Оглавление

Введение

В условиях рыночной экономики информация выступает как один из важнейших товаров. Новейшие достижения в области микроэлектроники привели к новым концепциям в организации информационных служб. Успех коммерческой и предпринимательской деятельности связан с муниципальными, банковскими, биржевыми информационными системами, информатизацией оптовой и розничной торговли, торговых домов, служб управления трудом и занятостью, созданием банка данных рынка товаров и услуг, развитием центров справочной и аналитико-прогнозной информации, электронной почты, электронного обмена данными и др. Как правило, работа этих систем базируется на локальных вычислительных сетях (ЛВС) различной архитектуры или их объединениях, получивших название корпоративных сетей.

Локальная вычислительная сеть (ЛВС) представляет собой особый тип сети, объединяющий близко расположенные системы. В настоящее время достаточно трудно представить себе организацию, занимающуюся любым видом деятельности, без локальной сети. В век информационных технологий и научно-технического прогресса наиболее актуальны такие проблемы, как:

- скорость обмена информацией;
- дорогостоящее оборудование;
- совместное использование внешних устройств;
- доступ к информации.

Эффективная обработка информации – одна из наиболее распространенных функций, выполняемых ЛВС. Применение информационно-вычислительных сетей может снять большинство проблем, связанных с использованием больших объёмов информации в таких организациях. Передача данных и связь занимает особое место среди перечисленных приложений сетей.

Вышеперечисленные факты позволяют говорить об актуальности темы исследования.

1. Общесистемный раздел

1.1. Анализ предметной области и постановка задач исследования

1.1.1 Анализ объекта проектирования

ЗАО “Талисман центр” представляет широкий спектр услуг в области защиты информации, имеющей степень конфиденциальности государственной тайны, коммерческой тайны, конфиденциальной информации, персональных данных. Талисман центр осуществляет свою деятельность на основании лицензий и аттестатов аккредитации Федеральной службы по техническому и экспортному контролю. Значительный опыт работы (более 10 лет), накопленный организацией, позволяет выполнять сертификационные испытания оперативно, качественно и на высоком профессиональном уровне.

В сферу деятельности также входят услуги по разработке программного обеспечения, тестированию ПО, оценке стоимости разработки программных средств.

Основные направления деятельности:

- Сертификация средств защиты информации
- Комплексная оценка защищенности (аудит) автоматизированных систем любой сложности;
- Аттестация информационных систем персональных данных по требованиям безопасности информации;
- Защита информации в платежных системах;
- Разработка программного обеспечения;
- Оценка стоимости разработки программного обеспечения;
- Тестирование и контроль качества программного обеспечения.

Структура объекта ЗАО " Талисман центр "

Схема. 1. Структура объекта

1.1.2. Анализ информационных потоков и предполагаемого трафика

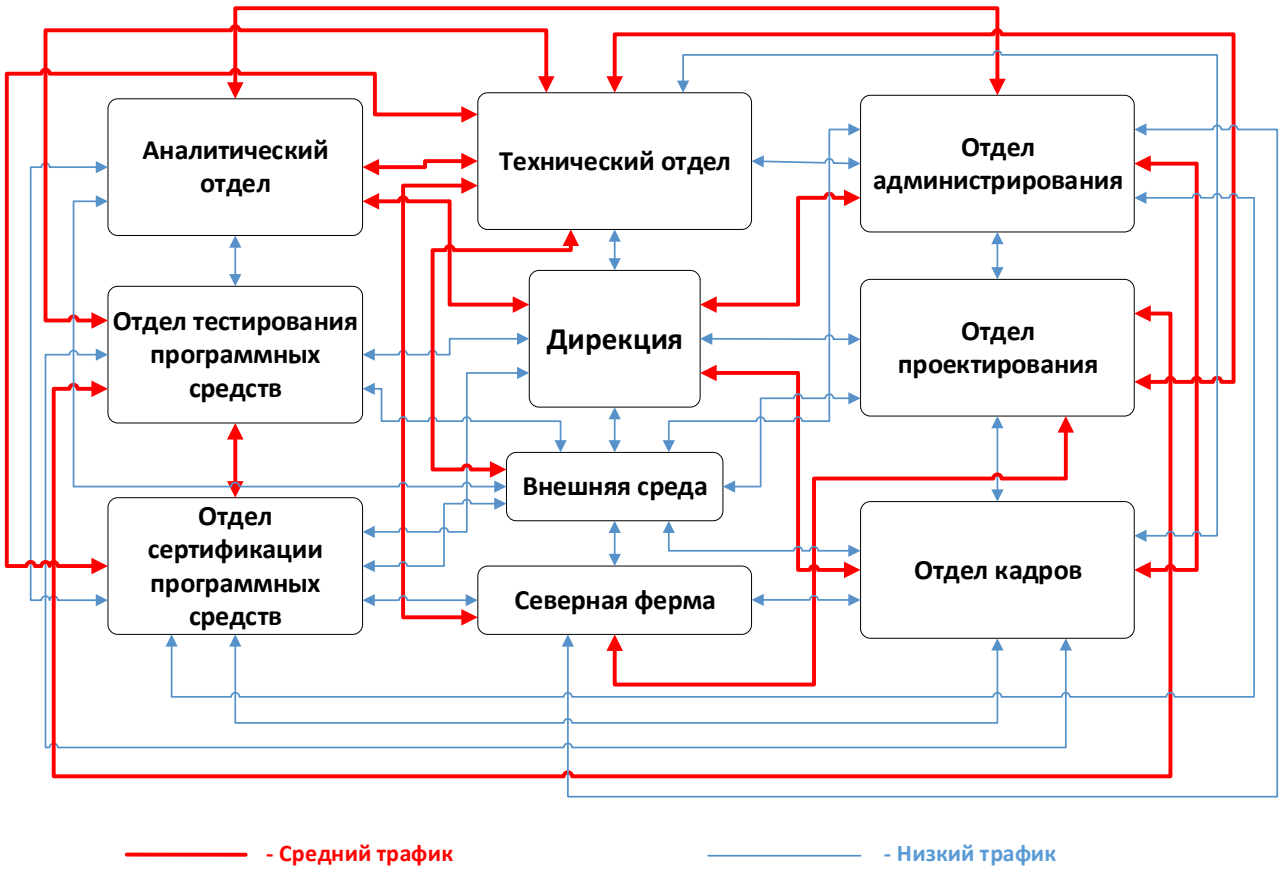
В процессе анализа информационных потоков предприятия необходимо изучить процессы возникновения, движения и обработки информации, а также направленность и интенсивность документооборота на предприятии.

Наиболее распространенный и, по-видимому, самый практичный метод анализа информационных потоков — составление графиков информационных потоков. Каждый информационный поток — единичное перемещение информации — имеет следующие признаки:

- Документ (на чем физически содержится информация);
- исполнителя (человека, который эту информацию передает);

- периодичность (частота передачи: ежемесячно, ежеквартально, ежедневно).
- На предприятии выделяют два уровня детализации информационных потоков:
- на уровне предприятия детализация производится до уровня подразделения, т.е. информация передается между подразделениями и службами предприятия;
- на уровне подразделения предприятия детализация производится до уровня рабочего места, т.е. информация передается между работниками подразделения и связанных с подразделением служб.

.



1.2. Выбор сетевой архитектуры системы

Локальные вычислительные сети (ЛВС сети) сегодня являются неотъемлемой частью современного офиса. Объединение компьютеров в

локальную сеть позволяет обеспечить совместное использование ресурсов сети и оперативный доступ к любой корпоративной информации, организовать высокоскоростной доступ в Интернет пользователей и создать надежные централизованные средства резервирования и хранения информации.

При построении ЛВС наиболее эффективным является применение многоуровневой архитектуры, базирующейся на принципах иерархичности и модульности. Принцип иерархичности подразумевает разделение сети на несколько уровней, каждый из которых выполняет определенные функции. Модульность означает, что уровни сети реализуются на основе модулей, и каждый модуль представляет собой функционально законченную группу оборудования, выполняющую функции соответствующего уровня. Архитектура сети включает в себя четыре уровня: ядро сети, уровень агрегации, уровень доступа и серверный уровень (серверная ферма).

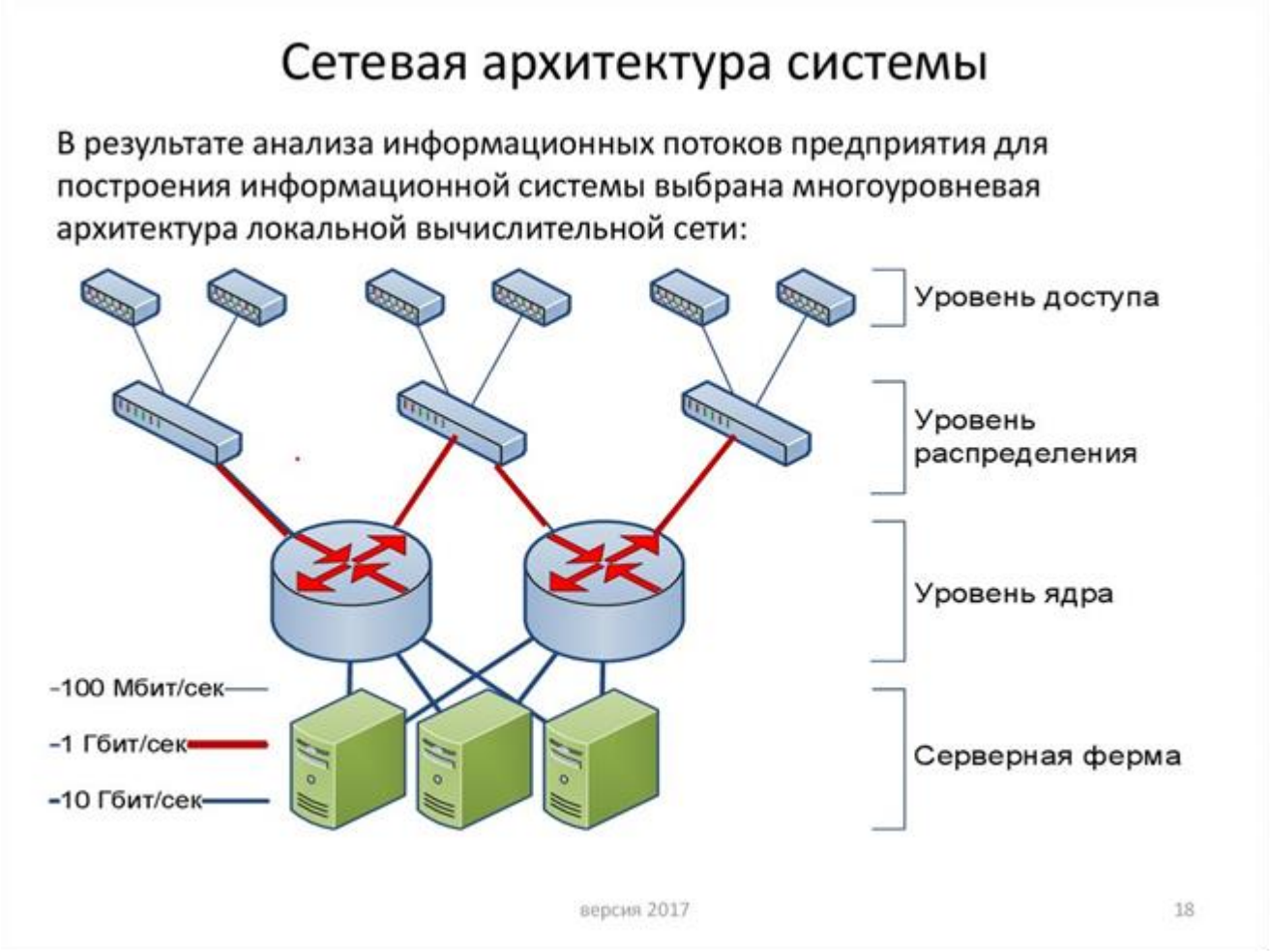


Рис. 1. Многоуровневая архитектура сети

Основная цель применения многоуровневой архитектуры при построении ЛВС заключается в обеспечении высокой надежности и производительности. При реализации каждого уровня основной задачей является обеспечение масштабируемости, то есть расширения мощности уровня без серьезных архитектурных изменений. Для этого каждый уровень реализуется на базе модулей – функционально законченных групп оборудования, как правило, одного типа.

Уровень доступа:

Данный уровень предназначен для подключения рабочих станций пользователей и других периферийных устройств (сетевых принтеров и др.) к ЛВС. Основное требование, предъявляемое к оборудованию уровня доступа, заключается в поддержке всевозможного функционала, обеспечивающего безопасность подключения абонента к сети. Коммутаторы доступа должны максимально облегчать администрирование подключений абонента, по возможности автоматизируя рутинные операции по поддержке сети.

Уровень агрегации:

Уровень агрегации (распределения) выполняет связующую функцию и функцию агрегации трафика абонентов. Основное требование к этому уровню состоит в обеспечении резервирования и оптимальном разделении нагрузки между параллельными соединениями (как в сторону уровня доступа, так в сторону ядра сети). Модули, используемые для организации уровня распределения, обычно организуются двумя аналогичными коммутаторами, функционирующими в режиме взаимного резервирования.

Ядро сети:

Уровень ядра сети обеспечивает высокоскоростную коммутацию трафика между виртуальными локальными сетями предприятия, подключение к глобальной сети Интернет, выполняет функции аппаратного файервола. Как правило, ядро сети строится из модулей, образованных одним

высокопроизводительным устройством, с обеспечением резервирования на аппаратном уровне и уровне каналов.

Серверный уровень:

В последнее время, в связи с увеличением трафика приложений, активного использования ресурсов локальных вычислительных сетей для передачи медиа-трафика (аудио и видео) возникла необходимость отделять серверы компании от рядовых компьютеров, подключать их через выделенные коммутаторы, с целью более гибкого управления пропускной способностью каналов.

Серверная ферма представляет собой группу коммутаторов, являющуюся ключевой компонентой ЛВС предприятия, обеспечивающей подключение к ней серверов. Важное требование, предъявляемое к серверной ферме, заключается в высокой производительности и надежности. Простои серверной фермы приводят к простоям работы информационных систем, а, следовательно, к потерям в бизнесе.

Таким образом, многоуровневая архитектура, используемая при построении ЛВС, позволяет индивидуально подходить к требованиям каждого клиента, сокращать время простоя сети и информационных систем и минимизировать потери рабочего времени, а также создает возможность внедрения дополнительных приложений и сервисов, таких как:

- IP-телефония;
- Видеоконференцсвязь;
- Контроль доступа к ресурсам КСПД (Network Admission Control);
- Резервирование каналов связи и отдельных элементов КСПД в автоматическом режиме;
- Защищенный доступ удаленных сотрудников к ресурсам КСПД;
- Мониторинг состояния активного сетевого оборудования и линий связи;
- Средства организации коллективной работы;

В результате анализа информационных потоков организации для построения информационной системы выбрана многоуровневая архитектура локальной вычислительной сети:

Иерархическая модель сети подразумевает наличие трех уровней.

- Ядро отвечает за высокоскоростную передачу сетевого трафика, а именно коммутация пакетов с максимальной скоростью.
- На уровне распределения происходит агрегация трафика и минимизация числа каналов с ядром сети.
- Уровень доступа формирует сетевой трафик и выполняет контрольные функции. Все политики доступа к сети реализуются на устройствах уровня доступа.

Данная архитектура полностью соответствует потребностям, выявленным в результате анализа информационных потоков.

1.3. Описание технологий сети

В данной курсовой работе будут применяться технологии Fast Ethernet, Gigabit Ethernet, рассмотрим их.

1.3.1 Fast Ethernet

Fast Ethernet — набор стандартов передачи данных в компьютерных сетях, со скоростью до 100 Мбит/с.

В 1992 году ряд производителей сетевого оборудования (3Com, SynOptics и др.) образовали объединение Fast Ethernet Alliance, предназначенное для создания новой спецификации, которая объединила бы отдельные наработки различных компаний в области кабельной передачи данных. Вместе с тем в институте IEEE была начата работа по стандартизации новой технологии. Созданная для этого исследовательская группа, с конца 1992 по конец 1993 года изучила множество 100-мегабитных решений, предложенных различными производителями.

26 октября 1995 года официально был принят стандарт IEEE 802.3u, который явился дополнением к уже существующему IEEE 802.3.

Отличия Fast Ethernet от Ethernet сосредоточены на физическом уровне.

Более сложная структура физического уровня технологии Fast Ethernet вызвана тем, что в ней используется три варианта кабельных систем - оптоволокно, 2-х парная витая пара категории 5 и 4-х парная витая пара категории 3, причем по сравнению с вариантами физической реализации Ethernet (а их насчитывается шесть), здесь отличия каждого варианта от других глубже - меняется и количество проводников, и методы кодирования. А так как физические варианты Fast Ethernet создавались одновременно, а не эволюционно, как для сетей Ethernet, то имелась возможность детально определить те подуровни физического уровня, которые не изменяются от варианта к варианту, и остальные подуровни, специфические для каждого варианта.

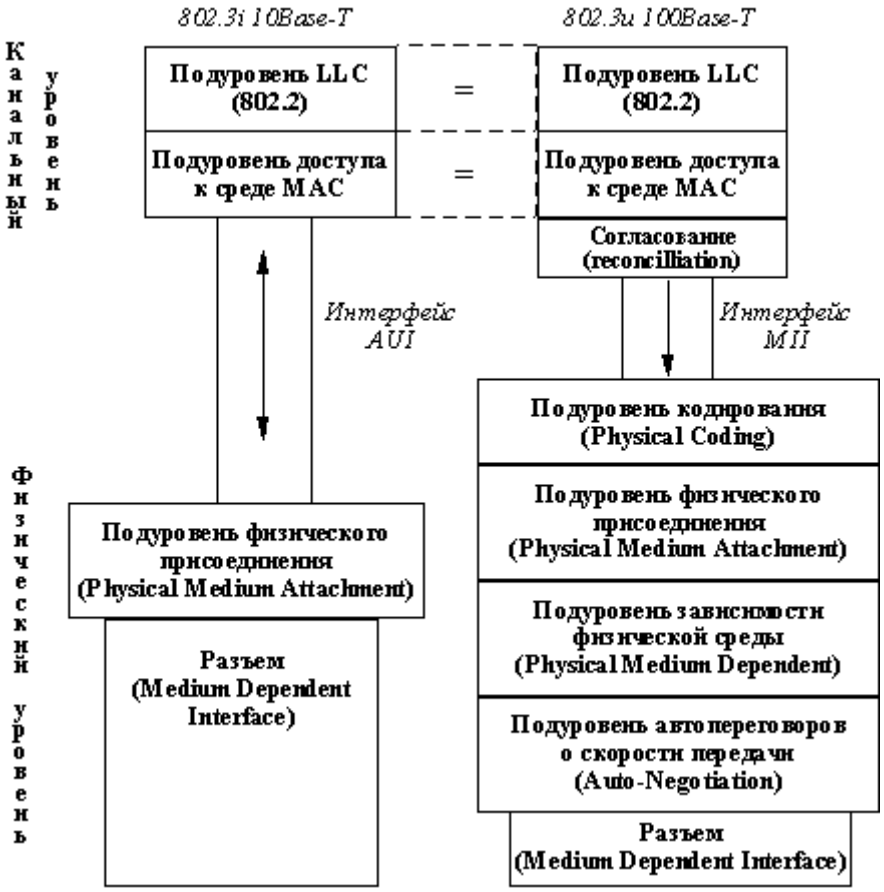


Рис. 3. Отличие 100Base-T от 10Base-T

Преимущества:

- Увеличение пропускной способности сегментов сети до 100 Мбит/с.
- Сохранение метода случайного доступа Ethernet.
- Сохранение звездообразной топологии сетей.
- Поддержка традиционных сред передачи данных — витой пары и волоконно-оптического кабеля.

Недостатки:

- При взаимодействии рабочих станций не происходит качественного их обслуживания.
- Невозможность проверки сетевого оборудования и тестирования работоспособности сети.
- Нет приоритетности при принятии трафика.
- Приличные временные задержки при передаче данных.

Стандарты:

100BASE-FX — вариант Fast Ethernet с использованием волоконно-оптического кабеля. В данном стандарте используется длинноволновая часть спектра (1300 нм) передаваемая по двум жилам, одна для приёма и одна для передачи. Длина сегмента сети может достигать 400 метров в полудуплексном режиме (с гарантией обнаруженияколлизий) и двух километров в полнодуплексном при использовании многомодового волокна. Работа на больших расстояниях возможна при использовании одномодового волокна.

100BASE-SX — удешевленная альтернатива 100BASE-FX с использованием многомодового волокна, так как использует недорогую коротковолновую оптику. 100BASE-SX может работать на расстояниях до 300 метров. Благодаря использованию более коротких волн (850 нм) и небольшой дистанции, на которой он может работать, 100BASE-SX использует менее дорогие оптические компоненты (светодиоды (LED) вместо лазеров). Все это делает данный стандарт привлекательным для тех,

кто модернизирует сеть 10BASE-FL и тех, кому не нужна работа на больших расстояниях.

100BASE-BX — вариант Fast Ethernet по одножильному волокну. Используется одномодовое волокно, наряду со специальным мультиплексором, который разбивает сигнал на передающие и принимающие волны.

100BASE-LX — 100 Мбит/с Ethernet с помощью оптического кабеля. Максимальная длина сегмента 15 километров в полнодуплексном режиме по паре одномодовых оптических волокон.

100BASE-LX WDM — 100 Мбит/с Ethernet с помощью волоконно-оптического кабеля. Максимальная длина сегмента 15 километров в полнодуплексном режиме по одному одномодовому оптическому волокну на длине волны 1310 нм и 1550 нм. Интерфейсы бывают двух видов, отличаются длиной волны передатчика и маркируются либо цифрами (длина волны), либо одной латинской буквой A(1310) или B(1550).

1.3.2 Gigabit Ethernet

Gigabit Ethernet — набор стандартов передачи данных в компьютерных сетях, со скоростью до 1000 Мбит/с.

В 1995 г. IEEE предписал исследовательской группе разработать более высокоскоростной (чем Fast Ethernet) стандарт. В 1996 г. этими исследованиями занялся Gigabit Ethernet Alliance. А уже в 1997 -98 гг. был рассмотрен и принят стандарт 802.3z (интерфейс 1000 Base-X).

Преимущества:

- Увеличение пропускной способности сегментов сети до 1000 Мбит/с.
- Сохранение совместимости с методом случайного доступа.
- Сохранение формата кадра Ethernet.

– Сохранение звездообразной топологии сетей и поддержка традиционных сред передачи данных — витой пары и оптоволоконного кабеля.

Недостатки:

– Большие задержки доступа к среде.
– Небольшие расстояния между узлами даже при использовании оптоволокна, что связано с работой метода обнаружения коллизий.
– Отсутствие механизмов выбора резервных связей.
– Отсутствие поддержки приоритетного трафика приложений реального времени.

Стандарты:

– **1000BASE-T**, IEEE 802.3ab — стандарт, использующий витую пару категорий 5e. В передаче данных участвуют 4 пары. Скорость передачи данных — 250 Мбит/с по одной паре. Расстояние до 100 метров
– **1000BASE-TX** использует раздельную приёмо-передачу (по одной паре в каждом направлении), что существенно упрощает конструкцию приёмопередающих устройств. На основе данного стандарта практически не было создано продуктов, хотя 1000BASE-TX использует более простой протокол, чем стандарт 1000BASE-T, и поэтому может использовать более простую электронику.
– **1000BASE-SX**, IEEE 802.3z — стандарт, использующий многомодовое волокно. Дальность прохождения сигнала без повторителя до 550 метров.
– **1000BASE-LX**, IEEE 802.3z — стандарт, использующий одномодовое волокно. Дальность прохождения сигнала без повторителя зависит только от типа используемых приемопередатчиков и, как правило, составляет от 5 до 50 километров.
– **1000BASE-LH** (Long Haul) — стандарт, использующий одномодовое волокно. Дальность прохождения сигнала без повторителя до 100 километров.

Для реализации выбранной архитектуры сети будут использоваться следующие технологии:

- Fast Ethernet
- Gigabit Ethernet

Технология Fast Ethernet – будет использоваться для реализации уровня доступа сети. Данная технология является наиболее универсальной, а также обладает очень большой гибкостью, и полностью соответствует архитектуре разрабатываемой сети.

Технология Gigabit Ethernet – будет использоваться для реализации уровня распределения сети и для реализации уровня ядра сети. Данная технология полностью совместима с технологией Fast Ethernet и предоставляет более производительное решение для высокоскоростного доступа.

На уровне доступа*: Fast Ethernet* реализована стандартом 100BaseT4, кабель – экранизированная витая пара S/FTP Cat.6a, полный дуплекс.

На уровне распределения: *Gigabit Ethernet* реализована стандартом 1000 Base-T, выбран SSTP кабель категории 7, обеспечивающий поддержку скорости передачи данных 1000 Мбит/с и полный дуплекс.

Локальная вычислительная сеть (ЛВС) - это комплекс оборудования и программного обеспечения, обеспечивающий передачу, хранение и обработку информации.

1.4. Топологии сетей

Под топологией (компоновкой, конфигурацией, структурой) компьютерной сети обычно понимается физическое расположение компьютеров сети друг относительно друга и способ соединения их линиями связи. Важно отметить, что понятие топологии относится, прежде всего, к локальным сетям, в которых структуру связей можно легко проследить. В глобальных сетях структура связей обычно скрыта от пользователей и не слишком важна, так как каждый сеанс связи может производиться по собственному пути.

Топология определяет требования к оборудованию, тип используемого кабеля, допустимые и наиболее удобные методы управления обменом, надежность работы, возможности расширения сети.

Различают физическую и логическую топологию. Логическая и физическая топологии сети независимы друг от друга. **Физическая** топология - это геометрия построения сети, а **логическая** топология определяет направления потоков данных между узлами сети и способы передачи данных.

Существует три основных топологии:

- "шина" (bus);
- “звезда” (star);
- “кольцо” (ring);

В настоящее время подавляющую часть локальных сетей составляет топология типа “звезда”.

Топология типа «Звезда»

Звезда – это топология локальной сети, где каждая рабочая станция присоединена к центральному устройству (коммутатору или маршрутизатору).

Центральное устройство управляет движением пакетов в сети. Каждый компьютер через сетевую карту подключается к коммутатору отдельным кабелем.

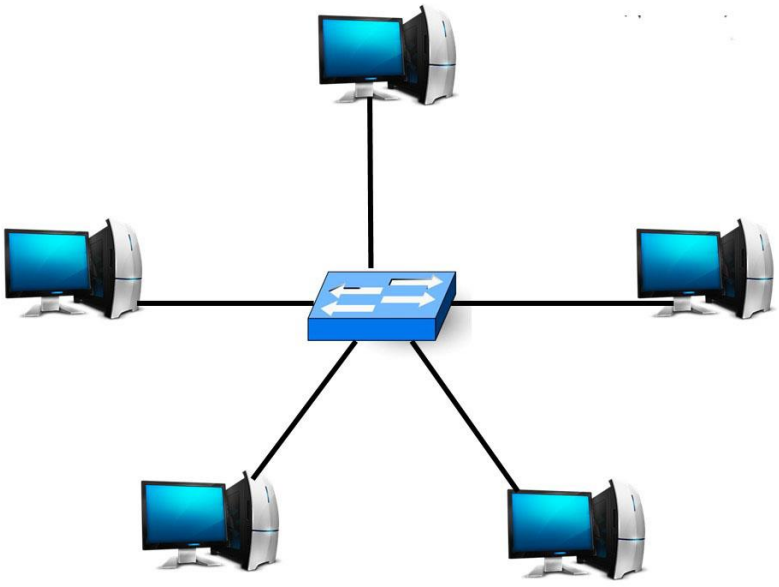


Рис. 4. Топология звезда

При необходимости можно объединить вместе несколько сетей с топологией “звезда” – в результате вы получите конфигурацию сети с ***древовидной*** топологией. Древовидная топология распространена в крупных компаниях. Мы не будем ее подробно рассматривать в данной статье.

Топология “звезда” на сегодняшний день стала основной при построении локальных сетей. Это произошло благодаря ее многочисленным достоинствам:

- выход из строя одной рабочей станции или повреждение ее кабеля не отражается на работе всей сети в целом;
- отличная масштабируемость: для подключения новой рабочей станции достаточно проложить от коммутатора отдельный кабель;
- легкий поиск и устранение неисправностей и обрывов в сети;
- высокая производительность;
- простота настройки и администрирования;
- в сеть легко встраивается дополнительное оборудование.

Однако, как и любая топология, “звезда” не лишена недостатков:

- выход из строя центрального коммутатора обернется неработоспособностью всей сети;
- дополнительные затраты на сетевое оборудование – устройство, к которому будут подключены все компьютеры сети (коммутатор);
- число рабочих станций ограничено количеством портов в центральном коммутаторе.

Звезда – самая распространенная топология для проводных и беспроводных сетей. Примером звездообразной топологии является сеть с кабелем типа витая пара, и коммутатором в качестве центрального устройства. Именно такие сети встречаются в большинстве организаций.

Топология сети типа "шина" (bus)

«Шина» (bus) — все компьютеры параллельно подключаются к одной линии связи. Информация от каждого компьютера одновременно передается всем остальным компьютерам

Рис. 5.

Топология «шина» (или, как ее еще называют, общая шина) самой своей структурой предполагает идентичность сетевого оборудования компьютеров, а также равноправие всех абонентов по доступу к сети. Компьютеры в шине могут передавать только по очереди, так как линия связи в данном случае единственная. Если несколько компьютеров будут передавать информацию одновременно, она исказится в результате наложения (конфликта, коллизии). В шине всегда реализуется режим так называемого полудуплексного (half duplex) обмена (в обоих направлениях, но по очереди, а не одновременно).

В топологии «шина» отсутствует явно выраженный центральный абонент, через которого передается вся информация, это увеличивает ее надежность (ведь при отказе центра перестает функционировать вся управляемая им система). Добавление новых абонентов в шину довольно просто и обычно возможно даже во время работы сети. В большинстве случаев при использовании шины требуется минимальное количество соединительного кабеля по сравнению с другими топологиями.

Поскольку центральный абонент отсутствует, разрешение возможных конфликтов в данном случае ложится на сетевое оборудование каждого отдельного абонента. В связи с этим сетевая аппаратура при топологии «шина» сложнее, чем при других топологиях. Тем не менее из-за широкого распространения сетей с топологией «шина» (прежде всего наиболее популярной в сети Ethernet) стоимость сетевого оборудования не слишком высока.

Важное преимущество «шины» состоит в том, что при отказе любого из компьютеров сети, исправные машины смогут нормально продолжать обмен.

При прохождении по линии связи сети с топологией «шина» информационные сигналы ослабляются и никак не восстанавливаются, что накладывает жесткие ограничения на суммарную длину линий связи. Причем каждый абонент может получать из сети сигналы разного уровня в зависимости от расстояния до передающего абонента. Это предъявляет дополнительные требования к приемным узлам сетевого оборудования.

Для увеличения длины сети с топологией «шина» часто используют несколько сегментов (частей сети, каждый из которых представляет собой «шину»), соединенных между собой с помощью специальных усилителей и восстановителей сигналов – репитеров или повторителей. Однако такое наращивание длины сети не может продолжаться бесконечно. Ограничения на длину связаны с конечной скоростью распространения сигналов по линиям связи.

Топология “кольцо”

В сети с топологией кольцо все узлы соединены каналами связи в неразрывное кольцо (необязательно окружность), по которому передаются данные. Выход одного ПК соединяется со входом другого ПК. Начав движение из одной точки, данные, в конечном счете, попадают на его начало. Данные в кольце всегда движутся в одном и том же направлении.

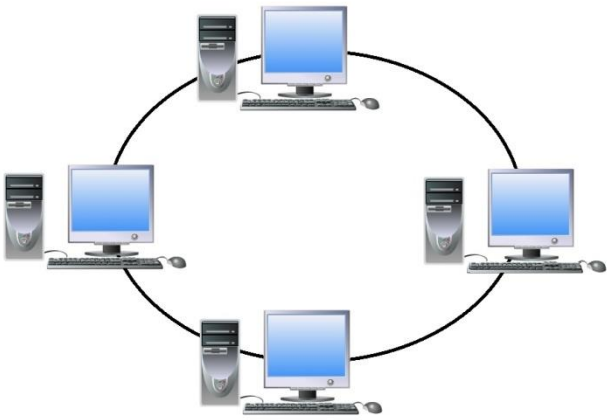


Рис. 6. Топология “кольцо”

Принимающая рабочая станция распознает и получает только адресованное ей сообщение. В сети с топологией типа физическое кольцо используется маркерный доступ, который предоставляет станции право на использование кольца в определенном порядке. Логическая топология данной сети - логическое кольцо.

Данную сеть очень легко создавать и настраивать. К основному недостатку сетей топологии кольцо является то, что повреждение линии связи в одном месте или отказ ПК приводит к неработоспособности всей сети. Как правило, в чистом виде топология “кольцо” не применяется из-за своей ненадёжности, поэтому на практике применяются различные модификации кольцевой топологии.

Топология Token Ring

Эта топология основана на топологии "физическое кольцо с подключением типа звезда". В данной топологии все рабочие станции подключаются к центральному концентратору (Token Ring) как в топологии физическая звезда. Центральный концентратор - это интеллектуальное устройство, которое с помощью перемычек обеспечивает последовательное соединение выхода одной станции со входом другой станции.

Другими словами с помощью концентратора каждая станция соединяется только с двумя другими станциями (предыдущей и последующей станциями). Таким образом, рабочие станции связаны петлей кабеля, по которой пакеты данных передаются от одной станции к другой и каждая станция ретранслирует

эти посланные пакеты. В каждой рабочей станции имеется для этого приемо-передающее устройство, которое позволяет управлять прохождением данных в сети. Физически такая сеть построена по типу топологии “звезда”. Концентратор создаёт первичное (основное) и резервное кольца. Если в основном кольце произойдёт обрыв, то его можно обойти, воспользовавшись резервным кольцом, так как используется четырёхжильный кабель. Отказ станции или обрыв линии связи рабочей станции не вличет за собой отказ сети как в топологии кольцо, потому что концентратор отключет неисправную станцию и замкнет кольцо передачи данных.

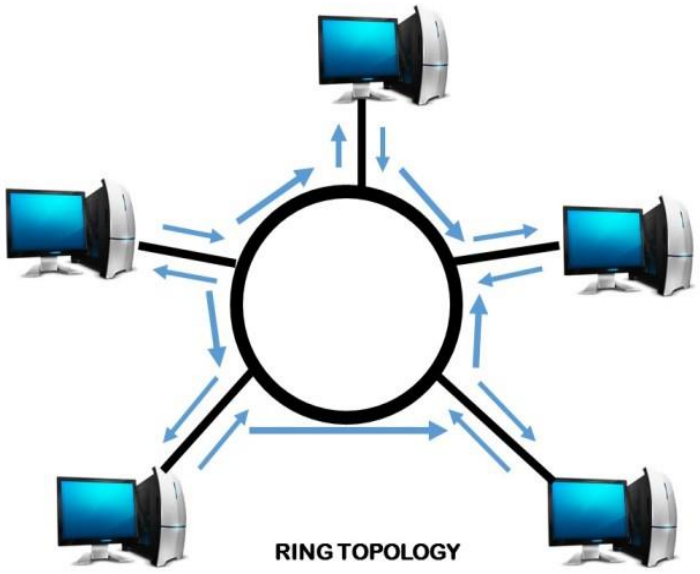


Рис. 7.

1.5 Анализ сетевого оборудования

При выборе активного сетевого оборудования в первую очередь необходимо обратить внимание на линейку продуктов, предоставляемых компанией D-Link, она является признанным мировым лидером в производстве сетевого оборудования, успешно работающим на глобальных рынках более 25 лет. Компания D-Link производит весь спектр оборудования для построения корпоративных сетей любого уровня, включая модульные коммутаторы уровня ядра, коммутаторы уровня предприятия для управления точками доступа.

Все оборудование, которое будет использоваться должно соответствовать международным стандартам и иметь сертификаты российских государственных органов в соответствии с действующим законодательством Российской Федерации.

Программное обеспечение активного сетевого оборудования, распространяемое на основе лицензий производителей, должно иметь соответствующие лицензии в необходимым количестве, приобретенные в установленном порядке.

Коммутаторы уровня ядра должны иметь:

- производительность, достаточную для осуществления своих функций
- высокую аппаратную надежность за счет возможности включения резервных системного модуля, источника питания и вентилятора
- возможность для конфигурирования оперативной и флэш-памяти разных объемов
- достаточное число интерфейсных модулей со слот-портами для подключения коммутаторов уровня распределения (с учетом их дублирования) и маршрутизаторов для выхода в смежные сети с возможностью использования трансиверов одномодового и многомодового оптоволокна
- не менее 2-х транковых портов для соединения коммутаторов между собой
- коммутацию 2-го и 3-го уровней модели OSI

Коммутаторы уровня распределения должны иметь:

- производительность, достаточную для осуществления своих функций
- высокую аппаратную надежность за счет возможности включения резервных системного модуля и источника питания
- возможность для конфигурирования оперативной и флэш-памяти разных объемов
- достаточное число интерфейсных модулей со слот-портами для подключения коммутаторов уровня доступа и уровня ядра (с учетом их

дублирования последних) с возможностью использования трансиверов одномодового и многомодового оптоволокна

- коммутацию 2-го и 3-го уровней модели OSI

Коммутаторы уровня доступа должны иметь:

- производительность, достаточную для осуществления своих функций
- достаточную аппаратную надежность за счет возможности включения источника питания (например, для этажных пунктов с расширенным числом пользователей)
- возможность для конфигурирования оперативной и флэш-памяти разных объемов
- достаточное число интерфейсных модулей с портами Ethernet / Fast Ethernet для подключения оконечных устройств пользователей и опционально слот-порты для подключения коммутаторов уровня распределения (с учетов дублирования последних) с возможностью использования трансиверов мультимодового оптоволокна
- коммутацию 2го уровня модели OSI (рекомендовано и 3го уровня).

1.5.1 Сетевые адаптеры.

Сетевая карта или сетевой адаптер - это плата расширения, вставляемая в разъем материнской платы компьютера, предназначенная для передачи сетевого сигнала.

Основные компоненты, необходимые для сетевого соединения:

- коннектор, соответствующий сетевой передающей среде;
- трансивер;
- контроллер, поддерживающий подуровень MAC канального уровня OSI;
- микропрограммное обеспечение.

Сетевые платы могут изготавливаться с несколькими разъемами, и поэтому могут использоваться с различными типами среды передачи данных.

Для каждого сетевого адаптера необходимы определенные сетевые драйверы, соответствующие методу доступа к сети, формату инкапсуляции

данных, типу кабельной системы и физической (MAC) адресации. В программных драйверах реализуются стандарты многоуровневых сетевых коммуникаций, заданные эталонной моделью OSI. Драйверы позволяют сетевому адаптеру выполнять передачу данных на Физическом (Уровень 1) и Канальном (Уровень 2) уровнях.

Сетевые адаптеры характеризуются:

- разрядностью: 16 бит, 32 бита и 64 бита;
- шиной данных, ISA, EISA, VL-Bus, PCI и др;
- поддерживаемой сетевой средой передачи;
- скоростью работы: Ethernet 10Mbit, Fast Ethernet 100Mbit, и т.д.;
- поддержка режима FullDuplex для витой пары;
- MAC адресом

В данном проекте необходимо использовать сетевые адаптеры поддерживающие сетевые технологии Fast Ethernet, Gigabit Ethernet.

1.5.2. Маршрутизаторы

Маршрутизатор (router) выполняет некоторые функции моста, такие как анализ топологии, фильтрация и пересылка пакетов. Однако, в отличие от мостов, маршрутизаторы могут направлять пакеты в конкретные сети, анализировать сетевой трафик и быстро адаптироваться к изменениям сети. Маршрутизаторы соединяют локальные сети на Сетевом уровне эталонной модели OSI, что позволяет им анализировать в пакетах больше информации, чем это возможно для мостов.

Главные задачи, которые могут решать маршрутизаторы:

- эффективно перенаправлять пакеты из одной сети в другую, устраняя ненужный трафик;
- соединять соседние или удаленные сети;
- связывать разнородные сети;
- устранять узкие места сети, изолируя ее отдельные части;
- защищать фрагменты сети от несанкционированного доступа.

В отличие от мостов, маршрутизаторы могут связывать сети, имеющие различные каналы данных. Например, сеть Ethernet на базе протокола TCP/IP можно подключить к коммутирующей сети с ретрансляцией кадров, в которой также используется протокол IP. Некоторые маршрутизаторы поддерживают только один протокол, например, TCP/IP или IPX. Многопротокольные маршрутизаторы могут выполнять преобразование протоколов разнородных сетей, т. е. осуществлять конвертацию протокола TCP/IP сети Ethernet в протокол AppleTalk сети с маркерным доступом, и наоборот.

Маршрутизаторы могут изолировать часть сети с высоким трафиком и распространять его на остальные участки сети. Эта способность маршрутизаторов позволяет предотвратить потерю производительности сети и возникновение широковещательного шторма. Рассмотрим для примера более загруженную лабораторную сеть, в которой студенты учатся сетевому администрированию. При этом учащиеся часто перенастраивают различные протоколы, серверы и сетевые устройства, создавая тем самым очень большой трафик. Кроме этого, в сети работают два преподавателя, которым нужен доступ к главной университетской сети.

По мере усложнения структуры сети растет необходимость передачи пакетов по самому короткому и наиболее эффективному маршруту. Чтобы обеспечить полный контроль над растущим сетевым трафиком и избежать падения производительности сети, вместо мостов часто используют маршрутизаторы. Кроме того, маршрутизаторы намного эффективнее мостов в случае объединения больших сетей. Однако при модернизации следует учитывать скорость обработки пакетов в маршрутизаторе в сравнении со скоростью обработки фреймов мостом. В принципе мост работает быстрее маршрутизатора, поскольку он не анализирует и не обрабатывает данные о маршрутизации. Чтобы компенсировать эти издержки, некоторые маршрутизаторы оснащаются специализированными процессорами, позволяющими сделать соразмерными эти скорости.

Многопротокольные маршрутизаторы могут выполнять преобразование протоколов разнородных сетей;

Маршрутизаторы получают от узлов регулярные сообщения, подтверждающие адреса узлов и их присутствие в сети.

Маршрутизаторы пересылают пакеты по маршрутам, где трафик самый маленький и для которых минимальна стоимость использования сетевых ресурсов.

Маршрут с наименьшей стоимостью определяется следующими факторами:

- расстоянием или длиной пути;
- нагрузкой в следующем пункте ретрансляции;
- имеющейся пропускной способностью;
- надежностью маршрута.

Программные средства маршрутизатора представляют один или несколько перечисленных факторов в виде единого параметра, называемого – метрикой.

Для вычисления метрики могут использоваться следующие величины в любых комбинациях:

- количество входящих пакетов, ожидающих обработки, на определенном порту;
- количество пакетов, которые маршрутизатор может обработать в течение определенного интервала времени;
- размер пакета;
- пропускная способность (скорость) между двумя взаимодействующими узлами;
- доступность (работоспособность) некоторого сегмента сети.

Основной функцией маршрутизатора является передача трафика по кратчайшему пути. Для этой цели используются разные способы маршрутизации:

Для статической маршрутизации необходимы таблицы маршрутизации, которые создает сетевой администратор. В них указываются фиксированные (статические) маршруты между любыми двумя маршрутизаторами.

Динамическая маршрутизация выполняется независимо от сетевого администратора.

Протоколы маршрутизации:

- Routing Information Protocol (RIP) – определяет число ретрансляций между маршрутизаторами;
- Open Shortest Path First (OSPF) – построение таблицы маршрутизации

1.5.3 Коммутаторы

Коммутаторы (switch) - обеспечивают функции моста, а также позволяют повысить пропускную способность существующих сетей.

Эффективным оказалось решение, которое и «породило» коммутаторы: для обслуживания потока, поступающего на каждый порт, в устройство ставился отдельный специализированный процессор, который реализовывал алгоритм моста.

В настоящее время в коммутаторах узел обмена строится на основе одной из трех схем:

- коммутационная матрица;
- общая шина;
- разделяемая многовходовая память.

Часто эти три схемы комбинируются в одном коммутаторе.

Коммутационная матрица обеспечивает наиболее простой способ взаимодействия процессоров портов, и именно этот способ был реализован в первом промышленном коммутаторе локальных сетей. Однако реализация матрицы возможна только для определенного числа портов, причем сложность схемы возрастает пропорционально квадрату количества портов.

В коммутаторах с общей шиной процессоры портов связывают высокоскоростной шиной, используемой в режиме разделения времени.

Чтобы шина не блокировала работу коммутатора, ее производительность должна равняться, по крайней мере, сумме производительностей всех портов коммутатора.

Для модульных коммутаторов характерно, что путем удачного подбора модулей с низкоскоростными портами можно обеспечить неблокирующий режим работы, и в то же время некоторые сочетания модулей с высокоскоростными портами могут приводить к структурам, у которых узким местом является общая шина.

Кадр должен передаваться по шине небольшими частями, по несколько байтов, чтобы передача кадров между портами происходила в псевдопараллельном режиме, не внося задержек в передачу кадра в целом.

Коммутаторы с разделяемой памятью

Входные блоки процессоров портов соединяются с переключаемым входом разделяемой памяти, а выходные блоки этих же процессоров — с ее переключаемым выходом. Переключением входа и выхода разделяемой памяти управляет менеджер очередей выходных портов. В разделяемой памяти менеджер организует несколько очередей данных, по одной для каждого выходного порта. Входные блоки процессоров передают менеджеру портов запросы на запись данных в очередь того порта, который соответствует адресу назначения кадра. Менеджер по очереди подключает вход памяти к одному из входных блоков процессоров, и тот переписывает часть данных кадра в очередь определенного выходного порта. По мере заполнения очередей менеджер производит также поочередное подключение выхода разделяемой памяти к выходным блокам процессоров портов, и данные из очереди переписываются в выходной буфер процессора.

Применение общей буферной памяти, гибко распределяемой менеджером между отдельными портами, снижает требования к размеру буферной памяти процессора порта. Однако она должна быть достаточно быстродействующей для поддержания необходимой скорости обмена данными между N портами коммутатора.

Существующие коммутаторы способны работать на 2 (канальном) и 3 (сетевом) уровнях модели OSI.

Коммутаторы 2-го уровня

При помощи коммутатора 2-го уровня можно достичь большей производительности. В этом случае входящий пакет переправляется только по одной выходной линии получающей станции. В то же самое время остальные линии могут использоваться для коммутации пакетов других станций. У коммутатора есть несколько привлекательных особенностей:

- Чтобы преобразовать локальную сеть с топологией общей шины или локальную сеть с хабом в коммутируемую локальную сеть, не требуется изменений программного или аппаратного обеспечения присоединенных устройств. В случае локальной сети, основанной на технологии FastEthernet каждое присоединенное устройство для доступа к локальной сети продолжает использовать протокол Ethernet управления доступом к несущей. С точки зрения присоединенного устройства в логике доступа ничего не меняется.
- У каждого присоединенного устройства есть выделенная пропускная способность, равная полной пропускной способности оригинальной локальной сети при условии, что у коммутатора 2-го уровня достаточно пропускной способности, чтобы поддерживать все присоединенные устройства. Например, если коммутатор 2-го уровня может поддерживать пропускную способность 200 Мбит/с, то у каждого присоединенного устройства и для приема, и для передачи как бы появляется выделенная линия с пропускной способностью в 100 Мбит/с.
- Коммутатор 2-го уровня легко масштабируется. Дополнительные устройства могут добавляться к коммутатору 2-го уровня при одновременном увеличении его мощности.

Два типа коммутаторов 2-го уровня распространяются на коммерческой основе.

- Коммутатор с промежуточным хранением (store-and-forward switch). Коммутатор 2-го уровня принимает кадр по входной линии, хранит его в буфере недолгое время, после чего направляет по соответствующей выходной линии.
- Сквозной коммутатор (cut-through switch). Коммутатор 2-го уровня пользуется тем преимуществом, что адрес получателя помещается в начале кадра MAC (Medium Access Control — управление доступом к носителю). Коммутатор

2-го уровня начинает передавать принимаемый кадр по нужной выходной линии, как только коммутатор 2-го уровня распознает адрес получателя.

Сквозной коммутатор позволяет достичь максимально возможной пропускной способности, но при этом рискуя передать неверный кадр, так как он не может проверить контрольную сумму перед передачей. Коммутатор с промежуточным хранением вносит задержку во взаимодействие между отправителем и получателем, но зато повышает общую целостность сети.

Поскольку коммутатор 2-го уровня обладает более высокой производительностью и может выполнять функции моста, на коммерческом рынке мосты потерпели поражение. В новых сетях, как правило, используются коммутаторы 2-го уровня, обладающие функциональностью мостов.

Коммутаторы 3-го уровня

Коммутаторы 2-го уровня обеспечивают более высокую производительность, удовлетворяя потребности в транспортировке трафика больших объемов, формируемого персональными компьютерами, рабочими станциями и серверами. Однако по мере того, как количество подключенных к сети устройств в здании или комплексе зданий растет, коммутаторы 2-го уровня перестают справляться со своей задачей. В частности, возникают две проблемы: широковещательная перегрузка и недостаток линий связи.

Считается, что у множества устройств и локальных сетей, соединенных коммутаторами 2-го уровня, адресное пространство плоское. Термин плоское (flat) означает, что все пользователи имеют общий широковещательный адрес MAC. Таким образом, если любое устройство отправляет кадр MAC с широковещательным адресом, этот кадр должен быть доставлен всем устройствам сети, объединенной при помощи коммутаторов 2-го уровня и/или мостов. В большой сети частая передача широковещательных кадров может вызвать огромную перегрузку. Что еще хуже, неисправное устройство способно создать широковещательный шторм (broadcast storm), при котором многочисленные широковещательные кадры заполоняют сеть и вытесняют остальной трафик.

Вторая проблема, связанная с производительностью и относящаяся к

использованию мостов и/или коммутаторов 2-го уровня, заключается в том, что современными стандартами для протоколов мостов предписывается отсутствие замкнутых контуров в сети. То есть между любыми двумя устройствами может существовать только один путь. Таким образом, оказывается невозможным соединить два устройства несколькими путями через несколько коммутаторов. Такое ограничение негативно влияет как на производительность, так и на надежность.

Для решения этих проблем кажется логичным разбить большую локальную сеть на несколько подсетей (subnetworks), соединенных маршрутизаторами. При этом широковещательный кадр MAC доставляется только в пределах своей подсети. Кроме того, IP-маршрутизаторами применяются сложные алгоритмы маршрутизации, позволяющие использовать между подсетями несколько путей, проходящих через разные маршрутизаторы.

Однако недостаток использования маршрутизаторов вместо мостов и коммутаторов 2-го уровня состоит в том, что маршрутизаторы, как правило, выполняют всю обработку IP-уровня программно. Высокоскоростные локальные сети и высокопроизводительные коммутаторы 2-го уровня могут пропускать миллионы пакетов в секунду, тогда как пропускная способность работающих программно маршрутизаторов значительно ниже миллиона пакетов в секунду. Для решения этой проблемы производители разработали коммутаторы 3-го уровня, в которых логика маршрутизации пакетов реализована аппаратно.

Сегодня на рынке представлено несколько схем коммутаторов 3-го уровня, но фундаментально они распадаются на две категории: пакетный коммутатор и потоковый коммутатор. Пакетный коммутатор (packet-by-packet switch) работает так же, как традиционный маршрутизатор. Поскольку логика маршрутизации пакетного коммутатора реализована аппаратно, с его помощью производительность может быть увеличена на порядок по сравнению с использованием программного маршрутизатора. Потоковый коммутатор (flow-based switch) пытается увеличить производительность, идентифицируя потоки IP-пакетов с одними и теми же отправителем и получателем. Это может быть

реализовано путем наблюдения за проходящим через коммутатор трафиком, а также с помощью специальной метки потока в заголовке пакета. Когда поток идентифицирован, может быть выбран заранее установленный маршрут, чтобы ускорить процесс доставки пакета. При помощи этого метода также можно достичь многократного увеличения производительности по сравнению с использованием программного маршрутизатора.

В отличие от традиционных маршрутизаторов, которые определяют конкретную подсеть только для одного порта, коммутаторы третьего уровня позволяют выделить в отдельную подсеть каждый порт коммутатора. Маршрутизация в коммутаторах третьего уровня осуществляется над уровнем коммутации, что обеспечивает более гибкую и масштабируемую сетевую архитектуру.

Коммутаторы 3-го уровня формируют локальную магистраль. Как правило, эти коммутаторы связаны друг с другом линиями с пропускной способностью 1 Гбит/с, а с коммутаторами 2-го уровня — линиями, работающими на скорости от 100 Мбит/с до 1 Гбит/с. Серверы соединяются напрямую с коммутаторами 2-го или 3-го уровня линиями с пропускной способностью 10 Гбит/с, 1 Гбит/с или 100 Мбит/с. Программный маршрутизатор обеспечивает соединение с глобальной сетью.[5]

1.5.4. Серверы

Сервер - аппаратное обеспечение, необходимое для выполнения на нём сервисного программного обеспечения (в том числе серверов тех или иных задач).

FTP-сервер

FTP-сервер – это удаленный компьютер, с файловой системой которого можно работать через специальный одноименный протокол.

Протокол FTP – один из стандартных протоколов передачи данных через Интернет, он позволяет переносить файлы с одного компьютера на другой. Чтобы установить соединение и обменяться файлами в Интернете, согласно протоколу FTP, необходимо запустить специальную прикладную программу, так

называемую клиентскую часть FTP. Клиентское программное обеспечение устанавливается вместе с коммуникационными утилитами TCP/IP. Получить доступ к другому компьютеру для обмена файлами можно, указав пользовательское имя и пароль.

Почтовый сервер

Почтовый сервер — в системе пересылки электронной почты так обычно называют агент пересылки сообщений. Это компьютерная программа, которая передаёт сообщения от одного компьютера к другому. Обычно почтовый сервер работает «за кулисами», а пользователи имеют дело с другой программой — клиентом электронной почты (программное обеспечение, устанавливаемое на компьютере пользователя и предназначенное для получения, написания, отправки и хранения сообщений электронной почты одного или нескольких пользователей).

Прокси-сервер

Прокси-сервер — служба (комплекс программ) в компьютерных сетях, позволяющая клиентам выполнять косвенные запросы к другим сетевым службам. Сначала клиент подключается к прокси-серверу и запрашивает какой-либо ресурс (например, e-mail), расположенный на другом сервере. Затем прокси-сервер либо подключается к указанному серверу и получает ресурс у него, либо возвращает ресурс из собственного кэша (в случаях, если прокси имеет свой кэш). В некоторых случаях запрос клиента или ответ сервера может быть изменён прокси-сервером в определённых целях. Также прокси-сервер позволяет защищать клиентский компьютер от некоторых сетевых атак и помогает сохранять анонимность клиента.

Виды серверов:

- **Прозрачный прокси** — схема связи, при которой трафик, или его часть, перенаправляется на прокси-сервер неявно (средствами маршрутизатора). При этом клиент может использовать все преимущества прокси-сервера без дополнительных настроек браузера (или другого приложения для работы с интернет).
- **Обратный прокси** — прокси-сервер, который в отличие от прямого,

ретранслирует запросы клиентов из внешней сети на один или несколько серверов, логически расположенных во внутренней сети. Часто используется для балансировки сетевой нагрузки между несколькими веб-серверами и повышения их безопасности, играя при этом роль межсетевого экрана на прикладном уровне.

Применение прокси-серверов:

- Обеспечение доступа с компьютеров локальной сети в Интернет.
- Кэширование данных: если часто происходят обращения к одним и тем же внешним ресурсам, то можно держать их копию на прокси-сервере и выдавать по запросу, снижая тем самым нагрузку на канал во внешнюю сеть и ускоряя получение клиентом запрошенной информации.
- Сжатие данных: прокси-сервер загружает информацию из Интернета и передаёт информацию конечному пользователю в сжатом виде. Такие прокси-серверы используются в основном с целью экономии внешнего трафика клиента или внутреннего — компании, в которой установлен прокси-сервер.
- Защита локальной сети от внешнего доступа: например, можно настроить прокси-сервер так, что локальные компьютеры будут обращаться к внешним ресурсам только через него, а внешние компьютеры не смогут обращаться к локальным вообще (они «видят» только прокси-сервер).
- Ограничение доступа из локальной сети к внешней: например, можно запретить доступ к определённым веб-сайтам, ограничить использование интернета каким-то локальным пользователям, устанавливать квоты на трафик или полосу пропускания, фильтровать рекламу и вирусы.
- Анонимизация доступа к различным ресурсам. Прокси-сервер может скрывать сведения об источнике запроса или пользователе. В таком случае целевой сервер видит лишь информацию о прокси-сервере, например, IP-адрес, но не имеет возможности определить истинный источник запроса
- Обход ограничений доступа. Прокси-серверы популярны среди пользователей несвободных стран, где доступ к некоторым ресурсам ограничен законодательно и фильтруется.

Веб-сервер

Веб-сервер — это сервер, принимающий HTTP-запросы от клиентов, обычно веб-браузеров, и выдающий им HTTP-ответы, обычно вместе с HTML-страницей, изображением, файлом, медиа-потоком или другими данными.

Веб-сервером называют как программное обеспечение, выполняющее функции веб-сервера, так и непосредственно компьютер, на котором это программное обеспечение работает.

Функции веб-сервера:

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

1.6 Цель и задачи курсовой работы.

Целью данной курсовой работы является проектирование высокоскоростной компьютерной сети для реализации автоматизированной системы обработки информации и управления ЗАО "Талисман Центр" с использованием технологий Fast и Gigabit Ethernet.

Задачами данной курсовой работы являются:

- Проанализировать организационную структуру учреждения
- Провести исследование информационных потоков на предприятии
- Выбрать архитектуру сети
- Выбрать технологию сети
- Рассмотреть вопросы обеспечения безопасности сети
- Выбрать необходимое оборудование ИС
- Выполнить расчет стоимости сети компьютерной сети

2. Специальный раздел

2.1. Проектирование высокоскоростной компьютерной сети

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.[12]

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.

2.1.1. Уровень ядра

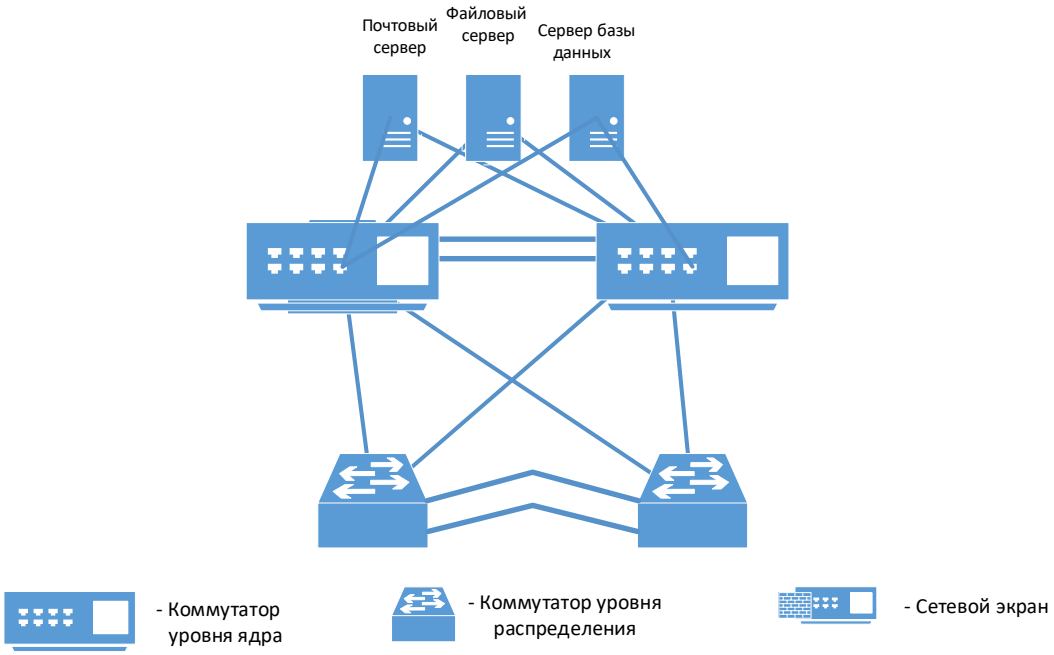


Рис. 5. Ядро сети

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, что может 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.

2.1.2. Узел резервирования

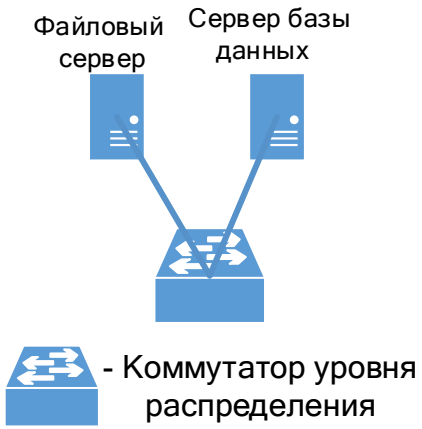


Рис. 6. Узел резервирования

– Бэкап сервер позволит обеспечить резервное копирование сохранить критические данные серверов в случае выхода их из строя, в случае случайной потери данных вследствии 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 дискового пространства и высокая скорость записи и чтения данных.

2.1.3. Уровень распределения

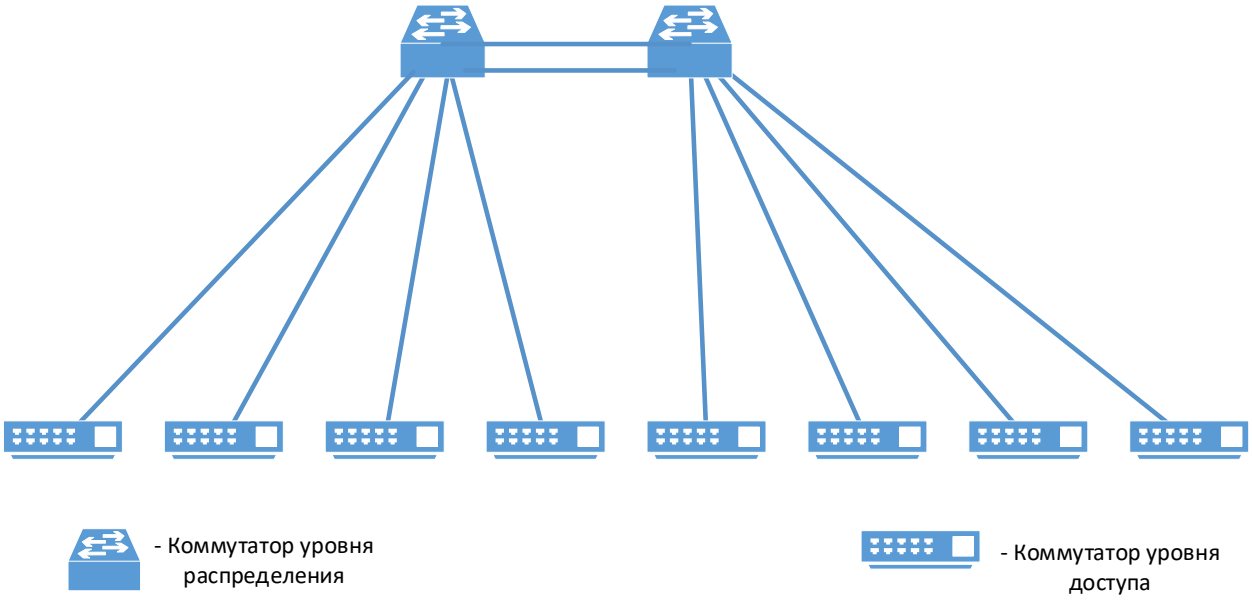


Рис. 7. Уровень распределения

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 наилучшего пути 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 или механизму запросов.

• Реализация системы безопасности и сетевых политик, включая трансляцию адресов и установку брандмауэров.

• Перераспределение между протоколами маршрутизации, включая использование статических путей.

• Маршрутизация между сетями VLAN и другие функции поддержки рабочих групп.

• Определение доменов широковещательных и многоадресных рассылок.

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.

2.1.4. Уровень доступа

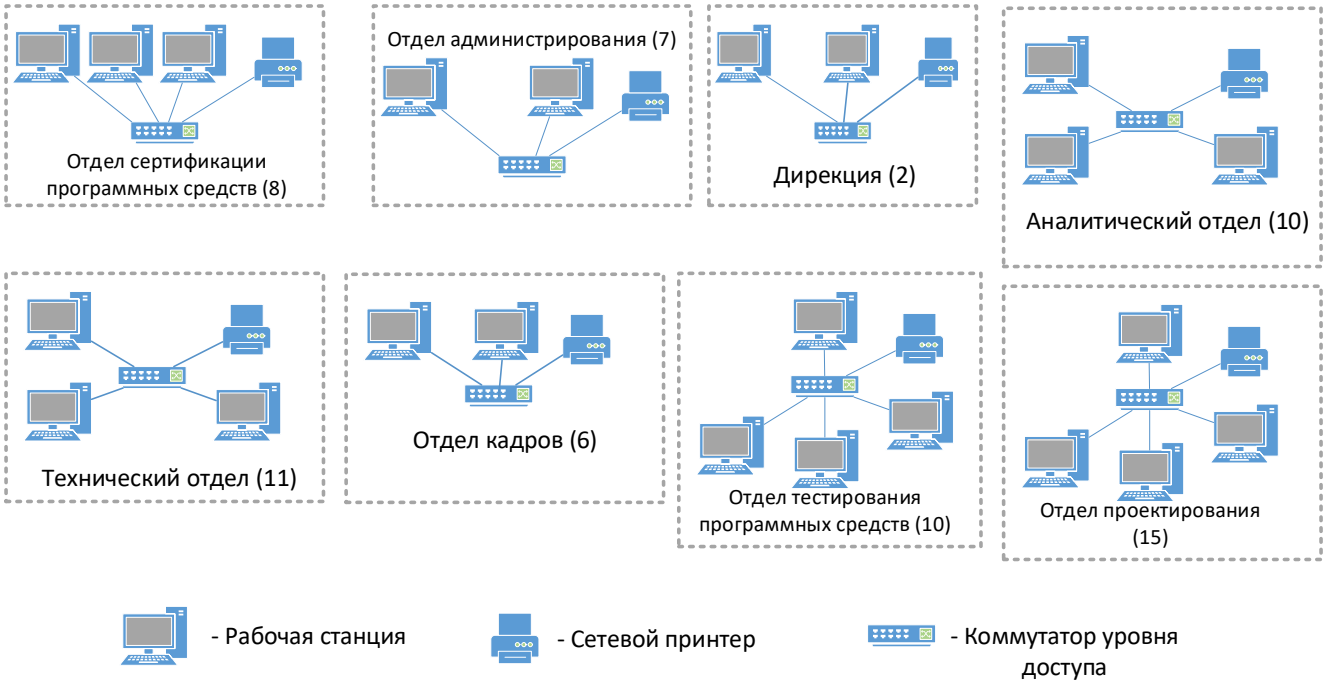


Рис. 8. Уровень доступа

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 подключены к коммутаторам уровня распределения каналами связи со скоростью до 1000 Мбит/сек. К коммутаторам уровня доступа подключены рабочие станции, скорость передачи данных 100 Мбит/сек.

2.1.5. Подключение к сети Интернет

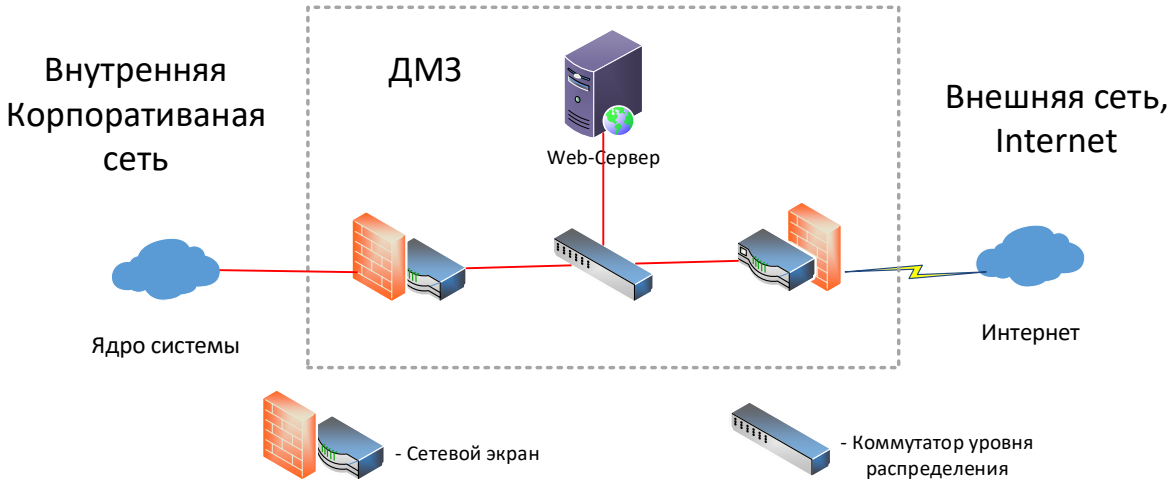


Рис. 9. Подключение к сети Интернет

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.

2.2. Обеспечение безопасности сети. Демилитаризованная зона

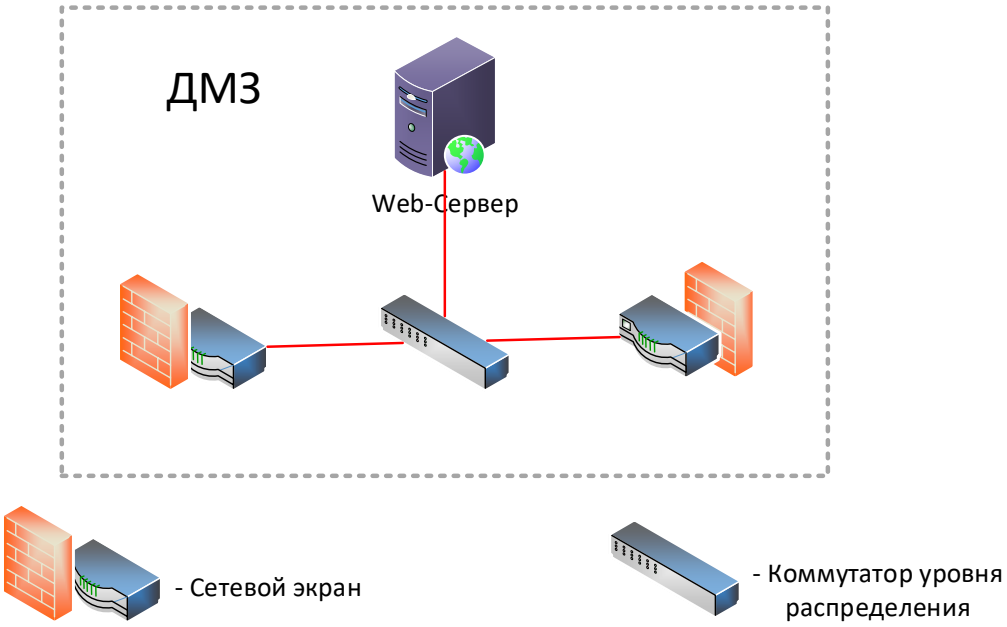


Рис. 10. Демилитаризованная зона

Администрация предприятия 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 предприятия, 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 авторизации пользователей;

- 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, компьютеров и 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.

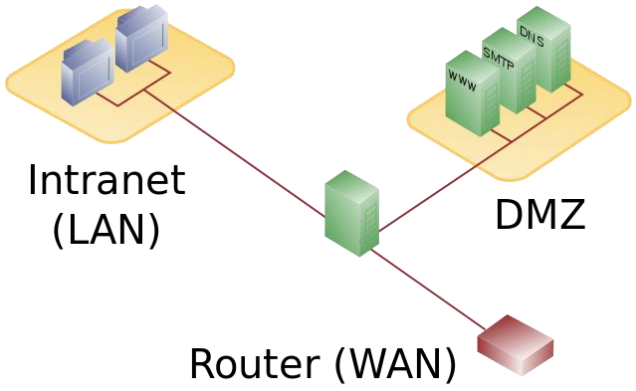


Рис. 11. Схема с одним межсетевым экраном

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.

2.3. Выбор оборудования

Сервер:
Сервер MicroXperts [ZX24-03]

Рис.12. 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.

Коммутатор уровень ядра:

Коммутатор D-link DGS-3612

Рис.13. Коммутатор D-link DGS-3612

Тип устройства - коммутатор (switch)

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.

Коммутатор уровня доступа на 24 порта:

Коммутатор D-link DGS-1024C

Рис.14. Коммутатор D-link DGS-1024C

Тип устройства - коммутатор (switch)

Интерфейсы	24 порта 10/100/1000Base-TX
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: 5 250 руб.

Коммутатор уровня распределения на 16 портов [8]:

Коммутатор D-link DGS-1016C

Рис. 15. Коммутатор D-link DGS-1016C

Тип устройства коммутатор - (switch)

Интерфейсы	16 портов 10/100/1000Base-T
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: 1 999 руб.

Принтер:

Kyocera FS-106

Рис.16. Kyocera FS-106

Устройство - принтер

Максимальный формат - A4

Объем памяти - 32 Мб

Процессор - ARM

Частота процессора - 390 МГц

Интерфейсы - Ethernet (RJ-45), USB 2.0

Поддержка - ОС Windows, Mac OS

Потребляемая мощность (при работе) - 346 Вт

Цена: 3600 руб.

Рабочая станция:

Компьютер моноблок MicroXperts [M500-06] W7HB

Рис.17. Моноблок MicroXperts [M500-06] W7HB

Производитель - MicroXperts

Операционная система - MS Windows 7 Home Basic

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: 39790 руб.

Серверный шкаф:

Серверный шкаф 19" 9U RackPro DW6609 (600x600x500)

Рис.18. Серверный шкаф 19" 9U RackPro DW6609 (600x600x500)

Высота - 9U

Ширина - 600 мм, глубина: 610 мм

Высота реальная - ~510 мм

Для размещения оборудования стандарта - 19" RACKMOUNT

Статическая нагрузка: до 60 кг

Цена: 11630 руб.

Межсетевой экран:

Межсетевой экран D-Link UTM Net Defend 1 10/100/1000WAN, 5 10/100/1000LAN, DMZ 10/100/1000Mpbs, DFL-260E/A1N

Рис.19. Межсетевой экран D-Link UTM Net Defend

Производитель	D-Link
Гарантия	12
Пропускная способность IPS	60 Мбит/с

Максимальное количество одновременных сессий	25000
Количество новых сессий в сек.	2000
Сетевые интерфейсы	1 x 10/100/1000 WAN, 1 x 10/100/1000 DMZ, 5 x 10/100/1000

Цена: 19 560 руб.

2.4. Расчет стоимости

Название оборудования	Фирма	Кол-во	Цена, руб.	Итого, руб.
Коммутаторы				
DGS-3612	D-Link	2	70 807	141 614
DGS-1024C	D-Link	3	5 250	15 750
DGS-1016C	D-Link	9	1 999	17 991
Серверное оборудование				
MicroXperts [ZX24-03]	MicroXperts	6	78 870	473 220
Сетевое оборудование и комплектующие				
19" 9U DW6609 (600x600x500)	RackPro	2	11 630	23260
UTM Net Defend	D-Link	2	19 560	39120
Оргтехника				
[M500-06]W7HB	MicroXperts	69	39790	2 745 510
Kyocera FS-106	Samsung	10	3600	36000
				3 492 465 руб.

3. Заключение

В данной проекте была спроектирована высокоскоростная компьютерная сеть для реализации управления в учреждении ЗАО "Испытательный сертификационный центр безопасности программных средств вычислительной техники – Талисман Центр", для чего был решен класс задач:

- Проанализирована организационная структура учреждения
- Проведено исследование информационных потоков в организации
- Выбрана архитектура сети
- Выбрана технология и к ресурсам сети
- Рассмотрены вопросы обеспечения безопасности сети
- Выбрано необходимое оборудование компьютерной сети
- Выполнен расчет стоимости сети

В итоге спроектированная компьютерная сеть:

- Высокоскоростная
- Использует современные технологии и оборудования
- Обеспечивает высокий уровень безопасности
- Прозрачна и легко расширяема
- Соответствует современным стандартам

4. Список использованной литературы

1. Лекция Проектирование высокоскоростной компьютерной сети. Технология Gigabit Ethernet [Электронный ресурс] – Профессор В.А. Григорьев
2. Лекция по дисциплине “Вычислительные машины, системы и сети” - https://studfiles.net/preview/948133/ - [Электронный ресурс],
3. Олифер В. Г., Олифер Н. А. Компьютерные сети: принципы, технологии, протоколы. – Учебник для ВУЗов, СПб.: 2004. – 864 с.
4. Слепов Н. Сети SDH новой генерации и их использование для передачи трафика Ethernet. – ЭЛЕКТРОНИКА: НТБ, 2005, №3, с.62; №4, с.
5. Технология Ethernet. – В кн.: Руководство по технологиям объединенных сетей. 3-е изд. – М., С.–Пб., К.: Изд. дом "Вильямс", 2002.
6. https://www.dnsshop.ru/product/f9fc0223e1063330/kommutator-d-link-dgs-1024ca1a/ [Интернет магазин DNS]
7. https://www.dns-shop.ru/product/66a0246df0018a5a/kommutator-d-link-des-1016c/ [Интернет магазин DNS]
8. https://www.computermarket.ru/main/catalog/catid/1163571.aspx [Интернет магазин Computer Market]
9. https://www.ulmart.ru/goods/4105874 [Интернет магазин Юлмарт]
10. https://www.computermarket.ru/main/catalog/catid/1132184.aspx [Интернет магазин Computer Market]
11. http://www.diatron.ru/index.php?productID=3795&ukey=product&did=34&view=printable [Электронный ресурс]
12. Понуренко Л. А. Проектирование двух кампусных сетей, соединённых оптоволоконным каналом: Авторефат .-М., 2007.-7с.

5. Приложения:

Приложение 1. Физическая схема сети

Приложение 2. Горизонтальная разводка

Приложение 3. Моделирование компьютерной сети предприятия в среде Cisco PacketTracer.

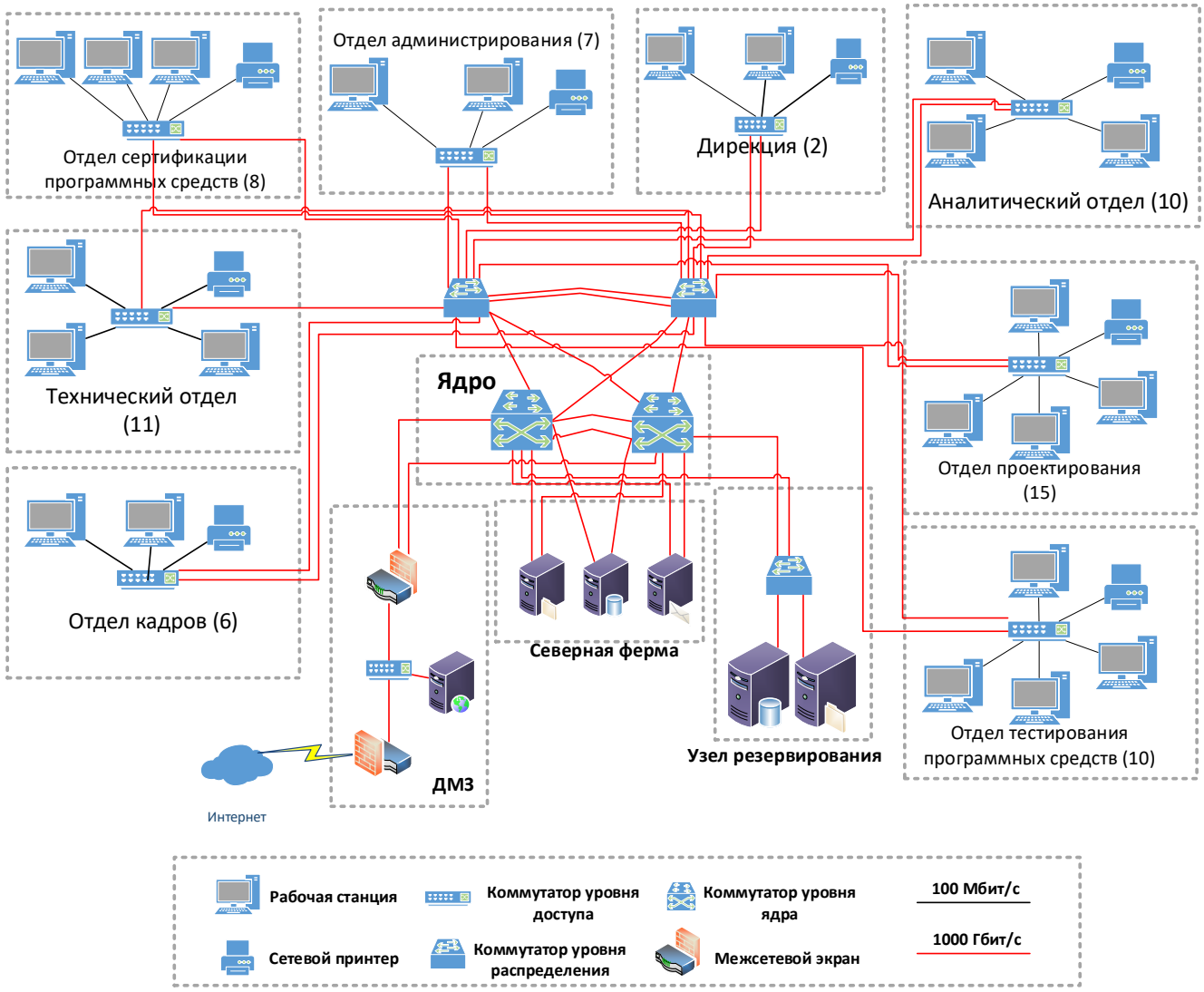


Рис.20. Физическая схема сети

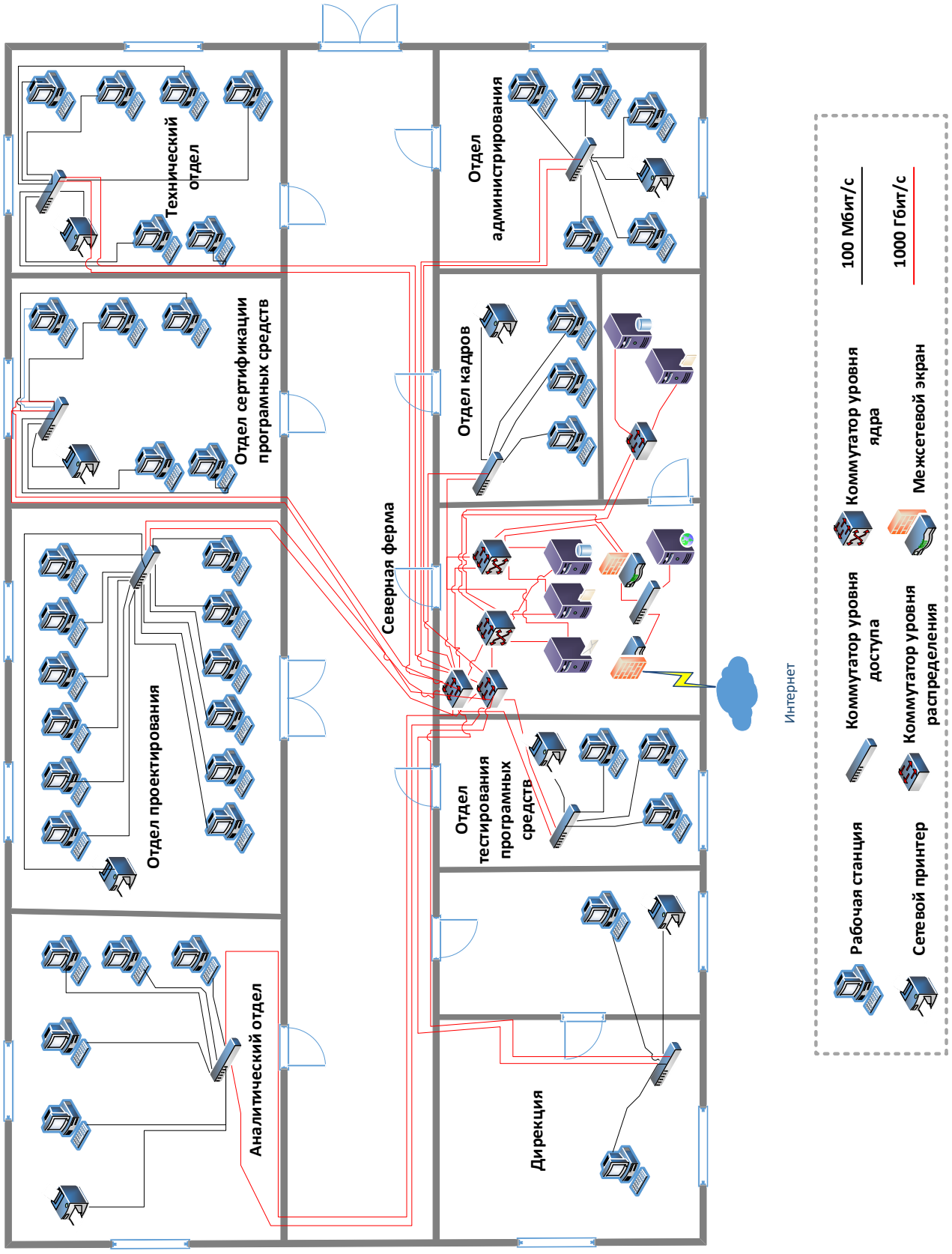


Рис.21. Горизонтальная разводка сети

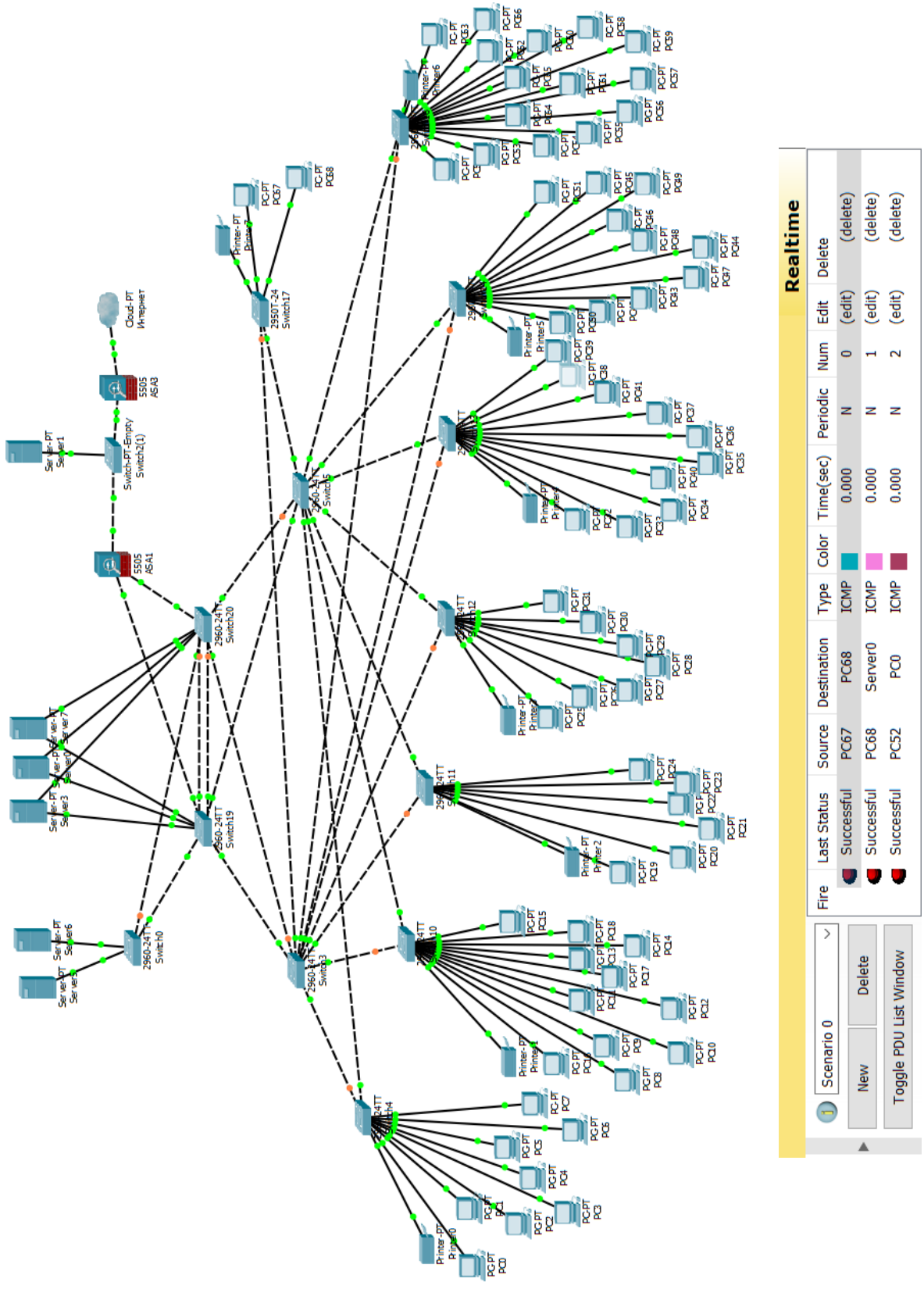


Рис.22. Моделирование компьютерной сети предприятия в среде Cisco PacketTracer.