Кафедра Информационно-коммуникационных технологий

**ПОЯСНИТЕЛЬНАЯ ЗАПИСКА**

к дипломной работе

На тему: «Реорганизация схемы управления и оптимизация сегмента сети передачи данных »

##

Москва, 2009 год

**Аннотация**

В данной работе была модернизирована домовая локальная вычислительная сеть. Модернизация проводилась на функционирующем оборудовании.

# Техническое задание

Модернизировать сеть передачи данных на основе имеющегося оборудования с минимизацией материальных затрат.

## **Список использованных сокращений**

CSMA/CD – метод множественного доступ с обнаружением несущей и обнаружением коллизий;

LLC – управление логической связью;

AUI – интерфейс устройства доступа к среде передачи;

MII – интерфейс независимый от среды (Fast Ethernet);

TTL – время жизни пакета;

PHY – устройство физического уровня (Fast Ethernet);

NLP – импульсные посылки контроля линии;

SM – одномодовое волокно;

STP – экранированная витая пара;

UTP – неэкранированная витая пара;

MSAU – многостанционное устройство доступа;

VLAN – виртуальная LAN. Широковещательный домен.

NIC – интерфейсная карта;

WI –Fi – спецификация оборудования для беспроводного доступа к локальным сетям общего пользования;

IP – Интернет протокол;

LAN – локальная сеть доступа;

MAC – канальный уровень;

QoS – уровень поддержки требуемого качества передачи информации;

CoS – общая поддержка требуемого качества передачи информации;

TCP – протокол контроля передачи;

WAN – глобальная сеть;

MAU –многостанционное устройство доступа;

GVRP – протокол обеспечивающий сервис регистрации VLAN;

CPU – Центральный процессор;

RAM – Оперативная память;

USB – Универсальный последовательный интерфейс;

SATA – последовательный интерфейс жесткого диска;

SCSI – высокоскоростной интерфейс жесткого диска;

UPS – источник бесперебойного питания;

UDP – протокол передачи дейтаграмм;

DHCP – протокол динамического конфигурирования хостов;

ICMP – протокол управляющих сообщений Интернет;

IGMP - протокол управления группами Интернет;

ACL – список прав доступа;

SSL – протокол конфиденциальной передачи в протоколе TCP/IP;

SNMP – протокол управления сетевыми ресурсами;

iSCSI – протокол осуществляет контроль передачи блоков данных;

VPN – частная виртуальная сеть;

xDSL - цифровая абонентская линия;

PPP – протокол точка-точка;

VoIP – IP телефония;

DoS/DDos - распределённый отказ в обслуживании;

ЛВС – локальная вычислительная сеть;

КПК – карманный персональный компьютер;

BRAS (broadband remote access server) - маршрутизатор широкополосного удалённого доступа, служит для маршрутизации трафика к/от пользователей. BRAS находится в ядре сети провайдера и агрегирует пользовательские подключения из сети уровня доступа

DHCP (Dynamic Host Configuration Protocol) – протокол динамической конфигурации узла.

DHCP-ретранслятор – узел в сети, который перенаправляет DHCP-запрос на указанный в его настройках централизованный DHCP-сервер.

DHCP-discover – запрос к DHCP-серверу от оконечного сетевого оборудования с целью обнаружить себя в сети и получить необходимые сетевые параметры для работы.

DHCP-offer – ответ от DHCP-сервера.

DHCP-snooping – функция коммутатора, предназначенная для защиты от атак с использованием протокола DHCP.

У-1 – коммутатор DXS-3326GSR уровня распределения находящиеся на первом уровне древообразной топологии сети (Узел первого уровня)

У-2 - коммутатор DXS-3326GSR уровня распределения находящиеся на втором уровне древообразной топологии сети (Узел второго уровня)

ТКД - коммутатор DES-3526 уровня доступа сети (Точка коммуникативного доступа)

Сегмент – сегмент сети включающий У-2 и все подключенные к нему ТКД

Район - сегмент сети, включающий У-1 и все коммутаторы, подключенные от него.

border - edge-маршрутизатор магистральной сети

Локальные ресурсы – ресурсы компании, предоставляющиеся без подключения к VPN-серверу

# Общая часть

## **Обзор и анализ современных существующих локальных вычислительных сетей**

На сегодняшний день существует множество сетевых технологий передачи данных. Сферы применения этих технологий различны. Начиная от малых локальных вычислительных сетей заканчивая общегородскими и глобальными мировыми сетями.

Существуют следующие основные современные стандарты локальных сетей:

1. Ethernet;
2. Fast Ethernet, Gigabit Ethernet
3. Wi-Fi (Wireless Fidetly);
4. WiMAX (Worldwide Interoperability for Microwave Access);
5. **Ethernet**

Ветераном сетевых технологий (архитектур) является Ethernet— эта спецификация была предложена фирмами DEC, Intel и Xerox в 1980 году и несколько позже на ее основе появился стандарт IEEE 802.3. По первым буквам названий них фирм образовано сокращение DIX, фигурирующее в описаниях этой технологии. Слово Ether (эфир) в названии технологии обозначает многообразие возможных сред передачи. Первые версии — Ethernet v1.0 и Ethernet v2.0 предназначались только для коаксиального кабеля, стандарт IEEE 802.3 рассматривает и иные варианты среды передачи — витую пару и оптоволокно. Сейчас под названием Ethernet подразумевают стандарт IEEE 802.3 (скорость 10 Мбит/с). В 1995 году был принят стандарт IEEE 802.3u — Fast Ethernet со скоростью 100 Мбит/с, а в 1997 году IEEE 802.3z - Gigabit Ethernet (1000 Мбит/с). Осенью 1999 года принят стандарт IEEE 802.3a/b — Gigabit Ethernet на витой паре категории 5, позже была анонсирован 10GBit Ethernet (10000 Мбит/с). Популярные разновидности Ethernet обозначаются как 100BaseTX и др. Здесь первый элемент обозначает скорость передачи, Мбит/с.

Второй элемент: Base — прямая (немодулированная) передача, Broad — использование широкополосного кабеля с частотным уплотнением каналов. Третий элемент: среда передачи (T, ТХ, Т2, Т4 — витые пары, FX, FL, FB, SX и IX — оптоволокно, СХ — твинаксиальный кабель для Gigabit Ethernet).

Технология Ethernet основана на методе множественного доступа к среде передачи с прослушиванием несущей и обнаружением коллизий — CSMA/CD. Суть этого метода применительно к «классической» версии Ethernet (10 Мбит/с на коаксиальном кабеле) и рассмотрим более поздние вариации. Возможная схема локальной сети показана на рисунке 1.1.

PC 3

PC 2

PC 1

PC 4

PC 7

PC 6

PC 5

Рисунок 1.1 - Пример сети Ethernet

1. **Fast Ethernet 100 Мбит/с**

Варианты Fast Ethernet со скоростью передачи данных 100 Мбит/с описываются стандартом IEEE 802.3u — дополнительными главами 802.3, принятыми в 1995 году. Они основаны на том же методе доступа CSMA/CD с сохранением форматов кадров. При этом все соотношения, измеренные в битовых интервалах, сохраняются. Поскольку длительность битового интервала сократилась в 10 раз, максимально допустимое время прохождения между двумя узлами сократилось до 2,6 мкс, что привело к ужесточению топологических ограничений. Все разновидности используют звездообразную топологию с активным устройством в центре, возможно и непосредственное соединение пары станций.

Стандарт 802.3u опирается на те же уровни MAC и LLC, которые были определены в исходном 802.3; изменения касаются физического уровня. Физический Уровень является трехслойным:

• Reconciliation sublayer — уровень согласования с МАС-уровнем 802.3, ориентированным на АUI-интерфейс;

• MII (Media Independent Interface) — электрический интерфейс, независимый от среды передачи. Представляет собой спецификацию сигналов TTL-уровня, использует 40-контактный штырьковый разъем. По идее он напоминает интерфейс AUI, но располагается на другом уровне. Длина кабеля МII не должна превышать 0,5 м. Наличие доступного интерфейса МII не является обязательным;

• PHY (Physical layer device) — устройство физического уровня, привязанное к конкретной среде передачи (100BaseTX, 100BaseFX или 100BaseT4).

Устройство физического уровня выполняет логическое кодирование — преобразование 4В/5В или 6В/8Т, физическое кодирование и присоединение к среде передачи, и необязательно — автоматическое согласование режимов передачи. Физический уровень в 100BaseTX и 100BaseFX позаимствован из технологии FDDI, в 100BaseT4 применена оригинальная разработка.

100BaseTX — наиболее популярная версия Fast Ethernet, использующая две витые пары категории 5. По использованию разъемов полностью соответствует 10BaseT. Возможна работа в полудуплексном и полнодуплексном режимах. Логическое кодирование производится по схеме 4В/5В — 4 бита исходной информации преобразуются в 5-битный символ. Избыточность используется для повышения достоверности и служебных целей. Метод физического кодирования MLT-3 заимствован из TP-PMD — «медной» реализации FDDI. В паузе между кадрами в линию посылается последовательности символов Idle.

100BaseT4 — версия, использующая 4 витых пары категории не ниже 3. Кроме однонаправленных пар, используемых в 100BaseTX, здесь две дополнительные пары являются двунаправленными и служат для распараллеливания передачи данных. Кадр передается по трем линиям параллельно, что позволяет снизить пропускную способность каждой пары до 33,3 Мбит/с. Каждые 8 бит (двоичных разрядов — Binary), передаваемые по конкретной паре, кодируются шестью троичными (Ternary) цифрами (кодирование 8В/6Т). В результате при битовой скорости 33,3 Мбит/с скорость изменения сигналов в линии составляет 25 Мбод (33,3x6/8=25). Эти меры позволяют сузить необходимую полосу пропускания кабеля до требований категории 3 (16 МГц). Четвертая пара при передаче используется для прослушивания сигнала от противоположного передатчика — по его появлению определяется факт коллизии. Для подключения конечных узлов к портам активного оборудования используется «прямой» кабель, для непосредственного соединения конечных узлов или соединения двух коммуникационных устройств применяют «перекрестный» кабель.

Для приведенных выше реализаций предусмотрен протокол согласования режимов (autonegotiation), по которому порт может выбрать самый эффективный из режимов, доступных обоим участникам обмена. Согласование осуществляется путем обмена посылками FLP (Fast Link Pulse), которые являются признаком исправной активной линии (аналогично NLP 10BaseT). В отличие от одиночных импульсов NLP, импульсы FLP идут пачкой. Различают синхронизирующие и сигнальные импульсы FLP. Сигнальные импульсы могут вставляться между синхронизирующими, идущими пачкой по 17 штук. Места между этими импульсами отводятся под кодирование 16-битного слова: наличие сигнального соответствует единичному биту, отсутствие - нулевому. Слово несет информацию о доступных режимах. Первый узел предлагает самый эффективный режим, кодируя его в посылке FLP. Приемник на эту посылку отвечает аналогичной, в которой кодирует свои возможности. В качестве рабочего выбирается самый приоритетный из доступных обоим узлам. Приоритеты режимов в порядке убывания: 100BaseTX полнодуплексный, 100BaseT4, 100BaseTX полудуплексный, 10BaseT полнодуплексный, 10BaseT полудуплексный. Если второй узел имеет порт 10BaseT, «не понимающий» FLP и посылающий NLP, будет принят протокол 10BaseT. Протокол автоматического согласования может быть отключен (или не реализован), в этом случае режим работы задается принудительно при конфигурировании порта. Возможность переключения режимов отражается в названиях портов (Fast Ethernet 10/100), поддержка режима 100BaseT4 встречается нечасто.

100BaseT2 - малораспространенная (и не стандартизованная) версия с использованием двух пар категории 3 и выше. Сужение полосы достигается за счет применения 5-уровневого кодирования РАМ-5. Поддерживает полу- и полный Дуплекс, в режиме полного дуплекса сигналы распространяются по каждой паре во встречных направлениях (пропускная способность 100 Мбит/с относится только к полному дуплексу, скорость передачи в одну сторону - 50 Мбит/с).

100BaseFX - версия для оптоволокна с длиной волны 1300 нм. Логически близка к 100BaseTX - то же логическое кодирование 4В/5В, но физическое -NRZI (как в FDDI). В полудуплексе дальность 412 м - ограничение по времени двойного оборота. В полном Дуплексе дальность определяется свойством волокна: по ММ-волокну может достигать 2 км, по SM - 32 км.

100BaseSX - стандарт на дешевых коротковолновых (830 нм) светодиодных передатчиках и многомодовом волокне. Дальность связи ограничена волокном и меньше, чем у FX,- всего 300 м, зато поддерживается совместимость с 10BaseFL и автоматическое согласование скорости передачи 10/100 Мбит/с (802.3u). Версия разработана как дешевая альтернатива дорогой 100BaseFX в случаях, когда не требуется преодоления больших расстояний.

Центральным устройством в Fast Ethernet может быть повторитель или коммутатор. Повторители делятся на два класса:

• Повторитель класса I является транслирующим, он поддерживает разные схемы кодирования, принятые в технологиях 100BaseTX/FX и 100BaseT4.

• Повторитель класса II является прозрачным (transparent repeater), он поддерживает только одну из схем кодирования — технологию 100BaseTX/FX или 100BaseT4.

Благодаря избыточности кодирования по сравнению с Ethernet повторители Fast Ethernet работают несколько сложнее. В случае обнаружения ошибочного сигнала вместо его прозрачной трансляции в остальные порты повторитель может посылать признак повреждения кадра. Если повторитель поддерживает две схемы кодирования, ему приходится производить декодирование по схеме 4В/5В и последующее кодирование в 6В/8Т (или наоборот), что вносит дополнительную задержку.

Топологические ограничения Fast Ethernet жестче — диаметр домена коллизий для витой пары не должен превышать 205 м, в одном домене коллизий может быть не более двух повторителей класса II, повторитель класса I может быть только один. Если принять допустимое расстояние от повторителя до станции равным 100 м, то повторители можно соединять между собой кабелем длиной не более 5 м.

Возможная схема локальной сети с оптической линией показана на рисунке 1.2.

PC 2

PC 4

PC 3

PC 1

Рисунок 1.2 - Пример сети Ethernet с оптической линией

PC 5

1. **Gigabit Ethernet 1000 Мбит/с**

Технология Gigabit Ethernet со скоростью передачи данных 1000 Мбит/с разработана для ускорения передачи данных при использовании популярнейшей технологии (Ethernet). Однако повышение скорости на порядок при сохранении всех пропорций предыдущих технологий привело бы к сужению диаметра домена коллизий до неприемлемого размера — 0,26 мкс задержки соответствует примерно 50 м кабеля, а еще задержку вносит и повторитель. По этой причине минимально допустимый размер кадра, определяющий максимально допустимую задержку передачи, был увеличен до 512 байт (4096 bit). С учетом задержек в повторителе и адаптерах диаметр домена коллизий может достигать 200 м, то есть вписываться в стандартную концепцию построения СКС. Ограничения, порожденные методом CSMA/CD, актуальны только для полудуплексного режима работы портов. Для Gigabit Ethernet более характерен полнодуплексный режим, при котором допустимая длина линии связи ограничивается затуханием сигнала и частотными свойствами линии.

Дополнительно предусматривается возможность пакетной передачи кадров (frame bursting). Узел, получивший доступ к среде, после передачи одного кадра вместо паузы посылает специальную последовательность, после которой идет следующий кадр. Кадры пакета могут адресоваться разным получателям. Смысл пакетной передачи заключается в сокращении накладных расходов на получение доступа к среде — между кадрами пакета среда для остальных узлов выглядит занятой.

Gigabit Ethernet описывается двумя стандартами — IEEE 802.3z (1000BaseSX, 1000BaseLX и 1000BaseCX), принятым в 1998 году, и IEEE 802.3ab (1000BaseT), принятым осенью 1999 г.

Стандарт 802.3z основывается на наработках технологии Fiber Channel. Здесь используется избыточное кодирование 8В/10В, а схемы физического уровня «разогнаны» со скорости 800 Мбит/с до 1 Гбит/с (тактовая частота — 1,25 ГГц). Стандарт предлагает следующие версии:

1000BaseSX (Short wavelength) — оптический интерфейс с коротковолновыми (850 нм) лазерными передатчиками для связи по ММ-волокну на небольшие расстояния. Для кабеля с невысокой полосой пропускания допустимая длина соединения оказывается меньше, чем ограничение на длину магистрального кабеля 500 м, установленное стандартами СКС.

1000BaseLX (Long wavelength) — интерфейс с длинноволновыми (1310 м) лазерными передатчиками для связи по SM и ММ-волокну на большие расстояния.

1000BaseLH — интерфейс с лазерными передатчиками 1310 нм для связи по SM и ММ-волокну на сверхбольшие расстояния, пока в стандарт IEEE не входит.

1000BaseCX — электрический интерфейс для связи на короткие дистанции (25 м), предназначенный для связи оборудования в пределах аппаратной комнаты или телекоммуникационного помещения. Использует двухосевой (twinaxial) кабель или скрученные четверки проводов (quad cable) с частотными характеристиками, превосходящими STP типов 1 и 2. В качестве коннекторов пока предлагается DB-9 (используемый для STP в Token Ring), разрабатывается новый тип коннектора HSSDC (High-Speed Serial Data Connector).

1000BaseT — электрический интерфейс на витой паре (4 пары проводов) категории 5е (и даже 5) при ограничении на длину линии в 100 м. Физическое кодирование — 5-уровневое. Сигнал передается одновременно по четырем парам проводов, причем для полного дуплекса передача ведется по каждой паре сразу в обоих направлениях. Оконечные цепи выделяют из смеси сигнал противоположного передатчика. Решение этой задачи на сверхвысоких частотах стало возможным благодаря применению современных сигнальных процессоров. Для удовлетворения требованиям к среде передачи рекомендуется применение в кабельной системе компонентов категории 5е (розетки, шнуры, 4-парные кабели стационарной проводки). Количество соединений в канале должно быть минимальным. В телекоммуникационных помещениях рекомендуется схема непосредственного подключения (interconnection), без кросс-панели. В горизонтальной кабельной системе исключается соединение двух кусков кабелей в одной линии в точке перехода или консолидации.

* 1. **100VG-AnyLAN**

100VG-AnyLAN — технология со скоростью передачи 100 Мбит/с по 4-парному кабелю категории 3. VG означает Voice-Grade TP — витая пара для голосовой телефонии, окончание «Any LAN» означает возможность работы с «любыми ЛВС» (Ethernet и Token Ring). Разработана фирмами Hewlett-Packard и AT&T Microelectronics как развитие Ethernet, описывается стандартом IEEE 802.12. Физическая и логическая топология — дерево, построенное на хабах. Метод доступа — Demand Priority (приоритет запросов), управление доступом к среде передачи реализуется аппаратурой хабов централизованно. Этим 100VG принципиально отличается от других технологий, в которых функции управления доступом распределены по узлам сети.

Использовать кабель с гарантированной полосой частот 16 МГц позволяет одновременная передача сигналов в одну сторону по всем четырем парам (quartet signaling), в результате чего каждая пара пропускает всего 25 Мбит/с. Однако при этом полный дуплекс невозможен. Информация логически кодируется по схеме 5В/6В, после чего физически — по NRZ («1» — высокий уровень, «0» — низкий). Битовая скорость в каждой паре проводов — 30 Мбит/с.

Центральным элементом в управлении доступом является хаб. Каждый хаб имеет один порт для каскадирования (uplink или cascade port) и несколько регулярных (обычных) портов, к которым подключаются конечные узлы или промежуточные хабы (каскадными портами). Без хабов построение сети невозможно Даже для соединения двух узлов. Сеть может содержать множество хабов, построенных в строго древовидную структуру. В сети имеется один корневой хаб (root hub), он может быть и единственным. Под ним могут находиться промежуточные хабы (к которым подключаются хабы следующих уровней) и хабы «листья», к которым подключаются только конечные узлы. Допускается иерархическое каскадирование до пяти уровней хабов. Возможная схема локальной сети показана на рисунке 1.5.

Топологические ограничения просты: длина любой линии (между хабом и узлом или между двумя хабами) не более 100 м (для кабеля категории 5 — 200 м), количество уровней хабов — не более пяти. Максимальное расстояние между узлами (диаметр сети) может достигать 2000 м (применение оптоволоконных соединений не дает возможности преодолевать этот барьер, поскольку ограничена максимальная задержка прохождения сигнала). Максимальное количество узлов сети — до 1024 (рекомендуемое — до 250).

PC 3

PC 2

PC 1

Рисунок 1.5 - Пример сети 100VG-AnyLAN

**Wi-Fi**

1. **Стандарт IEEE 802.11**

На сегодняшний день существуют следующие разновидности данного стандарта построения беспроводных локальных сетей IEEE 802.11 a/b/g.

Стандарт IEEE 802.11, принятый в 1997 г., стал первым стандартом данного семейства. Он предусматривает использование диапазона частот 2,4 ГГц – 5 ГГц, а также технологии расширения спектра скачкообразной сменой частоты (Frequency Hopping Spread Spectrum или технологии расширения спектра по методу прямой последовательности. Direct Sequence Spread Spectrum DSSS. Стандарт IEEE 802.11 обеспечивает пропускную способность до 2 Мбит/с в расчете на одну точку доступа. В стадии рассмотрения находятся такие стандарты как IEEE 802.11e/f/h/i/j/n. Возможная схема локальной сети показана на рисунке 1.6.

1. **Стандарт IEEE 802.11a**

Стандарт IEEE 802.11 а предусматривает использование нового, не требующего лицензирования частотного диапазона 5 ГГц и модуляции по методу ортогонального мультиплексирования с разделением частот (Orthogonal Frequency Domain Multiplexing [OFDM]). Применение этого стандарта позволяет увеличить скорость передачи в каждом канале с 11 Мбит/с до 54 Мбит/с. При этом одновременно может быть организовано до восьми непересекающихся каналов (или точек присутствия), а не три, как в диапазоне 2,4 ГГц. Продукты стандарта IEEE 802.11а (сетевые адаптеры NIC и точки доступа) не имеют обратной совместимости с продуктами стандартов 802.11 и 802.11b, так как они работают на разных частотах.

1. **Стандарт IEEE 802.11b**

Стандарт IEEE 802.11b был принят в 1999 г. в развитие принятого ранее стандарта IEEE 802.11. Он также предусматривает использование диапазона частот 2,4 ГГц, но только с модуляцией DSSS. Данный стандарт обеспечивает пропускную способность до 11 Мбит/с в расчете на одну точку доступа.

Продукты стандарта IEEE 802.11b, поставляемые разными изготовителями, тестируются на совместимость и сертифицируются организацией Wireless Ethernet Compatibility Alliance (WECA), которая в настоящее время больше известна под названием Wi-Fi Alliance. Совместимые беспроводные продукты, прошедшие испытания по программе Альянса WH могут быть маркированы знаком Wi-Fi.

В настоящее время ЕЕЕ 802.11b это самый распространенный стандарт, на базе которого построено большинство беспроводных локальных сетей.

* 1. **Стандарт IEEE 802.11g**

Проект стандарта IEEE 802.11g был утвержден в октябре 2002 г. Этот стандарт предусматривает использование диапазона частот 2,4 ГГц, обеспечивая скорость передачи 54 Мбит/с и превосходя, таким образом, ныне действующий стандарт 802.11b. Кроме того, он гарантирует обратную совместимость со стандартом 802.11b. Обратная совместимость стандарта IEEE 802.11g может быть реализована в режиме модуляции DSSS, и тогда скорость передачи будет ограничена одиннадцатью мегабитами в секунду либо в режиме модуляции OFDM, при котором скорость составляет 54 Мбит/с. Таким образом, данный стандарт является наиболее приемлемым при построении беспроводных сетей.

PC 3

PC 2

PDA

PC 1

Рисунок 1.6 - Пример сети Wi-Fi

* 1. **WiMAX**

WiMAX - Worldwide Interoperability for Microwave Access, стандартизированная институтом IEEE технология широкополосной беспроводной связи, дополняющая линии DSL и кабельные технологии в качестве альтернативного решения проблемы "последней мили" на больших расстояниях. Технологию WiMAX можно использовать для реализации широкополосных соединений "последней мили", развертывания точек беспроводного доступа, организации высокоскоростной связи между филиалами компаний и решения других подобных задач.

Предварительная версия технологии WiMAX обеспечивала функциональность с помощью оборудования, которое не было подвергнуто стандартизированному тестированию на предмет совместимости с технологией WiMAX. Целый ряд провайдеров услуг до сих пор используют такие предварительные аппаратные решения для реализации пилотных проектов WiMAX во многих уголках мира. Как только тестирование совместимости этих систем с технологией WiMAX будет выполнено, их, скорее всего, можно будет модернизировать программным образом в соответствии с требованиями окончательного стандарта WiMAX.

В идеале беспроводная технология WiMAX, основанная на отраслевых стандартах, разработана для организации недорогой скоростной связи для жилищ, предприятий и мобильных беспроводных сетей в городах и сельской местности. Обратите внимание на определение, в нем заранее "предусмотрено местечко" для взаимодействия магистрального WiMAX с "локальным" Wi-Fi.

Оборудование сетей WiMAX функционирует в нескольких частотных каналах шириной 10 МГц в пределах диапазона 2 ГГц - 11 ГГц. Разумеется, специфическое распределение частотных диапазонов разных стран диктует необходимость возможности работы WiMAX в разных участках. Столь широкий разброс диапазонов выбран для учета специфики большинства стран мира. Так, в Северной Америке для WiMAX используются участки в диапазонах 2,5 и 5 ГГц, в Центральной и Южной Америке - 2,5, 3,5 и 5 ГГц, на Ближнем Востоке, в Африке, Западной и Восточной Европе - 3,5 и 5 ГГц, в Азиатско-Тихоокеанском регионе - 2,3, 3,5 и 5 ГГц. По своей сути WiMAX представляет технологию, позволяющую обеспечить доступ в интернет со скоростью сетей класса T1, с производительностью и покрытием, гораздо большим, нежели у современных сетей Wi-Fi. В свою очередь, продолжением "магистральных веток" WiMAX как раз и становятся локальные сети Wi-Fi, различные типы бизнес и бытовых кабельных/DSL сетей конечных пользователей.

Обеспечивая коммуникации в радиусе 10 километров и более, точки WiMAX создают покрытие на значительных площадях, предоставляя провайдерам услуг достаточно гибкие условия для обеспечения этой самой пресловутой "связи последней мили". Возможная схема локальной сети показана на рисунке 1.7.

Рисунок 1.7 - Пример сети WiMAX

В целом базовые характеристики стандарта 802.16 предусматривают дальность действия до 50 километров, покрытие с возможностью работы вне прямой зоны видимости, в перспективе – пиковую скорость обмена данными до 70 Мбит/с на сектор одной базовой станции при том, что типовая базовая станция будет иметь до 6 секторов покрытия.

Внедрение WiMAX нынче подразделено на три основных фазы. Нынешняя первая фаза внедрения подразумевает внедрение и широкое распространение технологии WiMAX стандарта IEEE 802.16-2004, заменившего собой ранние версии IEEE 802.16a и 802.16d, при котором используются внешние антенны по типу "сотовой тарелочки", фактически нацеленные на потребителей в фиксированных направлениях.

Преимущества и недостатки СКС приведены в таблице 1.1.

Таблица 1.1 - Преимущества и недостатки СКС и Wi-Fi

|  |  |  |
| --- | --- | --- |
|  | **Преимущества** | **Недостатки** |
| **СКС** | Высокая надежность и скорость передачи данных. | Длительные сроки проектирования и монтажа.Отсутствие мобильности, как пользователей, так и самой сети.Сложность расширения на новые территории. |
| **Wi-Fi** | Скорость развертывания. Беспроводная сеть может быть запушена в работу всего за несколько часов.Мобильность. Пользователи беспроводной сети могут свободно перемещаться. Также мобильна и сама сеть, ее легко перенести в другое место. | Скорость передачи данных ниже, чем в проводной сети.Необходимость получения разрешения на использование полосы частот. |

## **Понятие виртуальной локальной сети**

* + 1. **Предпосылки внедрения технологии виртуальной локальной сети в локальных сетях**

Изначально коммутаторы не обеспечивали возможности создания Виртуальных Локальных сетей, так как они использовались для простой пересылки кадров между устройствами. Рынок коммутаторов начал быстро расти, когда концентраторы коллективного доступа к среде передачи данных (hubs) начали не справляться с растущими запросами на расширение полосы пропускания сети в связи с использованием приложений клиент-сервер, обеспечивающих Графический Интерфейс Пользователя (GUI).

Ключевая разница между коммутатором и концентратором заключается в том, как они работают с кадрами. Концентратор получает кадр, затем копирует и передает (повторяет) кадр во все другие порты. В этом случае сигнал повторяется, в основном продляя длину сетевого сегмента до всех подключенных станций. Коммутатор повторяет кадр во все порты, кроме того, из которого этот кадр был получен: *unicast* кадры (адресованные на конкретный MAC адрес), *broadcast* кадры, (адресованные для всех MAC адресов в локальном сегменте), и *multicast* кадры (адресованные для набора устройств в сегменте). Это делает их неприемлемыми для большого числа пользователей, так как каждая рабочая станция и сервер, подключенный к коммутатору, должен проверять каждый кадр для того, чтобы определить, адресован ли этот кадр ему или нет. В больших сетях, с большим количеством кадров, обрабатываемых сетевой картой, теряется ценное процессорное время. Это приемлемо для небольших рабочих групп, где передача данных имеет кратковременную "взрывную" природу.

Коммутатор работает с кадрами "интеллектуально" - он считывает MAC адрес входящего кадра и сохраняет эту информацию в таблице коммутации. Эта таблица содержит MAC адреса и номера портов, связанных с ними. Коммутатор строит таблицу в разделенной памяти и поэтому он знает, какой адрес связан с каким портом. Коммутаторы Cisco Catalyst создают эту таблицу, проверяя каждый кадр, попавший в память, и добавляют новые адреса, которые не были занесены туда ранее. Маршрутизаторы Cisco создали эту таблицу, адресуя ее по содержимому (content-addressable memory). Эта таблица обновляется и строится каждый раз при включении коммутатора, но мы можем настраивать таймер обновления таблицы в зависимости от наших нужд. На рисунке 1.8 показана CAM таблица коммутатора Catalyst 5000.

В этом примере столбец VLAN ссылается на номер VLAN, которой принадлежит порт назначения. Столбец Destination MAC ссылается на MAC адрес, обнаруженный в порту. Помните, что один порт может быть связан с несколькими MAC адресами, поэтому проверьте количество MAC адресов, которое может поддерживать наш коммутатор. Destination Ports описывает порт, из которого коммутатор узнал MAC адрес.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Cat5500> show cam dynamic**

|  |  |  |
| --- | --- | --- |
| **VLAN** | **Destination MAC** | **Destination Ports or VCs**  |
| --------------------- | ------------------------------- | ----------------------------------------- |
| 1 | 00-60-2f-9d-a9-00  | 3/1  |
| 1 | 00-b0-2f-9d-b1-00 | 3/5 |
| 1 | 00-60-2f-86-ad-00 | 5/12 |
| 1 | 00-c0-0c-0a-bd-4b | 4/10 |

**Cat5500>**  |

Рисунок 1.8. Таблица коммутации

Далее, коммутатор проверяет MAC адрес назначения кадра и немедленно смотрит в таблицу коммутации. Если коммутатор нашел соответствующий адрес, он копирует кадр только в этот порт. Если он не может найти адрес, он копирует кадр во все порты. Unicast кадры посылаются на необходимые порты, тогда как multicast и broadcast кадры передаются во все порты.

Коммутация была объявлена как "новая" технология, которая увеличивает пропускную способность и увеличивает производительность, но на самом деле коммутаторы это высокопроизводительные мосты (bridges) с дополнительными функциями. Коммутация это термин, используемый в основном для описания сетевых устройств Уровня 2, которые переправляют кадры, основываясь на MAC адресе получателя.

Два основных метода, наиболее часто используемых производителями для передачи трафика это *cut-through* и *store and forward.*

Коммутация cut-through обычно обеспечивает меньшее время задержки, чем store-and-forward потому, что в этом режиме коммутатор начинает передачу кадра в порт назначения еще до того, как получен полностью весь кадр. Коммутатору достаточно того, что он считал MAC адреса отправителя и получателя, находящиеся вначале Token Ring и Ethernet кадров. Большинство cut-through коммутаторов начинает пересылку кадра, получив только первые 30 - 40 байт заголовка кадра.

Store and forward копирует весь кадр перед тем, как пересылать кадр. Этот метод дает большую задержку, но имеет больше преимуществ. Возможности фильтрации, управления и контроль над потоком информации являются главными преимуществами этого метода. В дополнение, неполные и поврежденные кадры не пересылаются, так как они не являются правильными кадрами. Коммутаторы должны иметь буферную память для чтения и сохранения кадров во время принятия решения, что увеличивает стоимость коммутатора.

По мере улучшения технологий и захвата рынка новой технологией, начали возникать VLAN. Простейший путь понять Виртуальные сети - сравнить их с физической сетью. Физическая сеть может состоять из конечных станций, связанных маршрутизатором (или маршрутизаторами), которые используют одно физическое соединение. VLAN это логическое комбинирование конечных станций в одном сегменте на Уровне 2 и Уровне 3, которые, связаны напрямую без маршрутизатора. Обычно пользователям, разделенным физически, требуется маршрутизатор для связи с другим сегментом. Коммутаторы с возможностью построения VLAN изначально были внедрены в основных учебных городках и небольших рабочих группах. Сначала коммутация разрабатывалась по мере надобности, но сейчас это является обычной практикой внедрять коммутаторы и VLAN в сетях

**Функции технологии виртуальной локальной сети в локальных сетях**

Кроме своего основного назначения - повышения пропускной способности связей в сети - коммутатор позволяет локализовать потоки информации в сети, а также контролировать эти потоки и управлять ими, используя пользовательские фильтры. Однако пользовательский фильтр может запретить передачи кадров только по конкретным адресам, а широковещательный трафик он передает всем сегментам сети. Так требует алгоритм работы моста, который реализован в коммутаторе, поэтому сети, созданные на основе мостов и коммутаторов иногда называют плоскими - из-за отсутствия барьеров на пути широковещательного трафика.

Технология виртуальных сетей *(Virtual LAN, VLAN)* позволяет преодолеть указанное ограничение. Виртуальной сетью называется группа узлов сети, трафик которой, в том числе и широковещательный, на канальном уровне полностью изолирован от других узлов сети. Это означает, что передача кадров между разными виртуальными сегментами 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.

При использовании технологии виртуальных сетей в коммутаторах одновременно решаются две задачи:

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

**Основные преимущества технологии виртуальных локальных сетей в локальных сетях**

Виртуальные сети (VLAN) предлагают следующие преимущества:

* Контроль за широковещательным трафиком
* Функциональные рабочие группы
* Повышенная безопасность

Контроль над широковещательным трафиком:в отличие от традиционных LAN, построенных при помощи маршрутизаторов/мостов, VLAN может быть рассмотрен как широковещательный домен с логически настроенными границами. VLAN предлагает больше свободы, чем традиционные сети. Ранее используемые разработки были основаны на физическом ограничении сетей, построенных на основе концентраторов; в основном физические границы LAN сегмента ограничивались эффективной дальностью, на которую электрический сигнал мог пройти от порта концентратора. Расширение LAN сегментов за эти границы требовало использования повторителей (repeaters), устройств, которые усиливали и пересылали сигнал. VLAN позволяет иметь широковещательный домен вне зависимости от физического размещения, среды сетевого доступа, типа носителя и скорости передачи. Члены могут располагаться там, где необходимо, а не там, где есть специальное соединение с конкретным сегментом. VLAN увеличивают производительность сети, помещая широковещательный трафик внутри маленьких и легко управляемых логических доменов. В традиционных сетях с коммутаторами, которые не поддерживают VLAN, весь широковещательный трафик попадает во все порты. Если используется VLAN, весь широковещательный трафик ограничивается отдельным широковещательным доменом.

Функциональные рабочие группы: Наиболее существенным преимуществом технологии VLAN является возможность создания рабочих групп, основываясь на функциональности, а не на физическом расположении или типе носителя. Традиционно администраторы группировали пользователей функционального подразделения физическим перемещением пользователей, их рабочих мест и серверов в общее рабочее пространство, например в один сегмент. Все пользователи рабочей группы имели одинаковое физическое соединение для того, чтобы иметь преимущество высокоскоростного соединения с сервером. VLAN позволяет администратору создавать, группировать и перегруппировывать сетевые сегменты логически и немедленно, без изменения физической инфраструктуры и отсоединения пользователей и серверов. Возможность легкого добавления, перемещения и изменения пользователей сети - ключевое преимущество VLAN.

Повышенная Безопасность: VLAN также предлагает дополнительные преимущества для безопасности. Пользователи одной рабочей группы не могут получить доступ к данным другой группы, потому что каждая VLAN это закрытая, логически объявленная группа. Представим компанию, в которой Финансовый департамент, который работает с конфиденциальной информацией, расположен на трех этажах здания. Инженерный департамент и отдел Маркетинга также расположены на трех этажах. Используя VLAN, члены Инженерного отдела и отдела Маркетинга могут быть расположены на всех трех этажах как члены двух других VLAN, а Финансовый департамент может быть членом третьей VLAN, которая расположена на всех трех этажах. Сейчас сетевой трафик, создаваемый Финансовым департаментом, будет доступен только сотрудникам этого департамента, а группы Инженерного и отдела Маркетинга не смогут получить доступ к конфиденциальным данным Финансового департамента. Очевидно, есть другие требования для обеспечения полной безопасности, но VLAN может быть частью общей стратегии сетевой безопасности. Показанный ниже рисунок говорит о том, как функционирование VLAN может расширить традиционные границы.

Рис. 1.9 Функционирование ВЛС

**Обзор технологии виртуальных локальных сетей в локальных сетях.**

**Типы виртуальных сетей**

Технология образования и работы виртуальных сетей с помощью коммутаторов долгое время была не стандартизована, хотя и была реализована в очень широком спектре моделей коммутаторов разных производителей. Такое положение изменилось, так как институт IEEE окончательно принял спецификации 802.1q/p, которые описывают стандартный способ построения виртуальных сетей.

В виду долгого отсутствия стандартов каждый производитель разработал свою технологию построения виртуальных сетей, которая, как правило, была несовместима с технологией других производителей. Поэтому виртуальные сети проще создавать пока на оборудовании одного производителя. Исключение составляют только виртуальные сети, построенные на основе спецификации LANE (LAN Emulation), предназначенной для обеспечения взаимодействия АТМ-коммутаторов с традиционным оборудованием локальных сетей. Существует несколько способов построения виртуальных сетей:

* Группировка портов.
* Группировка МАС-адресов.
* Использование меток в дополнительном поле кадра - частные протоколы и спецификации IEEE 802.1 Q/p.
* Спецификация LANE для АТМ-комутаторов.
* Использование сетевого уровня.

**VLAN на основе группировки портов**

При создании виртуальных сетей на основе одного коммутатора обычно используется механизм группирования в виртуальные сети портов коммутатора

Рис. 1.10. Виртуальные сети, построенные на одном коммутаторе с помощью группировки портов

Это логично, так как виртуальных сетей, построенных на основе одного коммутатора, не может быть больше, чем портов. Если к одному порту подключен сегмент, построенный на основе повторителя, то узлы такого сегмента не имеет смысла включать в разные виртуальные сети - все равно трафик этих узлов будет общим.

Создание виртуальных сетей на основе группирования портов не требует от администратора большого объема ручной работы - достаточно каждый порт приписать к нескольким заранее поименованным виртуальным сетям. Обычно, такая операция выполняется путем перетаскивания мышью графических символов портов на графические символы сетей.

**Виртуальные локальные сети на основе группировки МАС-адресов**

Второй способ, который используется для образования виртуальных сетей, основан на группировании МАС-адресов. При существовании в сети большого количества узлов этот способ требует выполнения большого количества ручных операций от администратора. Однако он оказывается более гибким при построении виртуальных сетей на основе нескольких коммутаторов, чем способ группирования портов.

Рис. 1.11 Построение виртуальных сетей на нескольких коммутаторах с группировкой портов

Рисунок 1.11 иллюстрирует проблему, возникающую при создании виртуальных сетей на основе нескольких коммутаторов, поддерживающих технику группирования портов. Если узлы какой-либо виртуальной сети подключены к разным коммутаторам, то для соединения коммутаторов каждой такой сети должна быть выделена своя пара портов. В противном случае, если коммутаторы будут связаны только одной парой портов, информация о принадлежности кадра той или иной виртуальной сети при передаче из коммутатора в коммутатор будет утеряна. Таким образом, коммутаторы с группировкой портов требуют для своего соединения столько портов, сколько виртуальных сетей они поддерживают. Порты и кабели используются при таком способе очень расточительно. Кроме того, при соединении виртуальных сетей через маршрутизатор для каждой виртуальной сети выделяется в этом случае отдельный кабель, что затрудняет вертикальную разводку, особенно если узлы виртуальной сети присутствуют на нескольких этажах (рис. 1.12).

Рис. 1.12. Соединение виртуальных сетей, построенных на группировании портов, через маршрутизатор

Группирование МАС-адресов в сеть на каждом коммутаторе избавляет от необходимости их связи несколькими портами, однако требует выполнения большого количества ручных операций по маркировке МАС-адресов на каждом коммутаторе сети.

**Использование меток в дополнительном поле кадра - стандарты 802.1 Q/p и фирменные решения**

Описанные два подхода основаны только на добавлении дополнительной информации к адресным таблицам моста и не используют возможности встраивания информации о принадлежности кадра к виртуальной сети в передаваемый кадр. Остальные подходы используют имеющиеся или дополнительные поля кадра для сохранения информации и принадлежности кадра при его перемещениях между коммутаторами сети. При этом нет необходимости запоминать в каждом коммутаторе принадлежность всех МАС-адресов интерсети виртуальным сетям.

Если используется дополнительное поле с пометкой о номере виртуальной сети, то оно используется только тогда, когда кадр передается от коммутатора к коммутатору, а при передаче кадра конечному узлу оно удаляется. При этом модифицируется протокол взаимодействия "коммутатор-коммутатор", а программное и аппаратное обеспечение конечных узлов остается неизменным. Примеров таких фирменных протоколов много, но общий недостаток у них один - они не поддерживаются другими производителями. Компания Cisco предложила использовать в качестве стандартной добавки к кадрам любых протоколов локальных сетей заголовок протокола 802.10, предназначенного для поддержки функций безопасности вычислительных сетей. Сама компания использует этот метод в тех случаях, когда коммутаторы объединяются между собой по протоколу FDDI. Однако, эта инициатива не была поддержана другими ведущими производителями коммутаторов.

Новый стандарт IEEE 802.1Q определяет изменения в структуре кадра Ethernet, позволяющие передавать информацию о VLAN по сети. Стандарт IEEE 802.1p специфицирует метод указания приоритета кадра, основанный на использовании новых полей, определенных в стандарте IEEE 802.1Q. К кадру Ethernet добавлены два байта. Эти 16 бит содержат информацию по принадлежности кадра Ethernet к VLAN и о его приоритете. Говоря точнее, тремя битами кодируется до восьми уровней приоритета, 12 бит позволяют различать трафик до 4096 VLAN, а один бит зарезервирован для обозначения кадров сетей других типов (Token Ring, FDDI), передаваемых по магистрали Ethernet. Надо сказать, что добавление двух байтов к максимальному размеру кадра Ethernet ведет к возникновению проблем в работе многих коммутаторов, обрабатывающих кадры Ethernet аппаратно. Чтобы избежать их, группы по стандартизации предложили сократить на два байта максимальный размер полезной нагрузки в кадре. Спецификация IEEE 802.1p, создаваемая в рамках процесса стандартизации 802.1Q, определяет метод передачи информации о приоритете сетевого трафика. Стандарт 802.1p специфицирует алгоритм изменения порядка расположения пакетов в очередях, с помощью которого обеспечивается своевременная доставка чувствительного к временным задержкам трафика. В дополнение к определению приоритетов стандарт 802.1p вводит важный протокол GARP (Generic Attributes Registration Protocol) с двумя специальными его реализациями. Первая из них - протокол GMRP (GARP Multicast Registration Protocol), позволяющий рабочим станциям делать запрос на подключение к домену групповой рассылки сообщений. Поддерживаемую этим протоколом концепцию назвали подсоединением, инициируемым "листьями". Протокол GMRP обеспечивает передачу трафика только в те порты, из которых пришел запрос на групповой трафик, и хорошо согласуется со стандартом 802.1Q. Второй реализацией GARP является протокол GVRP (GARP VLAN Registration Protocol), похожий на GMRP. Однако, работая по нему, рабочая станция вместо запроса на подключение к домену групповой рассылки сообщений посылает запрос на доступ к определенной VLAN. Для согласования работы устройств, поддерживающих формат кадра 802.1 Q, с теми устройствами, которые не понимают этот формат, разработчики стандарта предложили делить весь трафик в сети на несколько типов:

* Трафик входного порта
* Внутренний трафик
* Трафик выходного порта

Трафик входного порта (Ingress Port)*.* Каждый кадр, достигающий коммутируемой сети и идущий либо от маршрутизатора, либо от рабочей станции, имеет определенный порт-источник. На основании его номера коммутатор должен "принять решение" о приеме (или отбрасывании) кадра и передаче его в ту или иную VLAN. Решение "судьбы" кадра, осуществляемое в единственной логической точке сети, делает возможным сосуществование самых разных видов VLAN. Приняв кадр, коммутатор "прикрепляет" к нему "ярлык" (tag) VLAN. Как только кадр с "ярлыком" VLAN оказывается в сети, он становится частью проходящего (Progress), или внутреннего трафика.

Внутренний трафик (Progress Traffic). Кадр с "ярлыком" коммутируется точно так же, как и без "ярлыка". Решения о его принадлежности к той или иной VLAN принимаются в пограничных элементах сети и остальные сетевые устройства индифферентно "относятся" к тому, как именно кадр попал в сеть. Так как максимальный размер кадра Ethernet остался неизменным, то пакеты всех VLAN смогут обрабатываться традиционными коммутаторами и маршрутизаторами внутренней части сети.

Трафик выходного порта (Egress Port). Чтобы попасть в межсетевой маршрутизатор или в оконечную рабочую станцию, кадр должен выйти за пределы коммутируемой сети. Ее выходное устройство "решает", какому порту (или портам) нужно передать пакет и есть ли необходимость удалять из него служебную информацию, предусмотренную стандартом 802.1Q. Дело в том, что традиционные рабочие станции не всегда воспринимают информацию о VLAN по стандарту 802.1Q, но сервер, обслуживающий несколько подсетей с помощью единственного интерфейса, должен ее активно использовать.

Условное деление трафика на внутренний, а также входного и выходного портов позволяет поставщикам нестандартных реализаций VLAN создавать шлюзы для их стыковки с VLAN, соответствующими стандарту 802.1Q.

**Настройка VLAN Транков**

Транки используются для обмена информацией о VLAN между коммутаторами, обеспечивая тем самым возможность построения сетей VLAN, перекрывающих физические границы коммутатора. Концепция транкинга подобна протоколам маршрутизации, используемым для построения сетевой топологии. Коммутаторы используют транковые протоколы для того, чтобы определить, на какой порт посылать кадры, если VLAN перекрывает физические границы. Используя транковый протокол, одна и та же VLAN может быть объявлена на каждом этаже 12-этажного дома. Коммутаторы Catalyst поддерживают различные транковые методы:

* Inter-Switch Link (ISL) Fast Ethernet (100 Mbps), Gigabit Ethernet (1000 Mbps)
* IEEE 802.1Q Fast Ethernet (100 Mbps), Gigabit Ethernet (1000 Mbps)
* IEEE 802.10 Fiber/Copper Distributed Data Interface (FDDI)/(CDDI) (100 Mbps)
* LAN Emulation ATM (155 Mbps OC-3 and 622 Mbps OC-12)

Это всегда хорошая идея, посмотреть "Release Notes" новых версий операционной системы коммутатора, так как они включают новые функции и возможности коммутаторов. Это поможет убедиться в том, что коммутатор будет поддерживать функции, требуемые для построения вашей сети

**Использование спецификации LANE**

Существует два способа построения виртуальных сетей, которые используют уже имеющиеся поля для маркировки принадлежности кадра виртуальной сети, однако эти поля принадлежат не кадрам канальных протоколов, а ячейкам технологии АТМ или пакетам сетевого уровня.

Спецификация LANE вводит такое понятие как эмулируемая локальная сеть - ELAN. Это понятие имеет много общего с понятием виртуальной сети:

* ELAN строится в сети, состоящей из коммутаторов (коммутаторов АТМ);
* связь между узлами одной и той же ELAN осуществляется на основе МАС-адресов без привлечения сетевого протокола;
* трафик, генерируемый каким-либо узлом определенной ELAN, даже широковещательный, не выходит за пределы данной ELAN.

Кадры различных ELAN не свешиваются друг с другом внутри сети коммутаторов АТМ, так как они передаются по различным виртуальным соединениям и номер виртуального соединения VPI/VCI является тем же ярлыком, который помечает кадр определенной VLAN в стандарте 802.1Q и аналогичных фирменных решениях.

Если VLAN строятся в смешанной сети, где имеются не только коммутаторы АТМ, то "чистые" коммутаторы локальных сетей, не имеющие АТМ-интерфейсов, должны использовать для создания виртуальной сети один из выше перечисленных методов, а пограничные коммутаторы, имеющие наряду с традиционными еще и АТМ-интерфейсы, должны отображать номера VLAN на номера ELAN при передаче кадров через сеть АТМ.

**Использование сетевого протокола**

При использовании этого подхода коммутаторы должны для образования виртуальной сети понимать какой-либо сетевой протокол. Такие коммутаторы называют коммутаторами 3-го уровня, так как они совмещают функции коммутации и маршрутизации. Каждая виртуальная сеть получает определенный сетевой адрес - как правило, IP или IPX.

Тесная интеграция коммутации и маршрутизации очень удобна для построения виртуальных сетей, так как в этом случае не требуется введения дополнительных полей в кадры, к тому же администратор только однократно определяет сети, а не повторяет эту работу на канальном и сетевом уровнях. Принадлежность конечного узла к той или иной виртуальной сети в этом случае задается традиционным способом - с помощью задания сетевого адреса. Порты коммутатора также получают сетевые адреса, причем могут поддерживаться нестандартные, для классических маршрутизаторов ситуации, когда один порт может иметь несколько сетевых адресов, если через него проходит трафик нескольких виртуальных сетей, либо несколько портов имеют один и тот же адрес сети, если они обслуживают одну и ту же виртуальную сеть.

При передаче кадров в пределах одной и той же виртуальной сети коммутаторы 3-го уровня работают как классические коммутаторы 2-го уровня, а при необходимости передачи кадра из одной виртуальной сети в другую - как маршрутизаторы. Решение о маршрутизации обычно принимается традиционным способом - его делает конечный узел, когда видит на основании сетевых адресов источника и назначения, что кадр нужно отослать в другую сеть.

Однако использование сетевого протокола для построения виртуальных сетей ограничивает область их применения только коммутаторами 3-го уровня и узлами, поддерживающими сетевой протокол. Обычные коммутаторы не смогут поддерживать такие виртуальные сети и, это является большим недостатком. За бортом также остаются сети на основе немаршрутизируемых протоколов, в первую очередь сети NetBIOS.

По этим причинам наиболее гибким подходом является комбинирование виртуальных сетей на основе стандартов 802.1 Q/p с последующим их отображением на "традиционные сети" в коммутаторах 3-го уровня или маршрутизаторах. Для этого коммутаторы третьего уровня и маршрутизаторы должны понимать метки стандарта 802.1 Q.

## **Агент ретрансляции DHCP**

Агент ретрансляции DHCP(dhcp-relay) позволяет ретранслировать DHCP и BOOTP запросы из подсети, в которой нет DHCP сервера в другую, или в несколько других подсетей, имеющих DHCP сервера.

Коммутатор может быть сконфигурирован как агент DHCP Relay. В этом случае расширяются возможности применения DHCP-серверов в сети, поскольку уже не нужно использовать несколько DHCP-серверов, по одному в каждой подсети. Коммутатор просто перенаправляет DHCP-запрос от клиента в локальной подсети на удалённый DHCP-сервер.

Option 82 используется для передачи дополнительной информации в DHCP-запросе. Причём эту информацию добавляет сам коммутатор. Эта информация может быть использована для применения политик для увеличения уровня безопасности и эффективности. Для простоты эти пакеты содержат информацию BOOTP, т.е. DHCP-запросы обрабатываются коммутатором также как BOOTP-запросы.

Когда DHCP клиент запрашивает информацию, агент ретрансляции DHCP пересылает запрос списку DHCP серверов, указанных при запуске агента. Когда DHCP сервер возвращает ответ, он отправляется либо широковещательно либо направленно в сеть, из которой был получен первоначальный запрос.

**Формат поля DHCP option 82 для DES-35XX:**

Формат поля опции с Circuit ID - в ней указывается порт коммутатора, за которым находится клиент и VID соответствующего VLAN:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1.  | 2.  | 3.  | 4.  | 5.  | 6.  | 7.  |
| 1  | 6  | 0  | 4  | VLAN  | Module | Port |
| 1 байт | 1 байт  | 1 байт  | 1 байт | 2 байта  | 1 байт  | 1 байт |

1. Тип опции

2. Длина

3. Тип Circuit ID

4. Длина

5. VLAN: VLAN ID DHCP-запроса клиента

6. Module: Для автономного коммутатора, поле Module всегда 0; для стекируемого коммутатора, Module = Unit ID.

7. Port: Порт коммутатора, с которого получен DHCP-запрос (начинается с 1) port

Формат поля опции с Remote ID - в ней указывается MAC-адрес коммутатора, являющегося агентом DHCP Relay:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1.  | 2.  | 3.  | 4.  | 5.  |
| 2  | 8  | 0  | 6  | MAC address  |
| 1 байт  | 1 байт  | 1 байт  | 1 байт  | 6 байтов |

1. Тип опции

2. Длина

3. Тип Remote ID type

4. Длина

5. MAC address: MAC-адрес коммутатора.

**Пример настройки:**

**Оборудование:**

1. DHCP-сервер 10.51.8.1 в подсети 10.0.0.0/8
2. Маршрутизатор или коммутатор L3, выступающий в роли шлюза для 2-ух подсетей
3. 10.51.8.11 для подсети 10.0.0.0/8
4. 30.51.8.11 для подсети 30.0.0.0/8
5. Коммутатор L2 (DES-3526/DES-3550) в роли агента DHCP Relay
6. 30.51.8.12 в подсети 30.0.0.0/8
7. MAC-адрес: 00-80-C8-35-26-0A
8. 2 ноутбука в качестве DHCP - клиентов, подсоединённые к портам 9 и 10 коммутатора L2 соответственно

**Схема сети:**

**Рисунок 1.13**

**Задача:**

1. DHCP-сервер использует диапазон адресов 30.51.8.100 - 30.51.8.200 для выдачи DHCP-клиенту, запросы которого перенаправляются агентом DHCP Relay 30.51.8.12 (коммутатор L2)
- Обычный режим DHCP
2. Как только какой-либо клиент DHCP подключается к порту 9 коммутатора L2, DHCP-сервер выдаст ему IP-адрес 30.51.8.161; если к порту 10 - то 30.51.8.162. - Функция DHCP option 82

**Команды для настройки коммутатора L2 (DES-3526/DES-3550):**

1. **create iproute default 30.51.8.11**
2. **config dhcp\_relay add ipif System 10.51.8.1**
3. **config dhcp\_relay option\_82 state enable**
4. **enable dhcp\_relay**
5. **Настройка DHCP-сервера:**

В этом примере используется 30-ти дневная версия haneWIN DHCP server 2.1, которую вы можете взять с сайта

1. В пункте Option -> Preferences -> DHCP взведите галочку Accept Relay Agent Information (Option 82)
2. Сконфигурируйте Option -> Default Client Profile -> Basic Profile Relay IP: 30.51.8.12 Dynamic IP Addresses: От 30.51.8.100 до 30.51.8.200 Subnet mask: 255.0.0.0 Gateway Address: 30.51.8.11
3. Сконфигурируйте DHCP option 82
4. a) Задайте IP-адрес 30.51.8.161 для DHCP-клиента A, подключённого к порту 9 коммутатора L2
5. "Add static entries"
6. Взведите галочки "Circuit Identifier" и "Remote Identifier"
7. Hardware Address: 00040001000900060080c835260a
8. IP Address: 30.51.8.161
9. b) Задайте IP-адрес 30.51.8.162 для DHCP-клиента B, подключённого
10. к порту 10 коммутатора L2
11. "Add static entries"
12. Взведите галочки "Circuit Identifier" и "Remote Identifier"
13. Hardware Address: 00040001000a00060080c835260a
14. IP Address: 30.51.8.162

## **Протоколы маршрутизации**

RIP — так называемый дистанционно-векторный протокол, который оперирует хопами в качестве метрики маршрутизации. Максимальное количество хопов, разрешенное в RIP — 15 (метрика 16 означает «бесконечно большую метрику»). Каждый RIP-маршрутизатор по умолчанию вещает в сеть свою полную таблицу маршрутизации раз в 30 секунд, генерируя довольно много трафика на низкоскоростных линиях связи. RIP работает на прикладном уровне стека TCP/IP, используя UDP порт 520.

В современных сетевых средах RIP — не самое лучшее решение для выбора в качестве протокола маршрутизации, так как его возможности уступают более современным протоколам, таким как EIGRP, OSPF. Ограничение на 15 хопов не дает применять его в больших сетях. Преимущество этого протокола — простота конфигурирования.

OSPF (англ. *Open Shortest Path First*) — протокол динамической маршрутизации в сетях IPv4 и IPv6.

OSPF был разработан для больших и развивающихся сетей. Основанный на технологии отслеживания состояния канала (link-state technology), протокол выполняет две основные функции, присущие любому алгоритму маршрутизации:

* Выбор пути
* Коммутация по выбранному пути

Протокол OSPF был разработан IETF в 1988 году. Последняя версия протокола представлена в RFC 2328. Протокол OSPF представляет собой протокол внутреннего шлюза (Interior Gateway Protocol — IGP).

Протокол OSPF распространяет информацию о доступных маршрутах между маршрутизаторами одной автономной системы.

OSPF предлагает решение следующих задач:

* Увеличение скорости сходимости
* Поддержка сетевых масок переменной длины (VLSM)
* Достижимость сети
* Использование пропускной способности
* Метод выбора пути

**Многоадресная рассылка**

Многоадресная рассылка (Multicast) – это технология экономии полосы пропускания, которая сокращает трафик за счет доставки одного потока информации сразу тысячам корпоративных или частных абонентов. Преимущества многоадресной рассылки используют такие приложения как видеоконференции, корпоративная связь, дистанционное обучение. Суть многоадресной рассылки заключается в том, что она позволяет нескольким получателям принимать сообщения без передачи сообщений каждому узлу широковещательного домена.

Многоадресная рассылка предполагает отправку сообщений или данных на IP-адрес группы многоадресной рассылки. У этой группы нет физических или географических ограничений: узлы могут находиться в любой точке мира. Узлы, которые заинтересованы в получении данных для определенной группы, должны присоединиться к этой группе (подписаться на рассылку) при помощи протокола IGMP. После этого пакеты многоадресной рассылки IP, содержащие групповой адрес в поле назначения заголовка, будут поступать на этот узел и обрабатываться.

**Адресация многоадресной рассылки**

Групповые адреса определяют произвольную группу IP-узлов, присоединившихся к этой группе и желающих получать адресованный ей трафик. Назначением групповых адресов управляет IANA (Internet Assigned Numbers Authority, Агентство по выделению имен и уникальных параметров протоколов Интернет). Оно выделило для групповой IP-адресации старые адреса класса D. Это означает, что область многоадресной рассылки охватывает адреса с 224.0.0.0 до 239.255.255.255.

IANA зарезервировало область многоадресной рассылки IP 224.0.0.0-224.0.0.255 для сетевых протоколов сегментов локальных сетей. Пакеты с такими адресами никогда не выходят за пределы локальной сети. Вторая группа адресов в диапазоне 224.0.1.0-224.0.1.255 – это глобальные адреса, которые могут использоваться для многоадресной передачи данных в

Интернет.

**Подписка и обслуживание групп**

Сам по себе многоадресный трафик не знает ничего о том, где находятся его адресаты. Как и для любого приложения для этого нужны протоколы.

**Протокол IGMP** (Internet Group Management Protocol, межсетевой протокол управления группами) используется для динамической регистрации отдельных узлов в многоадресной группе локальной сети. Узлы сети определяют принадлежность к группе, посылая IGMP сообщения на свой локальный многоадресный маршрутизатор. По протоколу IGMP маршрутизаторы получают IGMP-сообщения и периодически посылают запросы, чтобы определить, какие группы активны или неактивны в данной сети.

**Протокол IGMP v1**

В версии 1 протокола IGMP существуют два типа IGMP-сообщений:

􀂃 Запрос о принадлежности к группе;

􀂃 Ответ о принадлежности к группе.

Узлы отсылают IGMP-ответы, которые соответствуют u1086 определенной многоадресной группе, чтобы подтвердить свое желание присоединиться к этой группе. Маршрутизатор периодически отправляет IGMP-запрос, чтобы убедиться, что хотя бы один узел в подсети еще

намерен получать трафик, предназначенный для этой группы. При отсутствии ответа на три последовательных IGMP-запроса, маршрутизатор отключает группу и прекращает передавать адресованный ей трафик.

**Протокол IGMP v2**

В версии 2 протокола IGMP существуют четыре типа IGMP-сообщений:

􀂃 Запрос о принадлежности к группе;

􀂃 Ответ о принадлежности к группе по версии 1;

􀂃 Ответ о принадлежности к группе по версии 2;

􀂃 Покинуть группу.

В основном работа IGMP 2 не отличается от IGMP 1. Разница заключается в наличие сообщений о выходе из группы. Теперь узлы сами могут сообщить локальному многоадресному маршрутизатору о намерении покинуть группу. В ответ маршрутизатор отсылает группе специальный запрос, чтобы определить, остались ли в ней еще узлы, желающие получать данный трафик. Если ответа не поступит, маршрутизатор отключает группу и прекращает передачу трафика. Это может значительно сократить задержки, связанные с прекращением членства в группе, по сравнению с IGMP 1. Нежелательный и ненужный трафик может быть прекращен гораздо быстрее.

**Управление многоадресной рассылкой на 2 уровне**

Стандартное поведение коммутатора 2-ого уровня заключается в передаче всего многоадресного трафика на каждый порт, принадлежащий локальной сети-приемнику на данном коммутаторе. Это связано с тем, что коммутатор не находит записи об МАС-адресе групповой рассылки в своей таблице коммутации, и поэтому рассылает пакеты через все порты.

Это противоречит основному назначению коммутатора, которое заключается в ограничении трафика и доставке его только тем портам, для которых такие данные действительно предназначены.

Управление многоадресной рассылкой на коммутаторе может быть выполнено несколькими способами:

Виртуальные локальные сети VLAN могут определять соответствующие границы многоадресной группы. Этот подход прост, однако он не поддерживает динамическое добавление или исключение членов из группы.

Второй метод, который поддерживается коммутаторами D-Link – IGMP**-**

прослушивание (IGMP-snooping). IGMP-прослушивание – это проверки или прослушивание локальной сети на наличие в IGMP-пакетах, передаваемых между узлом и маршрутизатором, некоторой информации 3-его уровня. Когда коммутатор получает IGMP-отчет узла для многоадресной группы, он заносит номер порта узла в запись своей ассоциированной многоадресной таблицы. Когда коммутатор получает IGMP-сообщение о выходе узла из группы, он удаляет номер порта этого узла из записи таблицы.

Поскольку управляющие IGMP-сообщения передаются в виде многоадресных пакетов, они неотличимы от многоадресных данных 2-ого уровня. Коммутатор, на котором осуществляется IGMP-прослушивание, проверяет все многоадресные пакеты и ищет среди них те, которые содержат управляющую информацию. IGMP-прослушивание сильно загружает центральный процессор и может снизить производительность коммутатора. Поэтому в коммутаторах обычно используются специализированные микросхемы, которые проверяют IGMP-сообщения на аппаратном уровне.

Рисунок 1.14

## **Требования, предъявляемые к домовым локальным сетям при их модернизации**

Главным требованием, предъявляемым к домовым локальным сетям, является выполнение сетью ее основной функции - обеспечение пользователям возможности доступа в Интернет и внутренним ресурсам всех компьютеров, находящихся в данной сети. Остальные требования, такие как производительность, надежность, совместимость, управляемость и масштабируемость связаны с качеством выполнения этой основной задачи предоставления услуг пользователю.

Производительность - это свойство обеспечивается возможностью распараллеливания работ между несколькими компьютерами сети. Существуют следующие основные характеристики производительности сети – время реакции, пропускная способность и задержка передачи, и вариация задержки передачи.

Время реакции сети является интегральной характеристикой производительности с точки зрения пользователя. В общем случае время реакции определяется как интервал времени между возникновением запроса пользователя к какой-либо сетевой службе и получением ответа на этот запрос.

Пропускная способность отражает объем данных, переданных сетью или ее частью в единицу времени.

Задержка передачи определяется как задержка между моментом поступления пакета на вход какого-либо сетевого устройства или части сети и моментом появления его на выходе этого устройства.

Надежность ЛВС определяется следующими показателями:

• готовностью или коэффициентом готовности, который означает долю времени, в течении которого система может быть использована;

• вероятностью доставки пакета узлу назначения без искажений (вероятность потери пакета);

• вероятность искажения отдельного бита передаваемых данных, (отношение потерянных пакетов к доставленным);

• способностью системы защитить данные от несанкционированного доступа;

• отказоустойчивостью - способностью скрыть от пользователя отказ отдельных элементов сети;

• расширяемость означает возможность сравнительно легкого добавления отдельных элементов сети (пользователей, компьютеров, приложений и служб), наращивая длины сегментов сети и замены существующей аппаратуры более мощной;

• масштабируемость означает, что сеть позволяет наращивать количество узлов и протяженность связей в очень широких пределах, при этом производительность сети не ухудшается;

• поддержка разных видов трафика. Сеть должна обеспечить совместную передача традиционного компьютерного и мультимедийного трафика. Если сеть обладает поддержкой разных видов трафика эту сеть можно называть мультисервисной сетью;

• управляемость подразумевает собой возможность централизованно контролировать состояние магистральных и отдельных элементов сети, выявлять и разрешать проблемы, возникающие при работе сети, выполнять анализ производительности сети и планировать дальнейшее её развитие;

• совместимость или интегрируемость означает, что сеть способна включать в себя самое разнообразное программное и аппаратное обеспечение, то есть в ней могут сосуществовать различные операционные системы, поддерживающие различные стеки коммуникационных протоколов, и работать аппаратные средства и приложения от различных производителей.

## **Анализ домовой локальной вычислительной сети**

Необходимость модернизации домовой локальной сети обусловлена следующими основными причинами:

1. На данный момент домовая сеть является сетью второго уровня построенная по технологии Gigabit Ethernet с использованием топологии звезда. На магистральных оптических линиях используются управляемые коммутаторы второго уровня и программируемый коммутатор третьего уровня в центре топологии.

2. Сеть не разделена на логические сегменты, т.е. маршрутизация трафика в сети не осуществляется. В следствии этого, с сети в одном broadcast домене оказываются около 6500 компьютеров. Этот фактор сказывается на качестве предоставляемых услуг доступа в Интернет, особенно по вечерам, когда активность широковещательного трафика в сети возрастает.

3. Входящий гигабитный Интернет канал в локальную сеть уже не может обеспечить должную скорость и требует его расширения.

4. Внедрение IP-телевидения вносит ряд проблем, связанных с передачей данных в реальном режиме времени. Для этого разработаны методики приоритезации трафика в сетях передачи данных. Текущее сетевое оборудование, установленное в локальной сети может обеспечить передачи данных в реальном режиме времени, но не при нынешней логической структуре и настройки, при имеющейся структуре возможны сбои в работе сервиса телевидение и сервиса IP-телефонии также критичного ко времени.

5. Нужно учесть, что постоянно поступают звонки от потенциальных пользователей на подключение к сети и нужно обеспечить запас производительности сети для новых пользователей.

6. Так же на рынке услуг связи существует конкуренция и для того, чтобы не растерять клиентскую базу, нужно идти в ногу с современными технологиями и сервисами локальных сетей.

Таким образом, настоящая архитектура сети уже не может обеспечивать должную пропускную способность каналов связи для внедрения новых услуг и повышения качества обслуживания клиентов.

## **Выводы по аналитической части**

Рост клиентской базы, внедрение L2 услуг на построенной сети, влечёт за собой постоянное повышение нагрузки на коммутаторы всех уровней сети и border'ов, в целях недопущения перегрузки коммутаторов, снятия существующей предельной загрузки и для повышения качества предоставления услуг triple-play(данные, голос и видео), предлагается провести реорганизацию сети с минимальными финансовыми вложениями.

Исходя из анализа домовой локальной сети, однозначно можно сказать, что применяемая технология при модернизации сети останется Gigabit Ethernet, т.к. использование другой технологии экономически не выгодно и нецелесообразно. Так же эта технология экономически выгодна по цене за порт. Топологию менять нет смысла, так как это повлечет за собой строительство новых оптических трасс и потребует больших финансовые вложений, не говоря о всевозможных проблемах сопутствующих строительству новых каналов связи. Необходимо использовать как можно больше функций реализованных в имеющемся оборудование(DES-3526, DXS-3326GSR). Защита и управление на основе анализа пакетов и отслеживания состояния соединений, блокирование DoS-атак, списки контроля доступа (ACL).

1. Реорганизация инфраструктуры опорной сети для передачи голоса и видео, обеспечивающих улучшенное качество обслуживания, включая поддержку технологии для управления трафиком. Используя дифференцированные IP-услуги для приложений.
2. Вынести интерфейсы управления коммутаторов в отдельный VLAN, это позволит осуществлять удаленное управление и конфигурирование, через графический пользовательский интерфейс с помощью специального программного обеспечения или по протоколам Telnet, Secure Shell или Rlogin.
3. Централизованное оповещение о состоянии активного оборудования через протокол SNMP, что повысит возможность предупреждения и поиска неполадок в сети, наблюдение за загруженностью каналов связи.
4. Централизовать динамическую выдачу настроек сети пользователям, путём переноса dhcp-сервера с border'а на сервер находящийся в датацентре компании.

# Проектная часть

## **Концепция развития домовой локальной вычислительной сети**

С развитием информационных технологий люди передают по сетям передачи данных не только данные, но и голос, и изображение. Совокупность предоставления такого рода услуг, носит маркетинговый термин Triple-play, предполагающий наличие широкополосного доступа в сеть Интернет. Требования к такой услуге предъявляются высокие. Данные необходимо получать целиком. Голос необходимо слышать четко, не должно быть проблем с установкой связи, слышимостью. Видео должно быть качественным, не должно быть рассыпания картинки, зависаний изображений, звук и видео должны быть синхронизованы. Для того чтобы описанные критерии соблюдались, необходимо иметь надежную и качественную опорную сеть, где будет оптимально сбалансирована загрузка процессорной мощности коммутационного оборудования, пропускная способность каналов связи, паразитный трафик и шумы должны быть минимизированы чтоб не вызывать временных задержек.

Для реорганизации сети предлагаются следующие основные действия:

1. Вынести интерфейсы управления коммутаторов(management-интефейсов) в отдельный VLAN с выделением сети /21 для коммутаторов. Management-VLAN предлагается затерминировать на border. Выполнение этого пункта позволит исключить негативное влияние клиентского трафика на коммутаторы и позволит сократить размер ACL на ТКД за счёт выноса из него правил запрещающих пользователям подставлять ip-адреса из подсети management-интерфейсов коммутаторов. Вынос management'а будет осуществлён, не затрагивая предоставление сервисов клиентам

2. Перенести терминацию пользовательской подсети c border на У-2. На каждый У-2 выделить сеть /21, то есть 2045 адресов для клиентов. Выполнение данного пункта позволит сократить существующий огромный броадкаст домен в десятки раз, что во столько же раз снизит нагрузку на коммутаторы.

3. Поднять ospf-маршрутизацию между У-2 и border'ом, для направления трафика внутри района напрямую с У-2 на У-2 в обход border'а.

4.Вывести многоадресный трафик в отдельный VLAN из пользовательской подсети, это обеспечит беспрепятственный транспорт для введения нового бизнес процесса IP телевидения.

5. Централизовать динамическую выдачу настроек сети пользователям, путём переноса dhcp-сервера с граничного маршрутизатора на сервер находящийся в датацентре компании. Перенос будет осуществлён путём включения функции dhcp-relay на ТКД без прерывания сервиса клиентов. Выполнение данного пункта позволит нам выполнить последующие пункты данного проекта и получать дополнительную информацию о клиенте в полях dhcp option 82, которая может пригодиться для дальнейших разработок.

6. Поднять дистрибуцию статических маршрутов для сетей «локальных ресурсов» с У-2 в сторону клиентов, посредством протокола динамической маршрутизации OSPF. Данный протокол выбран из-за поддержки его операционными системами семейства Microsoft Windows. Данный пункт сделает более простой и удобной настройку клиентам. А главное добавит динамичность маршрутам прописываемых сейчас клиентами статикой

7. Перевести линки между ТКД и У-2 в полноценные транки. Данный пункт при необходимости, позволит легко внедрять QoS на домовой сети.

## **Аппаратное обеспечение модернизированной домовой локальной вычислительной сети**

Модернизированная домовая сеть, построенная по логической схеме, представлена на рисунке 2.1.

Рисунок 2.1

Рассмотрим архитектуру широкополосной сети доступа. Ключевым моментом дизайна сети является трехуровневая модель построения сети.  В сети можно выделить оборудование Уровня Доступа (Access Layer) - это свитчи, к которым подключены клиенты, Уровня Распределения (Aggregation Layer) - узловые свитчи (1ый, 2ой уровни и агрегаторы), Уровня Ядра сети (Backbone Layer).

Таким образом, общая схема сети делится на три уровня:

* Уровень доступа - осуществляет физическую концентрацию абонентских линий. Единицу оборудования данного уровня будем называть ТКД (Точка Коллективного Доступа). ТКД организует разделение абонентов на уровне Ethernet с использованием виртуальных сетей, обеспечивает ограничение скорости передачи данных на входе в сеть и осуществляет базовые функции безопасности.
* Уровень распределения - терминирует виртуальные сети Уровня Доступа с использованием протокола IP.
* Уровень ядра - служит высокоскоростной и надежной магистралью объединяющей все в единое целое.

Серверы широкополосного доступа (*BRAS*) – в качестве серверов широкополосного доступа устанавливаются маршрутизаторы Cisco 7301, на которых терминируются туннельные PPTP/L2TP сессии клиентов, обращающихся в Интернет. Трафик от клиентов в Интернет проходит сквозь серверы широкополосного доступа.

Для реорганизации сети потребуется 1 сервер для переноса dhcp-сервера с граничного маршрутизатора, коммутационное оборудование менять нет необходимости, так как коммутационной мощности и набора функций коммутаторов DES-3526, DXS-3326GSR хватит для основных пунктов модернизации.

**Сервер HP ProLiant DL320 (G3)**

Третье поколение серверов ProLiant DL320 (рисунок 2.2) разработано для работы со специализированными предложениями, используемые на малых и средних предприятиях. Кроме того, благодаря новейшим микросхемам Intel появилось множество новых технических возможностей.

• оптимизированные для плотного размещения, максимальной гибкости и управляемости;

• идеальное решение для развертывания много серверной конфигурации;

• стоечные и кластерные модели.

Рисунок 2.2 – Внешний вид сервера HP ProLiant DL320 (G3)

Таблица 2.1 Технические характеристики HP ProLiant DL320 (G3)

|  |  |
| --- | --- |
| Устройство | Характеристика |
| 1 | 2 |
| Процессор | Intel Pentium 4 3,2 ГГц с поддержкой Hyper-Threading и EM64T |
| Кэш-память | 2 MB кэш-памяти второго уровня |
| Количество процессоров | 1 |
| Набор микросхем | Intel E7221 с шиной FSB 800 МГц |
| Память | 2 ГБ PC3200 DDR SDRAM |
| Сетевой контроллер | двухпортовый интегрированный NC7782 10/100/1000 |
| Слоты расширения | 64-бит/133 МГц PCI-X — 1 (полноразмерный),64-бит/100 МГц PCI-X — 1 (в половину длины) |
| Контроллер/RAID-контроллер | интегрированный двухпортовый SATA контроллер с поддержкой RAID 0/1. |
| Флоппи-дисковод | опционально |
| Оптический привод | опционально |
| Максимальное количество стандартных внутренних дисковых отсеков | 2х1" (SATA или SCSI без горячей замены) |
| Дисковые массивы | 500 ГБ (SATA c/без горячей замены)  |
| Интерфейсы | USB 4 последовательный 1 указательное устройство (мышь) 1графический 1клавиатура 1разъем RJ-45 2 iLO remote management  |
| Графический адаптер | интегрированный видеоконтроллер ATI RAGE XL с 8 МБ видеопамяти SDRAM |
| Форм-фактор | для монтажа в стойку 1U |
| Соответствие отраслевым стандартам | ACPI 2.0, PCI 2.2 Compliant, PXE SupportWOL Support, Microsoft® Logo certificationsUSB 2.0 |
| Функции управления | ASR (Automatic Server Recovery); iLO Advanced Pack (дополнительно); HP Systems Insight Manager; встроенный журнал управления; монитор контроля параметров накопителя (с контроллерами Smart Array); функция динамического восстановления секторов (с контроллерами Smart Array); профилактическая гарантия на жёсткие диски SAS и SCSI, память и процессоры |
| Управление безопасностью | Пароль на включение питания; пароль клавиатуры; контроль дисковода гибких дисков; контроль загрузки с дискеты; контроль порта USB; съёмные приводы для компакт-дисков и флоппи дисков; пароль администратора |
| Блок питания | Блок питания с автоматическим определением, 350 Вт, PFC, соответствие CE Mark |

**Стекируемый коммутатор Gigabit Ethernet 2-го уровня D-LinkDES-3526.**

Рисунок 2.3

Коммутаторы серии 10/100 Мбит/с D-Link DES-3500 являются взаимно стекируемыми коммутаторами уровня доступа, поддерживающими технологию Single IP Management (SIM, управление через единый IP-адрес). Эти коммутаторы, имеющие 24 или 48 10/100BASE-TX портов и 2 комбо-порта 1000BASE-T/SFP Gigabit Ethernet в стандартном корпусе для установки в стойку, разработаны для гибкого и безопасного сетевого подключения. Коммутаторы серии DES-3500 могут легко объединяться в стек и настраиваться вместе с любыми другими коммутаторами с поддержкой D-Link Single IP Management, включая коммутаторы 3-го уровня ядра сети, для построения части многоуровневой сети, структурированной с магистралью и централизованными быстродействующими серверами.

В основном, коммутаторы серии DES-3500 формируют стек сети уровня подразделения, предоставляя порты 10/100 Мбит/с и возможность организации гигабитного подключения к магистрали. Трафик, передаваемый между устройствами стека, проходит через интерфейсы Gigabit Ethernet с поддержкой полного дуплекса и обычные провода сети, позволяя избежать использования дорогостоящих и громоздких кабелей для стекирования. Отказ от использования этих кабелей позволяет устранить барьеры, связанные с их длиной и ограничениями методов стекирования. В стек могут быть объединены устройства, расположенные в любом месте сети, исключая возможность появления любой точки единственного отказа (single point of failure).

Управление через единый IP-адрес (Single IP Management)

Коммутаторы серии DES-3500 упрощают и ускоряют задачу управления, т.к. множество коммутаторов могут настраиваться, контролироваться и обслуживаться через уникальный IP-адрес с любой рабочей станции, имеющей Web-браузер.

Cтек управляется как единый объект, и все устройства стека определяются по единственному IP-адресу. С помощью встроенного Web-менеджера, можно получить информацию, представленную в виде дерева (Tree View) о членах стека и топологии сети с указанием месторасположения устройств стека и связей между ними. Это простое и достаточно эффективное Web-управление исключает необходимость установки дорогого ПО для SNMP-управления.

В стек можно легко объединить до 32-х коммутаторов, независимо от модели. Виртуальный стек поддерживает любые модели коммутаторов со встроенным Single IP Management. Это означает, что стек может быть расширен коммутаторами, включая коммутаторы 3-го уровня для ядра сети, коммутаторы на основе шасси или любые другие коммутаторы.

Серия DES-3500 обеспечивает расширенный набор функций безопасности для управления подключением и доступом пользователей. Этот набор включает Access Control Lists (ACL) на основе МАС-адресов, портов коммутатора, IP адресов и/или номеров портов TCP/UDP, аутентификацию пользователей 802.1х и контроль МАС-адресов. Помимо этого, DES-3500 обеспечивает централизованное управление административным доступом через TACACS+ и RADIUS. Вместе с контролем над сетевыми приложениями, эти функции безопасности обеспечивают не только авторизованный доступ пользователей, но и предотвращают распространение вредоносного трафика по сети

Для повышения производительности и безопасности сети коммутаторы серии DES-3500 обеспечивает расширенную поддержку VLAN, включая GARP/GVRP, 802.1Q и асимметричные VLAN. Управление полосой пропускания позволяет установить лимит трафика для каждого порта, что дает возможность управлять объемом трафика на границе сети. Коммутатор поддерживает установку резервного источника питания. Другие характеристики включают поддержку 802.3ad Link Aggregation, 802.1d Spanning Tree, 802.1w Rapid Spanning Tree и 802.1s Multiple Spanning Tree для повышения надежности и доступности виртуального стека.

Серия DES-3500 имеет широкий набор многоуровневых (L2, L3, L4) QoS/CoS функций, для гарантии того, что критически важные сетевые сервисы, подобные VoIP, ERP, Intranet или видеоконференции будут обслуживаться с надлежащим приоритетом. Поддерживаются 4 очереди приоритетов для 802.1p/TOS/DiffServ с классификацией на основе МАС-адресов источника и приемник, IP-адресов источника или приемника и/или номеров портов TCP/UDP.

**Стекируемый коммутатор Gigabit Ethernet 3-го уровня D-LinkDES- 3326SR.**

Рисунок 2.4

Коммутаторы нового поколения серии xStack DGS-3300 предоставляют сетям крупных предприятий и предприятий малого и среднего бизнеса (SMB) высокую производительность, гибкость, безопасность, многоуровневое качество обслуживания (QoS) и возможность подключения резервного источника питания. Коммутаторы обеспечивают высокую плотность гигабитных портов для подключения рабочих мест, оснащены слотами SPF для гибкого подключения по оптике, слотами для установки модулей расширения с портами 10 Gigabit Ethernet и поддерживают расширенные функции программного обеспечения. Коммутаторы можно использовать в качестве устройств уровня доступа подразделений или в ядре сети для создания многоуровневой сетевой структуры с высокоскоростными магистралями и централизованным подключением серверов. Провайдеры услуг могут также использовать преимущества коммутаторов с высокой плотностью портов SFP для формирования ядра оптической сети (FTTB).

**Виртуальный стек.**

Любой из коммутаторов серии DGS-3300 может функционировать в качестве автономного устройства или части масштабируемого стека. Встроенная поддержка технологии Single IP Management позволяет автономному коммутатору стать частью виртуального стека, в котором внутристековый трафик передается по обычным сетевым кабелям, исключая необходимость использования дорогостоящих специализированных кабелей для стекирования. Это позволяет избежать проблем, связанных с длиной кабелей и методом физического стекирования и объединить в виртуальный стек устройства, расположенные в любом месте сети, минимизируя влияние единой точки возможного отказа.

**Безопасность, производительность и доступность**

Коммутаторы серии DGS-3300 предоставляют широкий набор функций безопасности, включая многоуровневые L2/L3/L4 списки контроля доступа и аутентификацию пользователей 802.1x через серверы TACACS+ и RADIUS. Кроме того, они поддерживают статическую IP v.4/v.6 маршрутизацию на 3 уровне для повышения производительности и безопасности сети. Встроенная технология ZoneDefense представляет собой механизм, позволяющий совместно работать коммутаторам D-Link серии xStack и межсетевым экранам и обеспечивающий активную сетевую безопасность. Функция Zone-Defense автоматически изолирует инфицированные компьютеры сети и предотвращает распространение ими вредоносного трафика.

Для повышения производительности и безопасности коммутаторы серии DGS-3300 обеспечивают расширенную поддержку VLAN, включая GARP/GVRP и 802.1Q. Для поддержки объединенных приложений, включая VoIP, ERP и видеоконференций, широкий набор функций QoS/CoS 2/3/4 уровней гарантирует, что критичные к задержкам сетевые сервисы будут обслуживаться в приоритетном режиме. Для предотвращения загрузки центрального процессор обработкой вредоносного широковещательного трафика, генерируемого злоумышленниками или обусловленного вирусной активностью, коммутаторы серии DGS-3300 предоставляют функцию D-Link Safeguard Engine, позволяющую повысить надежность и доступность сети. Благодаря поддержке функции контроля полосы пропускания для каждого порта можно устанавливать лимиты, гарантируя определенный уровень обслуживания для конечных пользователей. Функция управления полосой пропускания для каждого потока позволяет настраивать типы обслуживания на основе определенных IP-адресов или протоколов.

**2.3 Программное обеспечение и настройка коммутационного оборудования**

Структура исходной сети представленной на рисунке 2.5 является работающей системой приносящей доход, следовательно, предоставление сервиса для конечных абонентов является приоритетной задачей. При проведение всех работ по реорганизации схемы управления и оптимизации структуры, необходимо обеспечить минимальное прерывание сервиса и возможность отката на старую работающую схему.

Рисунок 2.5

**1. Этап подготовки сети.**

**Определение точной топологии домашней сети, если требуется заведение заявок на исправление (при наличии каких- либо временных каналов связи, каскадных подключениях) Проверка коммутаторов, определение портов сегмента.**

**2. Выделение требуемого количества сетей для реализации проекта.**

**Cети для работы OSPF /30**

**Cети для users /21**

**Cети для management /22**

**Сформировать конфиг DHCP сервера.**

**3. Подготовка конфигов:**

**Коммутаторов ДС для динамического формирования неблокируемого сервера DHCP**

**Магистрального оборудования для организации должного пиринга.**

**4. Запуск маршрутизации:**

**Терминируем интерфейсы на граничном маршрутизаторе**

**Терминируем интерфейсы на узлах сегментов**

**Убедиться, что маршрутизация работает правильно и сети анонсируются.**

**Удалить default route на узлах, убедиться что маршрут пришел по OSPF.**

**5.Запуск пользователей**

**Удаляем аплинк из влана пользователей**

**Терминируем пользователей на У2**

**Запускаем DHCP.**

**6. Убеждаемся, что пользователи начали получать ip и подключаться к vpn серверу.**

Все пункты будут выполняться последовательно, с оповещением клиентов и необходимыми промежутками для перехода клиентов на новую адресацию. Планируемый перерыв сервиса не больше минуты на каждого клиента. Проект внедряется на существующем оборудовании без каких либо существенных материальных затрат. L3 трафик проходящий через У-2 достаточно мал и ресурсов DXS-3326GSR вполне хватит для такой схемы организации, единственное затрагивающее нас ограничение в нём это размер таблицы ipfdb в 3000 записей, но при подключении более 2500 клиентов в сегменте - его легко заменить на более мощный, например DGS-3627G с таблицей ipfdb в 8000 записей. L3 функции на У-1 задействованы не будут, и значит повышенных требований к нему не предъявляется. Настройка активного оборудование находиться в Приложение 1.

Расширение входящего канала. При строительстве оптических линий связи используется многожильный оптический кабель. При наличии свободных волокон можно расширить входящий канал, используя технологию агрегирование каналов — технология, которая позволяет объединить несколько физических каналов в один логический. Такое объединение позволяет увеличивать пропускную способность канала и увеличить надежность канала. Агрегирование каналов может быть настроено как между двумя коммутаторами, так и между коммутатором и сервером. Настройка активного оборудование находиться в Приложение 1.

В качестве платформы для сервера DHCP предлагается использовать Unix-подобную операционную система для ПК, основанную на самых различных, современных архитектурах. Эта операционная система выбрана в первую очередь из-за своей очень высокой надёжности, стабильности, защищённости и высокой производительности. Так же важную роль в выборе этой операционной системы сыграли факторы, что она является операционной системой с открытым кодом и для неё доступны тысячи бесплатных пакетов и прикладных программ. Можно настроить сервер DHCP, используя файл конфигурации /etc/dhcpd.conf приложение 2.

## **Информационная безопасность модернизированной домовой локальной вычислительной сети**

Безопасность в локальной сети должна обеспечивать администрация сети, но пользователи тоже не должны забывать о безопасности в сети, так как большинство вредоносных программ распространяются через компьютеры пользователей. Таким образом требуется комплекс мер для обеспечения информационной безопасности в сети, как со стороны администрации, так и со стороны рядовых пользователей.

Пользователям сети нужно защищать только свой компьютер, что бы сохранить целостность конфиденциальной информации, скрыть её от других пользователей сети, так же компьютер может стать рассадником вирусов и всевозможных сетевых червей, которые будут мешать работать всем пользователям сети создавая создавать большой локальный трафик. Что бы пользователю защитить свой компьютер ему необходим комплекс программного обеспечения для обеспечения безопасности.

Существует множество программных комплексов защиты компьютера. Например: Kaspersky Internet Security, Norton Internet Security, Panda Internet Security, F-Secure Internet Security и т.д.

Состав этих программных комплексов почти одинаковый и в них входят следующие компоненты:

1. Антивирус:

• Программа осуществляет антивирусную проверку почтового трафика на уровне протокола передачи данных (POP3, IMAP и NNTP для входящих сообщений и SMTP для исходящих сообщений) независимо от используемой почтовой программы;

• Проверка интернет-трафика. Обеспечивает антивирусную проверку интернет-трафика, поступающего по сетевым протоколам, так же осуществляется отдельная проверка HTTP трафика на предмет spyware. В режиме реального времени, позволяя таким образом предотвратить заражение ещё до момента сохранения файлов на жестком диске компьютера;

• Защита файловой системы. Антивирусной проверке подвергаются любые отдельные файлы, каталоги и диски, так же возможна проверка только критических областей операционной системы и объектов, загружаемых при старте ОС;

• Проактивная защита. Осуществляется постоянное наблюдение за активностью программ и процессов, запущенных в оперативной памяти компьютера, и своевременно предупреждает пользователя в случае появления опасных, подозрительных или скрытых процессов; предотвращает опасные изменения файловой системы и реестра, а также восстанавливает систему после вредоносного воздействия.

1. Брандмауэр:

• Блокирует сетевые атаки. Фиксирует попытки сканирования портов компьютера, часто предшествующие сетевым атакам, и успешно отражает наиболее распространенные типы хакерских атак, запрещая взаимодействие с атакующим компьютером. Мониторинг сетевой активности позволяет вести статистику всех соединений;

• Контролирует все сетевые взаимодействия. На основе заданных правил программа контролирует обращения приложений к источникам в сети Интернет и отслеживает входящие и исходящие пакеты данных;

• Делает безопасной работу в любых сетях;

• Обладает режимом невидимости при работе в интернете. Режим невидимости предотвращает обнаружения компьютера извне. При переключении в этот режим запрещается вся сетевая деятельность, кроме предусмотренных правилами исключений, которые определяются самим пользователем.

## **Выводы по проектной части**

По итогам проведенных этапов по реорганизации схемы управления и оптимизации сети были достигнуты следующие результаты:

снижена загрузка процессорной мощности оборудования рисунок 2.6, 2.7

Рисунок 2.6 –загрузка процессора до сегментации

Рисунок 2.7 –загрузка процессора после сегментации

Сокращен броадкаст домен в десятки раз. Исключено влияние пользователей на оборудование за счет разноса терминации пользовательского интерфейса и интерфейса менеджмента на различном оборудовании.

У узловых коммутаторов создано 3 интерфейса (рисунок 2.8) на которые можно удаленно попасть, и в случае ненормальной активности в сегменте можно будет быстро локализовать проблему, сегмент в среднем состоит из 15-20 домов.

Рисунок 2.8 –интерфейсы оборудования

Трафик между пользователями маршрутизируется напрямую на узловых коммутаторах и не загружает граничный маршрутизатор. Так же для равномерности загрузки с граничного маршрутизатора перенесен DHCP сервер в дата-центр компании.

Сеть подготовлена к росту клиентской базы, вводу в эксплуатацию нового сервиса IPTV, расширен входящий канал до 2гбит\сек, что позволит увеличить скорость на клиентских тарифах.

# Охрана труда

##  **Исследование возможных опасных и вредных факторов при эксплуатации ЭВМ и их влияния на пользователей**

###  Введение

Охрана труда — это система законодательных актов, социально-экономических, организационных, технических, гигиенических и лечебно-профилактических мероприятий и средств, обеспечивающих безопасность, сохранение здоровья и работоспособности человека в процессе труда.

Полностью безопасных и безвредных производственных процессов не существует. Задача охраны труда — свести к минимуму вероятность поражения или заболевания работающего с одновременным обеспечением комфорта при максимальной производительности труда.

Любой производственный процесс, в том числе работа с ЭВМ, связан с появлением опасных и вредных факторов.

Опасный фактор — это производственный фактор, воздействие которого на работающего в определенных условиях приводит к травме или другому резкому внезапному ухудшению здоровья.

Вредный фактор — производственный фактор, приводящий к заболеванию, снижению работоспособности или летальному исходу. В зависимости от уровня и продолжительности воздействия вредный производственный фактор может стать опасным.

В процессе использования ПЭВМ различные вредные факторы, связанные с работой на персональном компьютере, угрожают здоровью, а иногда и жизни оператора. Типичными ощущениями, которые испытывают к концу дня люди, работающие за компьютером, являются: головная боль, резь в глазах, тянущие боли в мышцах шеи, рук и спины, зуд кожи на лице и т. п. Испытываемые каждый день, они могут привести к мигреням, частичной потере зрения, сколиозу, тремору, кожным воспалениям и другим нежелательным явлениям.

Была также выявлена связь между работой на компьютере и такими недомоганиями, как астенопия (быстрая утомляемость глаза), боли в спине и шее, запястный синдром (болезненное поражение срединного нерва запястья), тендениты (воспалительные процессы в тканях сухожилий), стенокардия и различные стрессовые состояния, сыпь на коже лица, хронические головные боли, головокружения, повышенная возбудимость и депрессивные состояния, снижение концентрации внимания, нарушение сна и немало других, которые не только ведут к снижению трудоспособности, но и подрывают здоровье людей.

Основным источником проблем, связанных с охраной здоровья людей, использующих в своей работе автоматизированные информационные системы на основе персональных компьютеров, являются дисплеи (мониторы), особенно дисплеи с электронно-лучевыми трубками. Они представляют собой источники наиболее вредных излучений, неблагоприятно влияющих на здоровье операторов и пользователей.

Конфигурация компьютеризированного рабочего места для работы над дипломом:

* ПК на основе процессора QuadCore Intel Core 2 Quad Q6600, 2400 MHz с необходимым набором устройств ввода-вывода и хранения информации (DVD-RW, HDD);
* лазерный принтер XEROX Phaser 3122 (A4);
* цветной SVGA-монитор LG 17” (TCO 99):
	+ разрешение по горизонтали (max) — 1280 пикселей; разрешение по вертикали (max) — 1024 пикселей;
	+ легко регулируемые контрастность и яркость;
	+ частота кадровой развертки при максимальном разрешении — 56-75 Гц;
	+ частота строчной развертки при максимальном разрешении — 30-83 кГц.

Питание ПЭВМ производится от сети 220В. Так как безопасным для человека напряжением является напряжение 40В, то при работе на ПЭВМ опасным фактором является поражение электрическим током.

В дисплее ПЭВМ высоковольтный блок строчной развертки и выходного строчного трансформатора вырабатывает высокое напряжение до 25кВ для второго анода электронно — лучевой трубки. А при напряжении от 5 до 300 кВ возникает рентгеновское излучение различной жесткости, которое является вредным фактором при работе с ПЭВМ (при 15-25 кВ возникает мягкое рентгеновское излучение).

Изображение на ЭЛТ создается благодаря кадрово-частотной развертке с частотой:

* 85 Гц (кадровая развертка);
* 42 кГц (строчная развертка).

Следовательно, пользователь попадает в зону электромагнитного излучения низкой частоты, которая является вредным фактором.

Во время работы компьютера дисплей создает ультрафиолетовое излучение, при повышении плотности которого > 10 Вт/м2, оно становиться для человека вредным фактором. Его воздействие особенно сказывается при длительной работе с компьютером.

Любые электронно-лучевые устройства, в том числе и электронно-вычислительные машины во время работы компьютера вследствие явления статического электричества происходит электризация пыли и мелких частиц, которые притягивается к экрану. Собравшаяся на экране электризованная пыль ухудшает видимость, а при повышении подвижности воздуха, попадает на лицо и в легкие человека, вызывает заболевания кожи и дыхательных путей.

### Выводы

При эксплуатации перечисленных элементов вычислительной техники могут возникнуть следующие опасные и вредные факторы:

1. Поражение электрическим током.
2. Электромагнитное излучение.
3. Ультрафиолетовое излучение.
4. Статическое электричество.

###  Анализ влияния опасных и вредных факторов на пользователя

#### Влияние электрического тока

Проходя через тело человека, электрический ток оказывает следующие воздействия:

1. Термическое — нагрев тканей и биологической среды.
2. Электролитическое — разложение крови и плазмы.
3. Биологическое — способность тока возбуждать и раздражать живые ткани организма.
4. Механическое — возникает опасность механического травмирования в результате судорожного сокращения мышц.

Тяжесть поражения электрическим током зависит от: величины тока, времени протекания, пути протекания, рода и частоты тока, сопротивления человека, окружающей среды, состояния человека, пола и возраста человека. Последствия влияния электрического тока на организм человека представлены на иллюстрации «1. Последствия влияния электрического тока на организм человека»

Электрический ток, воздействуя на человека, приводит к травмам:

* общие травмы:
	+ судорожное сокращение мышц, без потери сознания;
	+ судорожное сокращение мышц, с потерей сознания;
	+ потеря сознания с нарушением работы органов дыхания и кровообращения;
	+ состояние клинической смерти.
* местные травмы:
	+ электрические ожоги;
	+ электрический знак;
	+ электроавтольмия.

Наиболее опасным переменным током является ток 20-100Гц. Так как компьютер питается от сети переменного тока частотой 50Гц, то этот ток является опасным для человека.

#### Влияние электромагнитных излучений

Электромагнитные поля с частотой 60 Гц и выше могут инициировать изменения в клетках животных (вплоть до нарушения синтеза ДНК). В отличие от рентгеновского излучения, электромагнитные волны обладают необычным свойством: опасность их воздействия при снижении интенсивности не уменьшается, мало того, некоторые поля действуют на клетки тела только при малых интенсивностях или на конкретных частотах. Оказывается переменное электромагнитное поле, совершающее колебания с частотой порядка 60 Гц, вовлекает в аналогичные колебания молекулы любого типа, независимо от того, находятся они в мозге человека или в его теле. Результатом этого является изменение активности ферментов и клеточного иммунитета, причем сходные процессы наблюдаются в организмах при возникновении опухолей.

#### Влияние ультрафиолетового излучения

Ультрафиолетовое излучение — электромагнитное излучение в области, которая примыкает к коротким волнам и лежит в диапазоне длин волн ~ 200-400 нм.

Различают следующие спектральные области:

1. 200-280 нм — бактерицидная область спектра.
2. 280-315 нм — зрительная область спектра (самая вредная).
3. 315-400 нм — оздоровительная область спектра.

При длительном воздействии и больших дозах могут быть следующие последствия:

1. Серьезные повреждения глаз (катаракта).
2. Меломанный рак кожи.
3. Кожно-биологический эффект (гибель клеток, мутация, канцерогенные накопления).
4. Фототоксичные реакции.

#### Влияние статического электричества

Результаты медицинских исследований показывают, что электризованная пыль может вызвать воспаление кожи, привести к появлению угрей и даже испортить контактные линзы. Кожные заболевания лица связаны с тем, что наэлектризованный экран дисплея притягивает частицы из взвешенной в воздухе пыли, так, что вблизи него «качество» воздуха ухудшается, и оператор вынужден работать в более запыленной атмосфере. Таким же воздухом он и дышит.

Особенно стабильно электростатический эффект наблюдается у компьютеров, которые находятся в помещении с полами, покрытыми синтетическими коврами.

При повышении напряженности поля Е>15 кВ/м, статическое электричество может вывести из строя компьютер.

Из анализа воздействий опасных и вредных факторов на организм человека следует необходимость защиты от них.

##  **Методы и средства защиты пользователей от воздействия на них опасных и вредных факторов**

###  Методы и средства защиты от поражения электрическим током

Зануление — преднамеренное соединение нетоковедущих частей с нулевым защитным проводником (иллюстрация 2, стр. 9).

Защитное зануление применяется в трехфазных сетях с глухо заземленной нейтралью, в установках до 1000В и является основным средством обеспечения электробезопасности.

Принцип защиты пользователей при занулении заключается в отключении сети за счет тока короткого замыкания, который вызывает отключение ПЭВМ от сети.

Для отключения ПЭВМ от сети в случае короткого замыкания или других неисправностей в цепь питания ПЭВМ необходимо ставить автомат с Jном = 8 А.

###  Методы и средства защиты от ультрафиолетового излучения

Энергетической характеристикой является плотность потока мощности [Вт/м2].

Биологический эффект воздействия определяется внесистемной единицей эр: 1 эр — это поток (280-315 нм), который соответствует потоку мощностью 1 Вт.

Воздействие ультрафиолетового излучения сказывается при длительной работе за компьютером.

Максимальная доза облучения:

* 7.5 мэр\*ч/ м2 за рабочую смену;
* 60 мэр\*ч/м2 в сутки.

Для защиты от ультрафиолетового излучения применяют:

* защитный фильтр или специальные очки (толщина стекол 2 мм, насыщенных свинцом);
* одежда из фланели и поплина;
* побелка стен и потолка (ослабляет на 45-50%).

###  Методы и средства защиты от статического электричества

Защита от статического электричества и вызванных им явлений осуществляется следующими способами:

* проветривание без присутствия пользователя;
* влажная уборка;
* отсутствие синтетических покрытий;
* нейтрализаторы статического электричества;
* подвижность воздуха в помещении не более 0.2 м/с;
* иметь контурное заземление.

Для защиты от статического электричества предусмотрены специальные шнуры питания с встроенным заземлением. Там, где это не используется (отсутствует розетка) необходимо заземлять корпуса оборудования.

Также для защиты от воздействия электрического тока все корпуса оборудования, клавиатура, защелки дисководов и кнопки управления выполнены из изоляционного материала.

Для уменьшения влияния статического электричества необходимо пользоваться рабочей одеждой из малоэлектризующихся материалов, например халатами из хлопчатобумажной ткани, обувью на кожаной подошве. Не рекомендуется применять одежду из шелка, капрона, лавсана.

###  Методы и средства защиты от электромагнитных полей низкой частоты

Защита от электромагнитных излучений осуществляется следующими способами:

* время непрерывной работы — не более 4 часов в сутки, суммарное время работы за неделю — не более 20 часов;
* расстояние — не менее 50 см от источника;
* экранирование экрана монитора, поверхность экрана покрывается слоем оксида олова, либо в стекло ЭЛТ добавляется оксид свинца;
* расстояние между мониторами — не менее 1,5 м;
* не работать слева от монитора ближе 1.2 м, сзади — 1 м.

###  Общие рекомендации при работе с вычислительной техникой

Для защиты от вредных факторов имеющих место при эксплуатации ЭВМ необходимо придерживаться следующих рекомендаций:

* правильно организовывать рабочие места;
* правильно организовать рабочее время оператора, соблюдая ограничения при работе с вычислительной техникой.

###  Требования к помещениям и организации рабочих мест

Особые требования к помещениям, в которых эксплуатируются компьютеры:

1. Не допускается расположение рабочих мест в подвальных помещениях.
2. Площадь на одно рабочее место должна быть не меньше 6 м2, а объем — не менее 20 м3.
3. Для повышения влажности воздуха в помещениях с компьютерами следует применять увлажнители воздуха, ежедневно заправляемые дистиллированной или прокипяченной питьевой водой. Перед началом и после каждого часа работы помещения должны быть проветрены.

Рекомендуемый микроклимат в помещениях при работе с ПЭВМ:

* температура 19- 21°С;
* относительная влажность воздуха 55-62%.

В помещениях, где размещены шумные агрегаты вычислительных машин (матричные принтеры и тому подобное), уровень шума не должен превышать 75 дБА, в обычных же помещениях, где стоят персональные машины, допускается максимум 65 дБА.

Снизить уровень шума в помещениях с мониторами и ПЭВМ можно использованием звукопоглощающих материалов с максимальными коэффициентами звукопоглощения в области частот 63-8000 Гц для отделки помещений (разрешенных органами и учреждениями Госсанэпиднадзора России), подтвержденных специальными акустическими расчетами.

Дополнительным звукопоглощением служат однотонные занавеси из плотной ткани, гармонирующие с окраской стен и подвешенные в складку на расстоянии 15-20 см от ограждения. Ширина занавеси должна быть в 2 раза больше ширины окна.

Помещения должны иметь естественное и искусственное освещение. Желательна ориентация оконных проемов на север или северо-восток. Оконные проемы должны иметь регулируемые жалюзи или занавеси, позволяющие полностью закрывать оконные проемы. Занавеси следует выбирать одноцветные, гармонирующие с цветом стен, выполненные из плотной ткани и шириной в два раза больше ширины оконного проема. Для дополнительного звукопоглощения занавеси следует подвешивать в складку на расстоянии 15-20 см от стены с оконными проемами.

Рабочие места по отношению к световым проемам должны располагаться так, чтобы естественный свет падал сбоку, преимущественно-слева.

Для устранения бликов на экране, также как чрезмерного перепада освещенности в поле зрения, необходимо удалять экраны от яркого дневного света.

Рабочие места должны располагаться от стен с оконными проемами на расстоянии не менее 1,5 м, от стен без оконных проемов на расстоянии не менее 1,0 м.

Поверхность пола в помещениях должна быть ровной, без выбоин, не скользкой, удобной для чистки и влажной уборки, обладать антистатическими свойствами.

Освещенность на рабочем месте с ПЭВМ должна быть не менее:

* экрана — 200 лк;
* клавиатуры, документов и стола — 400 лк.

Для подсветки документов допускается установка светильников местного освещения, которые не должны создавать бликов на поверхности экрана и увеличивать его освещенность до уровня более 300 лк. Следует ограничивать прямые блики от источников освещения.

Освещенность дисплейных классов, рекомендуемая отраслевыми нормами лежит в пределах 400-700 лк и мощностью ламп до 40Вт.

В качестве источников света при искусственном освещении необходимо применять преимущественно люминесцентные лампы типа ЛБ цветовая температура (Тцв) излучения которых находится в диапазоне 3500-4200°K.

Допускается применение ламп накаливания в светильниках местного освещения. Для того чтобы избегать ослепления, необходимо устранять из поля зрения оператора источники света (лампы, естественный солнечный свет), а также отражающие поверхности (например, поверхность блестящих полированных столов, светлые панели мебели). При электрическом освещении упомянутые требования могут быть удовлетворены при выполнении следующих условий: освещение должно быть не прямым, для чего необходимо избегать на потолке зон чрезмерной освещенности. При этом освещенность должна быть равномерной, потолок должен быть плоским, матовым и однородным. Необходима также достаточная высота потолка для возможности регулирования высоту подвеса светильников.

При установке рабочих мест нужно учитывать, что мониторы должны располагаться на расстоянии не менее 2 метров друг от друга, если брать длины от задней поверхности одного до экрана другого, и 1,2 метра между их боковыми поверхностями. При выполнении творческой работы, требующей «значительного умственного напряжения или высокой концентрации внимания», между компьютерами должны быть установлены перегородки высотой 1,5-2,0 метра.

Дисплей должен поворачиваться по горизонтали и по вертикали в пределах 30 градусов и фиксироваться в заданном направлении. Дизайн должен предусматривать окраску корпуса в мягкие, спокойные тона с диффузным рассеиванием света. Корпус дисплея, клавиатура и другие блоки и устройства должны иметь матовую поверхность одного цвета с коэффициентом отражения 0.4-0.6 и не иметь блестящих деталей, способных создавать блики.

Рабочий стул должен быть подъемно-поворотным и регулируемым по высоте и углам наклона сиденья и спинки, а также расстоянию спинки от переднего края сиденья.

Экран монитора должен находиться от глаз пользователя на расстоянии 600-700 мм, но не ближе 500 мм. В помещениях ежедневно должна проводиться влажная уборка.

Рабочее место должно быть оборудовано подставкой для ног, шириной не менее 300 мм, глубину не менее 400 мм, регулировку по высоте в пределах 150 мм и по углу наклона опорной поверхности до 20 градусов. Клавиатуру следует располагать на поверхности стола на расстоянии 100-300 мм от края, обращенного к пользователю, или на специальной, регулируемой по высоте рабочей поверхности.

###  Требования к организации работы

Для преподавателей вузов и учителей средних учебных заведений длительность работы в дисплейных классах устанавливается не более 4 часов в день. Для инженеров, обслуживающих компьютерную технику, — не более 6 часов в день. Для обычного пользователя продолжительность непрерывной работы за компьютером без перерыва не должна превышать 2 часов.

Необходимо делать 15-минутные перерывы каждые 2 часа, менять время от времени позу.

Для тех, у кого смена работы за компьютером 12 часов, установлено — в течение последних четырех часов каждый час должен прерываться 15-минутным перерывом.

При работе с ПЭВМ в ночную смену, независимо от вида и категории работ, продолжительность регламентированных перерывов увеличивается на 60 минут. В случаях возникновения у работающих с ПЭВМ зрительного дискомфорта и других неблагоприятных субъективных ощущений, несмотря на соблюдение санитарно-гигиенических, эргономических требований, режимов труда и отдыха следует применять индивидуальный подход в ограничении времени работ с ПЭВМ и коррекцию длительности перерывов для отдыха или проводить смену деятельности на другую, не связанную с использованием ПЭВМ.

Профессиональные пользователи обязаны проходить периодические медицинские осмотры. Женщины во время беременности и в период кормления ребенка грудью к работе за компьютером не допускаются.

Необходимо строго регламентировать время и условия работы с компьютером для сотрудников, страдающих заболеваниями опорно-двигательного аппарата, глаз и т.д.

Выбранные методы и способы защиты пользователей от воздействии на них опасных и вредных факторов, при соблюдении эргономических требований, позволяют обеспечить безопасную работу и здоровье.

## **Заключение**

В результате проектирования было произведено успешное внедрение технологии *VLAN****.***

Благодаря данной технологии загруженность текущего оборудования значительно снизилась, появились перспективы масштабирования пользовательских сервисов. Так с внедрением технологии VLAN стал возможен запуск таких сервисов как IPTV (цифровое телевидение), VoIP (телефония), появилась возможность увеличения скорости на клиентских тарифах, за счет увеличения пропускной способности внешнего канала связи.

Подводя итоги всему вышесказанному, следует отметить, что все задачи, поставленные в техническом задании, выполнены. Оптимизация работы сети проведена успешно, и мы получили заметный потенциал для внедрения и развития современных сервисов на сети.

## **Список использованной литературы**

1. М. Гук «Аппаратные средства локальных сетей.» Энциклопедия - СПб.: Питер, 2004 г. – 573 с.
2. Дж. Скотт Хокдал «Анализ и диагностика компьютерных сетей.» - М.: Лори, 2001 г. – 353 с.
3. Олифер В. Г., Олифер Н. А. Компьютерные сети: принципы, технологии, протоколы. – Учебник для ВУЗов, СПб.: 2004. – 864 с.
4. Поляк-Брагинский «Обслуживание и модернизация локальных сетей.» - Питер, 2005 г. – 546 с.
5. Терри Джонсон. Модернизация и ремонт сетей. – М.: Диалектика-Вильямс, 2000. – 944 с.
6. Шиндер Дебра. Основы компьютерных сетей. – М.: Диалектика-Вильямс, 2002. – 656 с.
7. Дансмор Брэдли, Скандьер. Справочник по телекоммуникационным технологиям. – М.: Диалектика-Вильямс, 2003. – 640 с.
8. Амато, Вито. Основы организации сетей Cisco, том 1, Пер. с англ. – М.: Издательский дом “Вильямс”, 2004. – 512 c.
9. http://www.dlink.ru/products/index.php Технические характеристики оборудования фирмы dlink.
10. «Методические указания по организации и проведению дипломного проектирования», к.т.н., доцент Медведев В.В., Москва, МГИЭМ 2008.
11. ГОСТ 12.0.003-86 Опасные и вредные производственные факторы. Классификация.
12. «Охрана труда на ВЦ», Сибаров Ю.Г. и др. М. 1989 г.
13. ГОСТ 12.1.030-81 Электробезопасность. Защитные заземления, зануления.
14. САНПиН 1340-03 Гигиенические требования к персональным ЭВМ и организация работы.
15. ФЗ РФ №181 1999 г. «Об основах охраны труда в РФ».