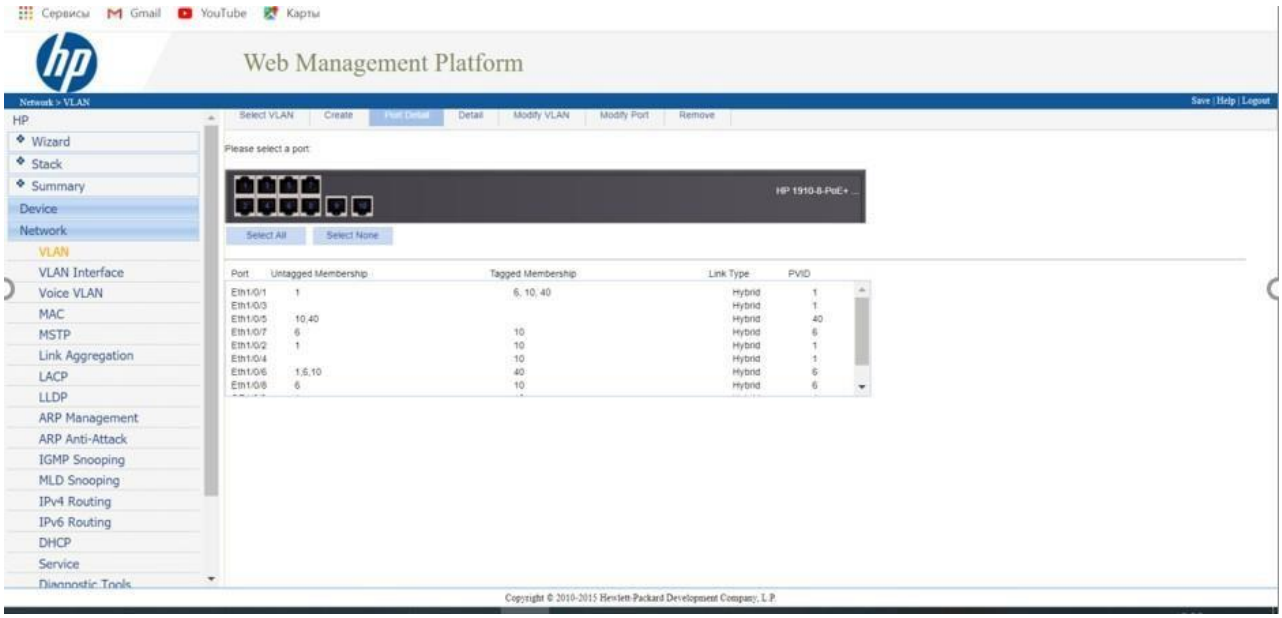


Рис. 4.9 VLAN ID-идентификатор

Я указал PVID. Порт VLAN ID-идентификатор VLAN, к которой порт открыть или немаркированный (Untagged)

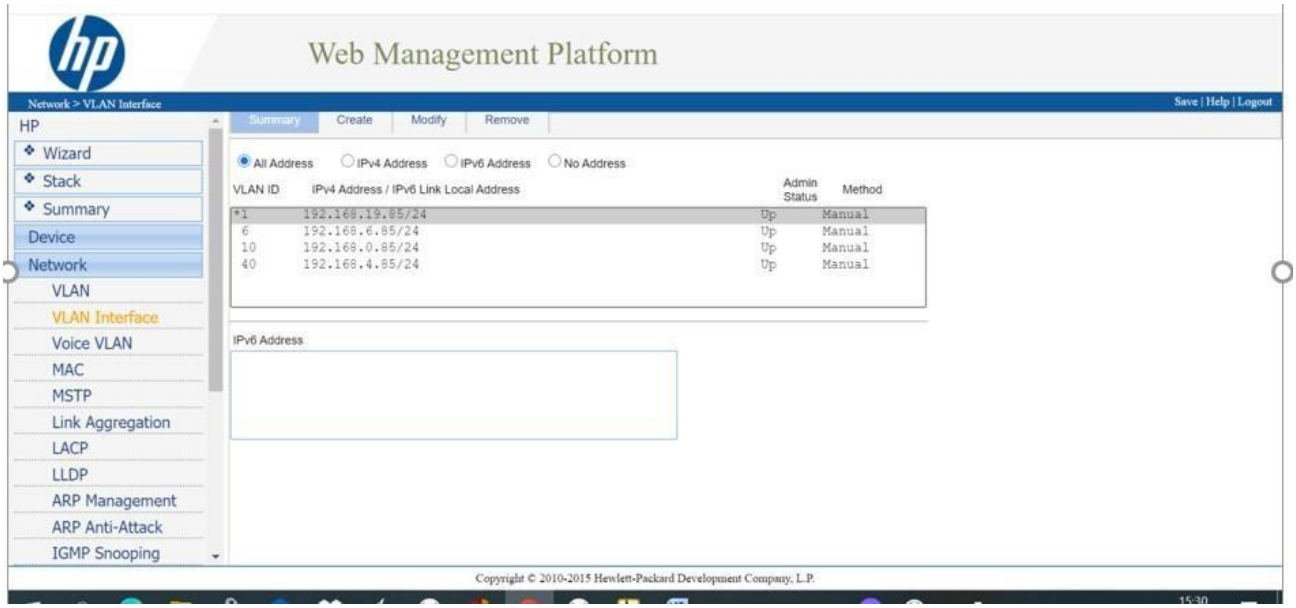


Рис. 5 назначение портов

В разделе интерфейс Vlan мы можем назначить IP-адрес vlan, изменить или удалить ip-адрес. Принцип VLAN диктует, что магистраль на одном концеVLAN должна совпадать с магистралью на другом конце VLAN в моем случаея выбрал порт 9 в качестве магистрального порта для каждой VLAN, потому что это порт, к которому мой коммутатор подключен к другому коммутатору (trunk порт).

5.4 Моделирования vlan в cisco packet tracer

По умолчанию все компьютеров подключены к VLAN 1 вот что поддерживает связью без ограничения.

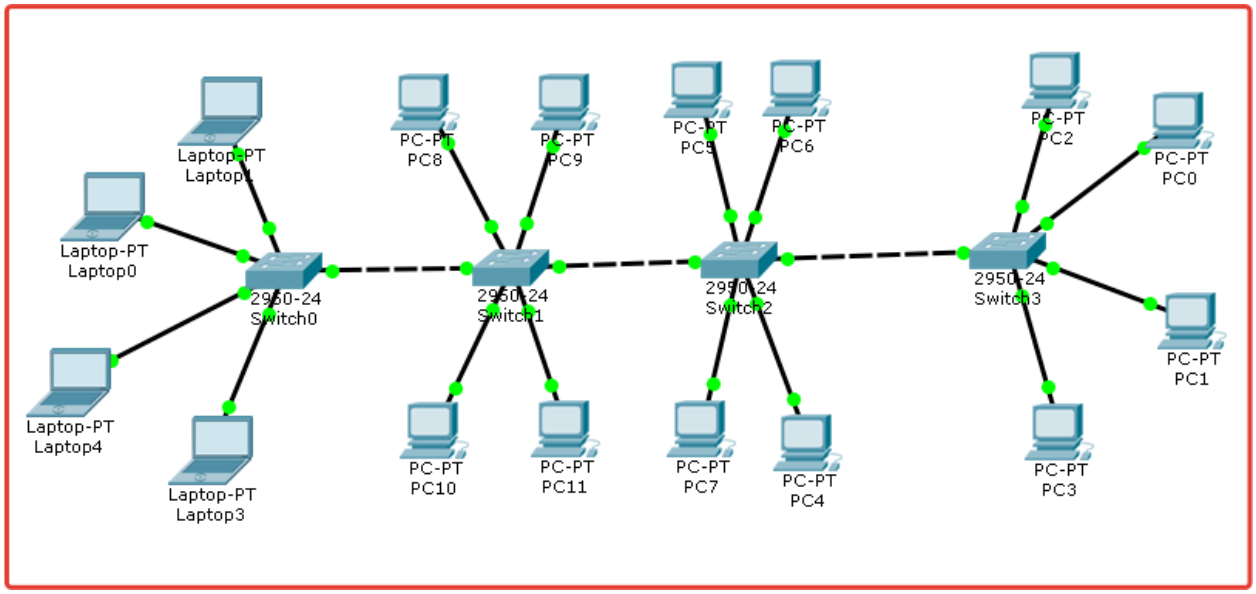


Рис.5.1 все компьютеров подключены к сети

Когда компьютеров подключены в разные VLAN они не могу больше связаться с друг с другом.

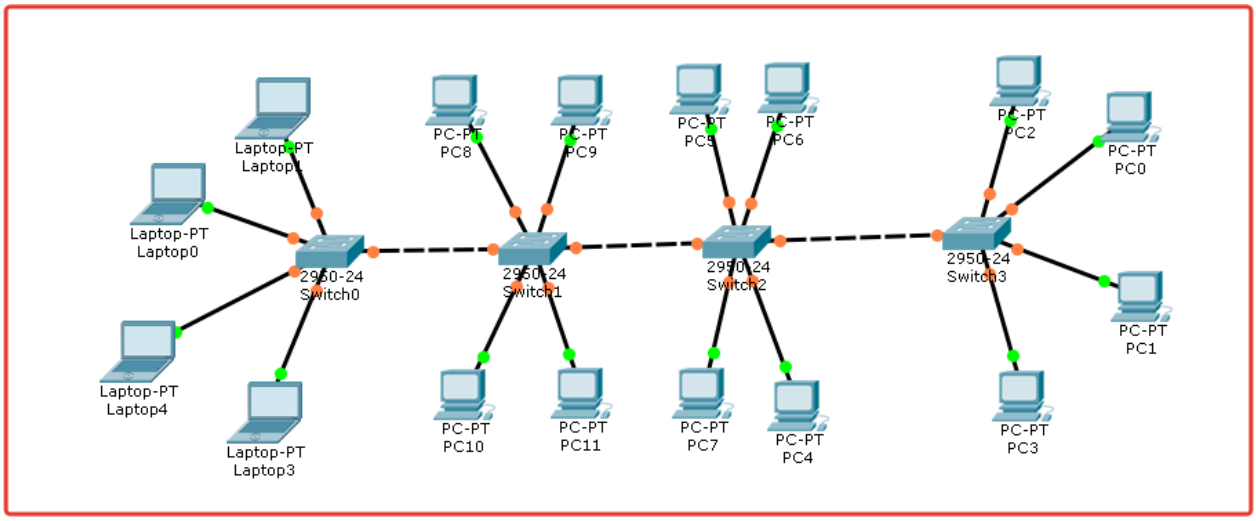


Рис. 5.2 ПК из разные VLAN больше не подключен

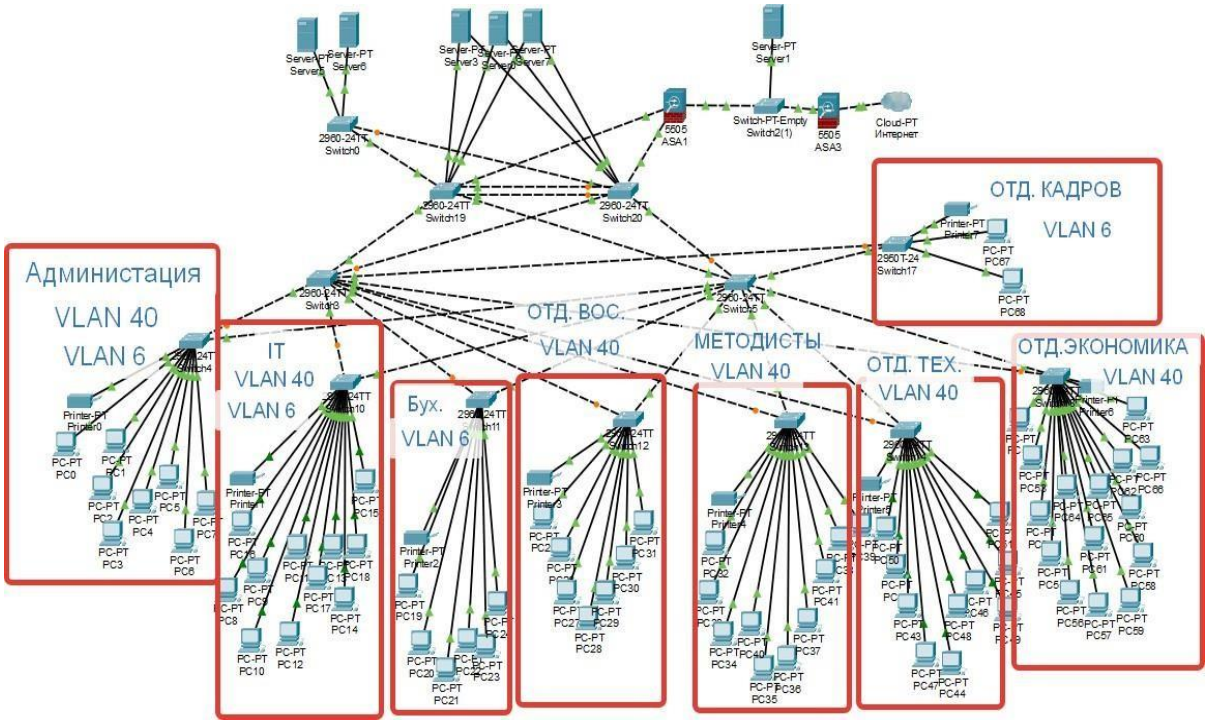


Рис. 5.3 Схема моделирования vlan в cisco packet tracer

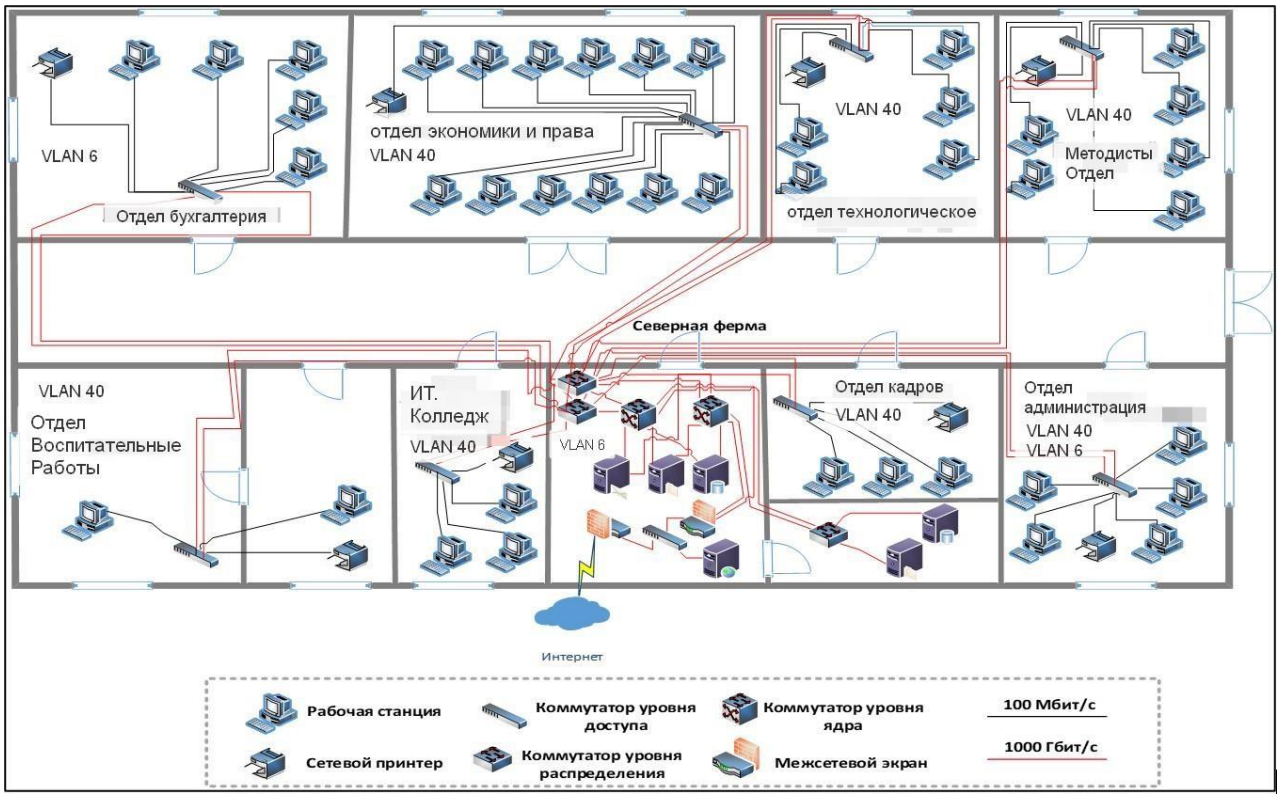


Рис.5.4 Горизонтальная разводка сети

Тверской колледж им. Коняева состоит из восьми отделов: отдел кадров 3 компьютеры, администрация колледжа 7 компьютеров, методисты 12 компьютеры, отдел ит. колледж 10 компьютеров, отдел экономики и права 11 компьютеров, отдел технологическое 10 компьютеров, отдел воспитательные работы 7 компьютеров, бухгалтерия 8 компьютеров. Администрация, ит отдел, методисты, отдел экономики и права, отдел технологическое, отдел воспитательные работы в одном vlan VLAN 40, все компьютеров, которые в этих отделов могут общаться без ограничения доступа. Отдел бухгалтерия,кадров, администрация, ит. отдел в vlan 6. все компьютеров, которые в этих отделов могут общаться без ограничения доступа.

5.5 Расчёт нагрузки в сети

Нагрузка на сеть – объем данных, реально передаваемый по сети в единицу времени. Другими словами, это скорость передачи данных. Нагрузка сети рассчитывается по формуле:

$$V = n*v_i$$

где n – число ПЭВМ (персональная электронно-вычислительная машина) в сети, vi – нагрузка на один ПЭВМ в сети. Нагрузка на один ПЭВМ в сети рассчитывается по формуле:

$$v_{сред} = D / t$$

где D – количество переданных данных, t – время, за которое были переданы данные. До создания VLAN произведённый анализ при отправке нескольких пакетов с объемом 10 Мбайт по разным компьютерам и разным адресам показал, что среднее время задержки является 0,08 секунды. А после создание VLAN адресам показал, что среднее время задержки является 0,04 секунды. Считаю это хорошим результатом по эффективности передачи пакета во внутреннюю и внешнюю сеть в колледж Коняева. Так как нагрузка на одну ПЭВМ составляет:

До создания VLAN: $v_{сред}$ = 10 Мбайт / 0,08 сек = 125 Мбайт/сек

После создания VLAN: $v_{сред}$ = 10 Мбайт / 0,04 сек = 250 Мбайт/сек

Пропускная способность сети (C) — это наибольшая возможная в данной сети скорость передачи информации. Она определяется некоторыми ограничивающими факторами (объем передаваемой по сети служебной информации, длительность интервалов между передаваемыми блоками данных) и битовой скоростью. Значения пропускной способности для сетевых технологий известны и приводится в стандарте.

Для проверки пропускной способности используется соответствующий метод тестирования. При проведении типового тестирования пропускной способности с одного устройства на другое с определенной скоростью отправляется трафик в течение заданного периода времени. Принимающее устройство считает количество кадров, полученных во время тестирования. Если при передаче данных не был потерян ни один кадр, пропускная способность будет равна скорости передачи. Если же один или несколько кадров потеряны, то пропускная способность окажется ниже, чем скорость передачи. Чтобы узнать максимальную пропускную способность линии, необходимо начать с максимальной теоретической скорости передачи и постепенно снижать скорость, пока на принимающем устройстве больше не будет потерян ни один кадр.

ЗАКЛЮЧЕНИЕ

Технология VLAN позволяет разделять сеть на логические сегменты. Каждый такой логический сегмент имеет свой широковещательный домен. Уникастовый, бродкастовый и мультикастовый трафик передается только между устройствами входящими в один VLAN. VLAN часто используется для разделения IP сегментов сети, с последующей маршрутизацией и фильтрацией трафика между разными VLAN на маршрутизаторе или на коммутаторе третьего уровня. VLAN обладают следующими преимуществами:

- повышение безопасности каждой виртуальной сети. Работники одного отдела офиса не смогут отслеживать трафик отделов, не входящих в их VLAN, и не получат доступ к их ресурсам;
- сокращение числа широковещательных запросов, которые снижают пропускную способность сети;
- создать новую виртуальную сеть можно без прокладки кабеля и покупки коммутатора;
- позволяет объединить в одну сеть компьютеры, подключенные к разным коммутаторам;
- возможность разделять или объединять отделы или пользователей, территориально удаленных друг от друга. Это позволяет привлекать к рабочему процессу специалистов, не находящихся в здании офиса.

Использование VLAN не только упрощает жизнь системным администраторам, позволяя быстро вносить изменения в структуру сети, но и даёт организациям возможность экономить на сетевом оборудовании.

В большинстве случаев при работе как системный администратор, я обошёлся без покупки дополнительного оборудования, настроив на коммутаторах VLAN для каждого отдела. Это позволило высвободить из старого офиса два коммутатора и использовать их для построения сети в новом

офисе. Кроме того, благодаря VLAN решилась проблема с маршрутизацией трафика по WAN-каналу

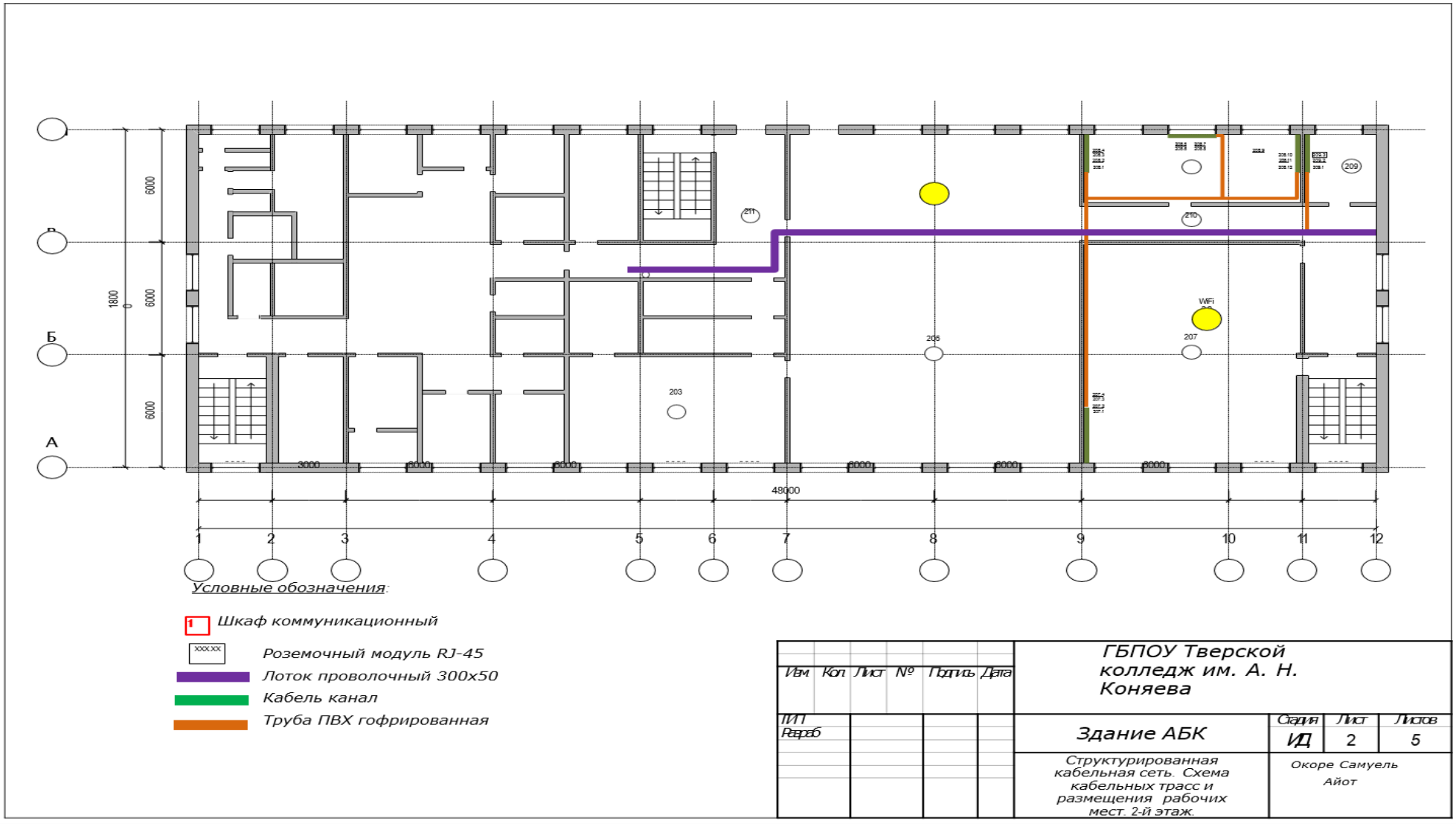
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Enterprise Resource Planning Systems: Systems, Life Cycle, Electronic
2. Путь аналитика. Практическое руководство IT-специалиста/Вера Иванова
3. Гибкое управление проектами и продуктами/Борис Вольфсон - Издательство «Питер», 2016.
4. Software Requirements (Разработка требований к программному обеспечению)/ Карл И. Вигерс, Джой Битти. - Издательство «БХВ-Петербург, Русская Редакция», 2016.
5. Лекция Проектирование высокоскоростной компьютерной сети. Технология Gigabit Ethernet [Электронный ресурс] – Профессор В.А. Григорьев
6. Лекция по дисциплине “Вычислительные машины, системы и сети” - ht
7. Олифер В. Г., Олифер Н. А. Компьютерные сети: принципы, технологии, протоколы. – Учебник для ВУЗов, СПб.: 2004. – 864 с.
8. Слепов Н. Сети SDH новой генерации и их использование для передачи трафика Ethernet. – ЭЛЕКТРОНИКА: НТБ, 2005, №3, с.62; №4, с.
9. Технология Ethernet. – В кн.: Руководство по технологиям объединенных сетей. 3-е изд. – М., С.–Пб., К.: Изд. дом "Вильямс

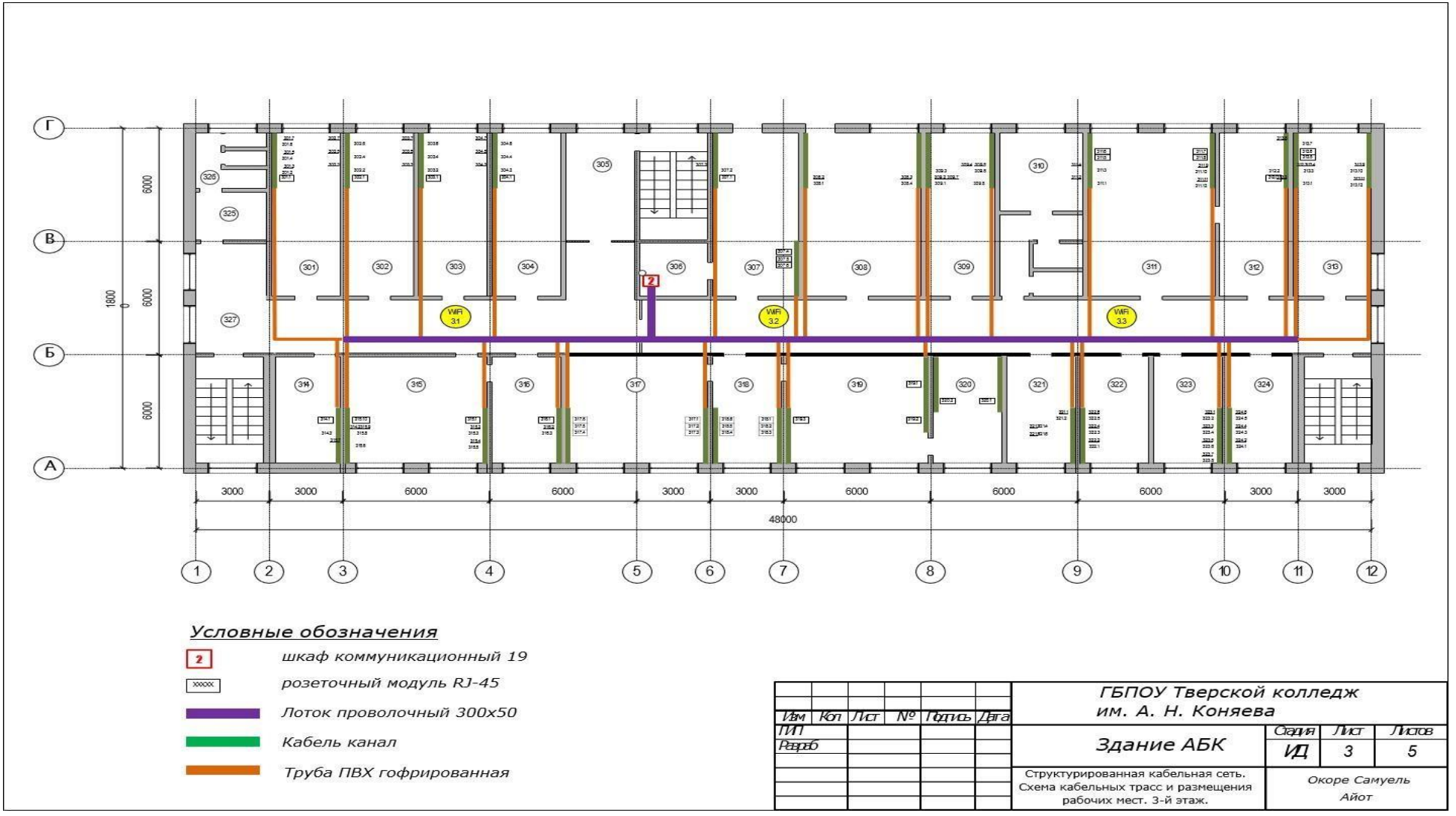
Приложения

Первый этаж структура сети в колледже Приложение А

Второй этаж структура сети в колледже **Приложение Б**

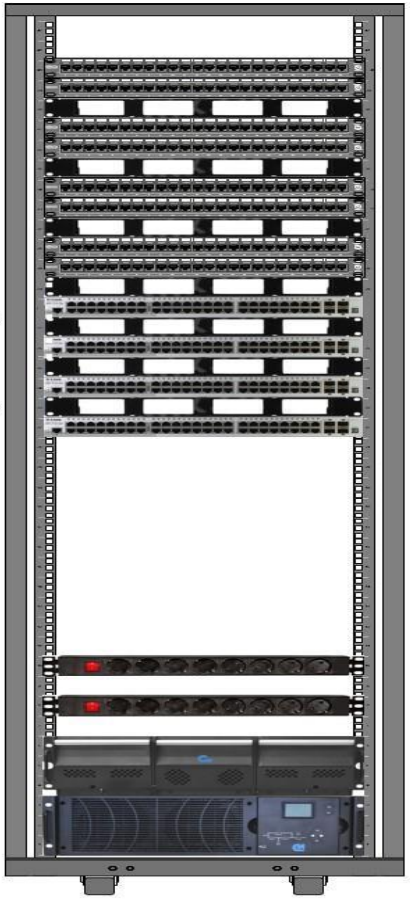


Третий этаж структура сети в колледже **Приложение В**



Структурированная кабельная сеть. Шкаф1. Приложение Г

PL-24-Cat.5e-Dual Патч-панель 24 порта №1
PL-24-Cat.5e-Dual Патч-панель 24 порта №2
CO35-1MSRM Кабельный органайзер №1
PL-24- Cat.5e-Dual Патч-панель 24 порта №3
PL-24-Cat.5e-Dual Патч-панель 24 порта №4
CO35-1MSRM Кабельный органайзер №2
PL-24-Cat.5e-Dual Патч-панель 24 порта №5
PL-24-Cat.5e-Dual Патч-панель 24 порта №6
CO35-1MSRM Кабельный органайзер №3
PL-24-Cat.5e-Dual Патч-панель 24 порта №7
PL-24-Cat.5e-Dual Патч-панель 24 порта №8
CO35-1MSRM Кабельный органайзер №4
DGS-1510-52X/A1 Коммутатор 48 портов №1
CO35-1MSRM Кабельный органайзер №5
DGS-1510-52XMP/A1A Коммутатор 48 портов с PoE №2
CO35-1MSRM Кабельный органайзер №6
DGS-1510-52X/A1 Коммутатор 48 портов №3
CO35-1MSRM Кабельный органайзер №7
DGS-1510-52XMP/A1A Коммутатор 48 портов с PoE №4

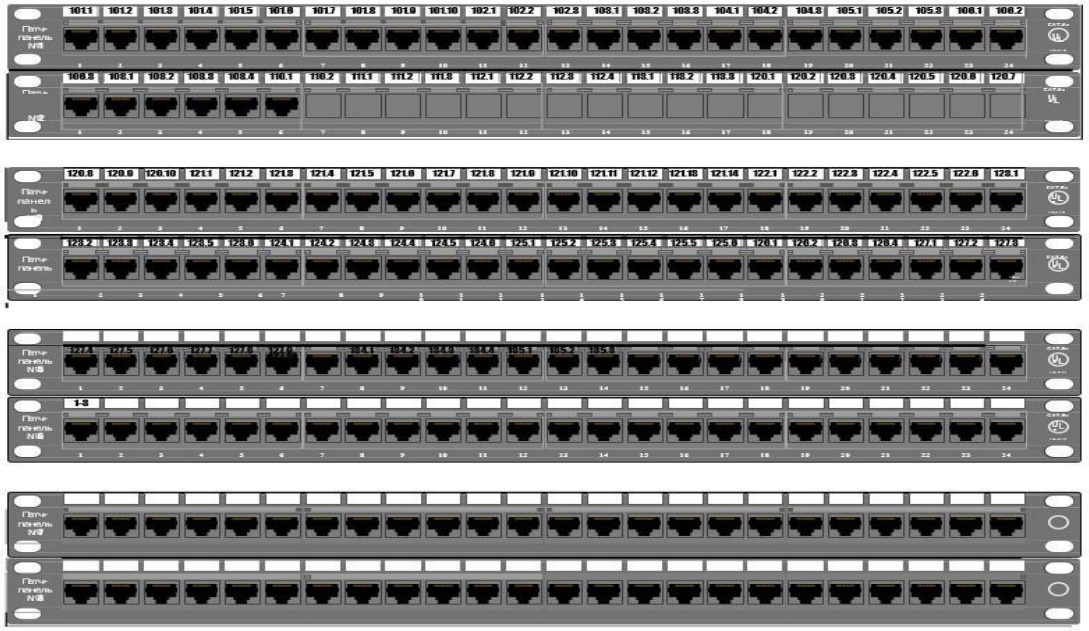


PDU-8P-2EU Блок электрических розеток №1

PDU-8P-2EU Блок электрических розеток №2

БМСИПБ6-10КД Батарейный модуль

ИБП СИПБ6КД.9-11 Источник бесперебойного питания



Изм	Кол	Лист	№	Подпись	Дата	ГБПОУ Тверской колледж им. А. Н. Коняева			
ГИП						Здание АБК	Стадия	Лист	Листов
Разраб							ИД	4	5
						Структурированная кабельная сеть. Шкаф1. каб.109. Схема подключений и размещения оборудования.	Окоре Самуель Айот		

Структурированная кабельная сеть. Шкаф 2. Приложение Д

Supermicro YS-5018A-MLTN4
Маршрутизатор

PL-24-Cat.5e-Dual Патч-панель 24 порта №1

PL-24-Cat.5e-Dual Патч-панель 24 порта №2

CO35-1M5RM Кабельный органайзер №1

PL-24- Cat.5e-Dual Патч-панель 24порта №3

PL-24-Cat.5e-Dual Патч-панель 24 порта №4

CO35-1M5RM Кабельный органайзер №2

PL-24-Cat.5e-Dual Патч-панель 24 порта №5

PL-24-Cat.5e-Dual Патч-панель 24 порта №6

CO35-1M5RM Кабельный органайзер №3

PL-24-Cat.5e-Dual Патч-панель 24 порта №7

PL-24-Cat.5e-Dual Патч-панель 24 порта №8

CO35-1M5RM Кабельный органайзер №4

DGS-1510-52X/A1 Коммутатор 48 портов №1

CO35-1M5RM Кабельный органайзер №5

DGS-1510-52XMP/A1A Коммутатор 48 портов с PoE №2

CO35-1M5RM Кабельный органайзер №6

DGS-1510-52X/A1 Коммутатор 48 портов №3

CO35-1M5RM Кабельный органайзер №7

DGS-1510-52XMP/A1A Коммутатор 48 портов с PoE №4

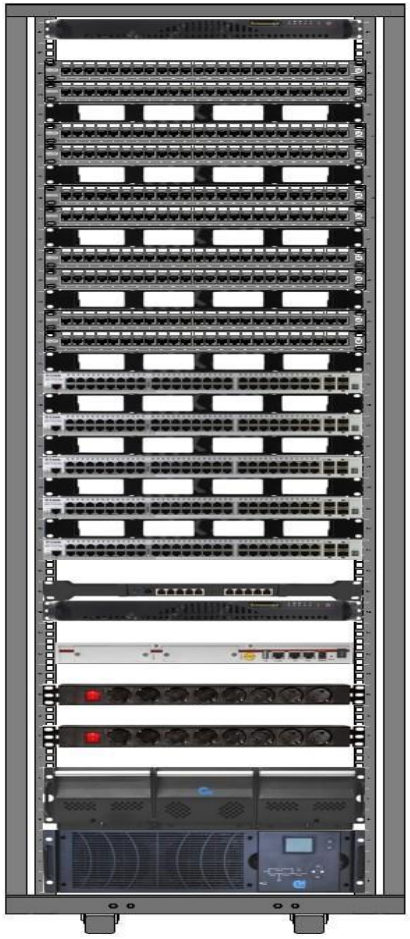
MIKROTIK RB4011iGS+RM
Контроллер SoftWLC Supermicro SYS-5018A-MLTN4 Контроллер WiFi LAVoice-100 IP ATC на 50 абонентов

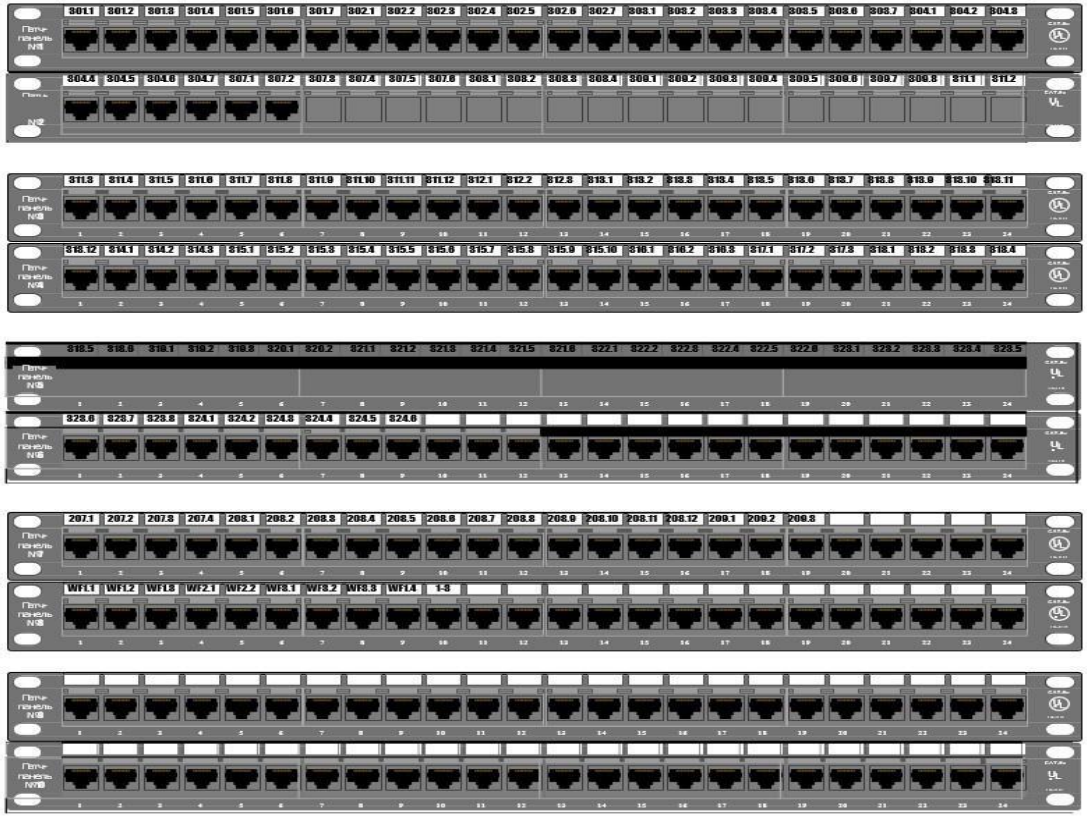
PDU-8P-2EU Блок электрических розеток №1

PDU-8P-2EU Блок электрических розеток №2

БМСИПБ6-10КД Батарейный модуль

ИБП СИПБ6КД.9-11 Источник бесперебойного питания





Изм.	Кол.	Лист	№	Подпись	Дата	ГБПОУ Тверской колледж им. А. Н. Коняева			
ПП						Здание АБК	Стадия	Лист	Листов
Разраб							ИД	5	5
						Структурированная кабельная сеть. Шкаф коммуникационный 19" каб.306	Окоре Самуель Айот		

Уровень доступа **Приложение Е**

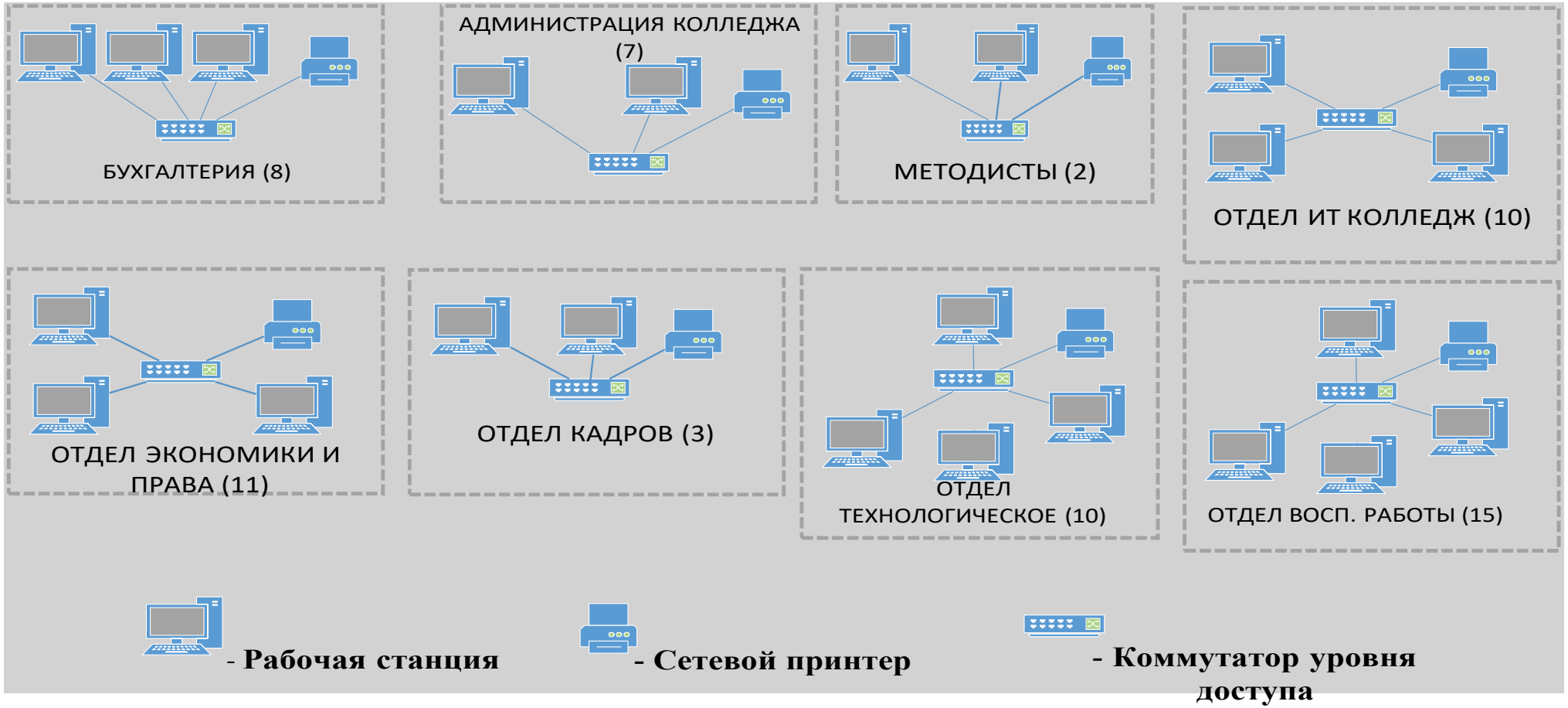
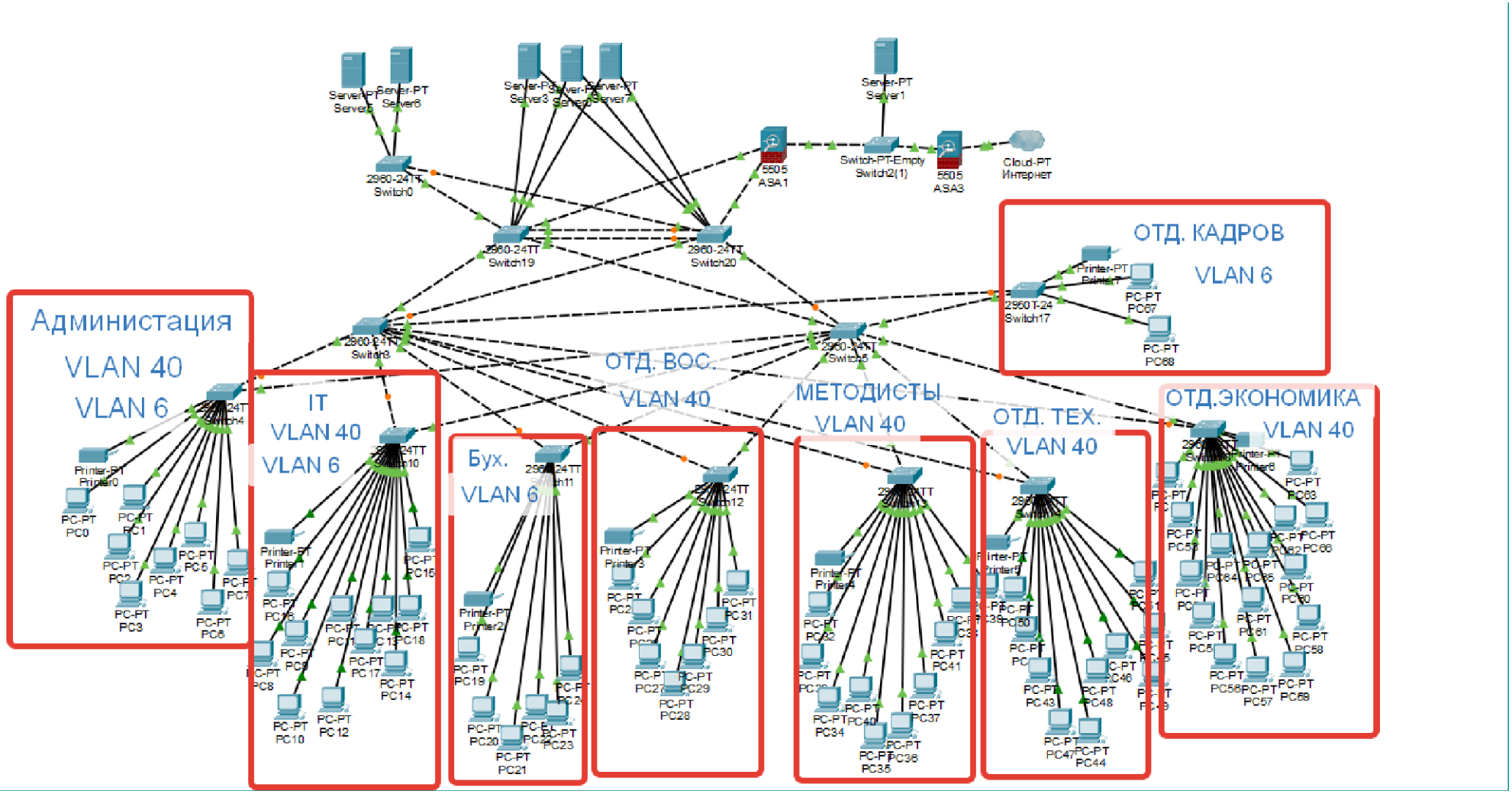


Схема моделирования VLAN в cisco packet tracer **Приложение Ё**



Горизонтальная разводка сети **Приложение Ж**