Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное
учреждение высшего образования
«Севастопольский государственный университет»

В.С.ЧЕРНЕГА

ПРОЕКТИРОВАНИЕ ЛОКАЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ УРОВНЯ ОРГАНИЗАЦИЙ И ПРЕДПРИЯТИЙ

Учебное пособие
по курсовому проектированию
для высших учебных заведений

Севастополь 2019

ББК 32.973.202 я73
Ч 46
УДК 681.324 (075)

Рецензенты:

Апраксин Ю.К. проф., д-р техн. наук, профессор кафедры «Информационные технологии и компьютерные системы», Севастопольский государственный университет

Шувалов В.П. проф., д-р техн. наук, зав. кафедрой передачи дискретных сообщений и метрологии. Сибирский государственный университет телекоммуникаций и информатики

Чернега В.С.

Проектирование локальных компьютерных сетей уровня предприятий и организаций: Учебное пособие по курсовому проектированию для высших учебных заведений / В. Чернега, — Севастополь: «Издательство СевГУ», 2019.— 291 с.

ISBN

Учебное пособие предназначено для студентов университетов, обучающихся по направлениям «Информационные системы и технологии», «Прикладная информатика», «Информатика и вычислительная техника», «Управление в технических системах». В нем изложены основные положения и методика проектирования локальных компьютерных сетей уровня предприятий и организаций. Освещены топологии локальных сетей разнообразных уровней, особенности размещения серверов, проектирования структурированных кабельных систем, разработки политики безопасности, построения и использования сетевых коммутаторов и маршрутизаторов в локальных сетях и их конфигурирования.

Приведены много примеров сценариев конфигурации коммутаторов Cisco, D-link и Huawei для реализации разнообразных сетевых функций. Один из разделов пособия посвящен компьютерному моделированию спроектированной сети с целью проверки ее функционирования и соответствия параметров сети техническому заданию. Приведена методика и пример выполнения курсового проекта и варианты заданий.

ISBN
ББК

Содержание

Список сокращений

ВОЛС	Волоконно-оптическая линия связи
ИР	Информационная розетка
ЛКМ	Левая кнопка мышки
ЛКС	Локальная компьютерная сеть
КЗ	Кроссовая здания
КС	Компьютерная сеть
МК	Магистральный кабель
МККТТ	Международный консультативный комитет по телефонии и телеграфии
ОЗУ	Оперативное запоминающее устройство
ОС	Операционная система
ПЭВМ	Персональная электронно-вычислительная машина
ПЗУ	Постоянное запоминающееся устройство
ПКМ	Правая кнопка мышки
ПО	Программное обеспечение
РП	Распределительный пункт
РПЗ	Распределительный пункт здания
РПЭ	Распределительный пункт этажа
РС	Рабочая станция
РПЗ	Распределительный пункт здания
РПК	Распределительный пункт кампуса
РПЭ	Распределительный пункт этажа
СВТ	Средства вычислительной техники
СКС	Структурированная кабельная система
СУБД	Система управления базами данных
СФ	Серверная ферма
ТП	Точка перехода между кабелями различных типов
ТР	Телекоммуникационный разъем/розетка
УАТС	Учрежденческая автоматическая телефонная станция
УК	Узел коммутации
УОД	Устройство обслуживания данных
УОК	Устройство обслуживания канала
ФС	Файл-сервер
ЦОД	Центр обработки данных

AAL	*ATM Adaptation Layer*	Уровень адаптации ATM
ABR	*Available Bit Rate*	Трафик с доступной скоростью
ACL	*Access Control List*	Список контроля доступа

ACR	*Attenuation to crosstalk Ratio*	Защищенность от переходных помех
ANSI	*American National Standards Institute*	Американский институт стандартизации
AON	*Actsive Optical Network*	Активная оптическая сеть доступа
ARP	*Address Resolution Protocol*	Протокол преобразования адресов
ATM	*Asynchronous Transfer Mode*	Режим асинхронной передачи
AUX	*Auxiliary*	Порт дополнительного устройства
AWG	*American Wire Gauge*	Американский калибр проводов
BGP4	*Border Gateway Protocol 4*	Протокол граничного шлюза
BPDU	*Bridge Protocol Data Unit*	Протокольный блок данных моста
BRI	*Basic Rate Interface*	Интерфейс базовой скорости
CBR	*Constant Bit Rate*	Трафик с постоянной скоростью
CFI	*Canonical Format Indicator*	Индикатор формата
CHAP	*Challenge Handshake Authentication Protocol*	Протокол проверки подлинности
CIDR	*Classless Inter-Domain Routing*	Бесклассовая адресация
CIR	*Committed Information Rate*	Гарантированная полоса пропускания
CLI	*Command Line Interface*	Интерфейс командной строки
CMS	*Cisco Cluster Management Suite*	Система управления кластером
CO	*Central Office*	Центральный офис
COS	*Catalyst Operating System*	Операционная система коммутаторов
CoS	*Class of Service*	Класс обслуживания
CSMA/CD	*Carrier Sense Multiple Access with Collision Detection*	Множественный доступ с контролем несущей и обнаружением коллизий
CSU	*Channel Service Unit*	Устройство обслуживания канала
CWDM	*Coarse Wavelength Division Multiplexing*	Грубое спектральное мультиплексирование
CWSI	*Cisco Works for Switched Internetworks*	Система управления для коммутируемых сетей
DCE	*Data Circuit Terminating Equipment*	Оборудование канала данных
DDM	*Digital Diagnostic Monitoring*	Система диагностики и мониторинга

DHCP	*Dynamic Host Configuration Protocol*	Протокол динамической конфигурации хостов
DLCI	*Data-Link Connection Identifier*	Идентификатор канального соединения
DMZ	*Demilitarized Zone*	Демилитаризованная зона
DNS	*Domain Name System*	Служба доменных имен
DOM	*Digital Optical Monitoring*	Цифровой оптический контроль
DRAM	*Dynamic Random Access Memory*	Динамическое ОЗУ с произвольным доступом
DSL	*Digital Subscriber Line*	Цифровая абонентская линия
DSCP	*Differentiated Services Code Point*	Код дифференциального обслуживания
DSU	*Data Service Unit*	Устройство обслуживания данных
DTE	*Data Terminal Equipment*	Оконечное оборудование данных
EEE	*Energy Efficient Ethernet*	Технология сокращение энергопотребления
EFM	*Ethernet in the First Mile*	Ethernet на первой миле
EFTTH	*Ethernet* FTTH	Оптоволокно до сетевого узла с использованием *Ethernet*
EIA	*Electronics Industries Association*	Ассоциация электронной индустрии
EIRGP	*Enhanced Interior Gateway Routing Protocol*	Усовершенствованный внутренний протокол маршрутизации шлюзов
EPON	*Ethernet Passive Optical Nerwork*	Ethernet пассивная оптическая сеть доступа
EPON PMD	EPON *Physical Medium Dependent*	Физический уровень сети EPON
ESF	*Extended Superframe Framing*	Метод расширенного суперкадра
FC	*Fiber Connector*	Оптический коннектор
FDDI	*Fiber Distributed Data Interface*	Высокоскоростной сетевой стандарт
FEC	*Fast EtherChanel*	Объединенный порт Fast Ethernet
FEXT	*Far End Cross Talk*	Переходная помеха на дальнем конце
FIFO	*First Input First Output*	Правило обслуживание очереди
FR	*Frame Relay*	Сеть с ретрансляцией кадров
FTP	*File Transfer Protocol*	Протокол передачи файлов
FTTB	*Fiber To The Building*	Оптоволокно до здания

FTTC	*Fiber To The Curb*	Оптоволокно до распределительного шкафа
FTTH	*Fiber To The Home*	Оптоволокно в дом
FTTN	*Fiber To The Node*	Оптоволокно до сетевого узла
FTTx	*Fiber To The x*	Оптоволокно до точки *x*
GARP	*Generic Attribute Registration Protocol*	Протокол регистрации общих атрибутов
GBIC	*Gigabit Interface Converter*	Гигабитовый преобразователь интерфейса
GEC	*Gigabit EtherChannel*	Гигабитовый объединенный канал
GEPON	*Gigabit Ethernet Passive Optical Network*	Гигабитовая пассивная оптическая Ethernet-сеть
GVRP	*GARP VLAN Registration Protocol*	Протокол регистрации общих параметров виртуальных сетей
HDLC	*High-Level Data Link Control*	Высокоуровневый протокол управления линией данных
HDTV	*High Definition Television*	Телевидение высокой четкости
HP	*Hewlett-Packard*	Название фирмы
HTTP	*HyperText Transfer Protocol*	Протокол передачи гипертекста
ICMP	*Internet Control Message Protocol*	Протокол межсетевых управляющих сообщений
IDS	*Intrusion Detection System*	Система обнаружения вторжений
IEEE	*Institute of Electrical and Electronics Engineers*	Институт инженеров электротехники и электроники
IEC	*International Electrotechnical Commission*	Международная электротехническая комиссия
IGRP	*Interior Gateway Routing Protocol*	Внутренний протокол маршрутизации шлюза
IMAP	*Internet Message Access Protocol*	Протокол для доступа к электронной почте
IOS	*Internetwork Operating System*	Сетевая операционная система
IP	*Internet Protocol*	Протокол межсетевых сообщений
IPX	*Internetwork Packet eXchange*	Протокол межсетевого обмена пакетами
ISL	*Inter Switch Link*	Межкоммутаторный канал
ISDN	*Integrated Services Digital Network*	Цифровая сеть с интеграцией услуг
ISO	*International Organization for Standardization*	Международная организация по стандартизации

ITU-T	*International Telecommunication Union - Telecommunication Standardization Sector*	Международный союз электросвязи
LACP	*Link Aggregation Control Protocol*	Протокол управления агрегированным каналом
LAN	*Local Area Network*	Локальная сеть
LAP-B	*Link Access Procedure Balanced*	Балансная процедура доступа к линии
LAPF	*Link Access Procedure Frame Mode*	Протокол доступа к каналу при работе в пакетном режиме
LCP	*Link Control Protocol*	Протокол управлением линией связи (соединением)
LMI	*Local Management Interface*	Интерфейс локального управления
MAC	*Medium Access Control*	Управление доступом к среде
MBGP		Протокол маршрутизации
MPLS	*MultiProtocol Label Switching*	Мультипротокольная коммутация на основе меток
MVRP	*Multiple VLAN Registration Protocol*	Протокол множественных регистраций виртуальных сетей
NAT	*Network Address Translation*	Способ трансляции сетевых адресов
NCP	*Network Control Protocol*	Протокол управления сетью
NEXT	*Near End Cross Talk*	Переходная помеха на ближнем конце
NFS	*Network File System*	Сетевая файловая система
NLSP	*NetWare Link Services Protocol*	Протокол коммуникационных услуг в среде NetWare
NNTP	*Network News Transfer Protocol*	Протокол чтения сетевых новостей
NPE	*Network Processing Engine*	Сетевой операционный модуль
NSAP	*Network Service Access Point*	Точка доступа к сетевой службе
NVRAM	*Non Volatile RAM*	Энергонезависимая память
OLT	*Optical Line Terminal*	Оптический линейный терминал
ONU	*Optical Network Unit*	Оптический сетевой блок
OSPF	*Open Shortest Path First*	Протокол поиска наикратчайшего пути
P2MP	*Point-to-Multipoint*	Точка-много точек
P2P	*Peer-to-Peer Protocol*	Протокол точка-точка
PACL	*Port-based ACLs*	Списки доступа на основе портов

PAgP	*Port Aggregation Protocol*	Протокол агрегирования портов
PAP	*Password Authentication Protocol*	Протокол аутентификации
PAT	*Port Address Translation*	Трансляция адресов на основе порта
PCI SSC	*Payment Card Industry Security Standards Council*	Стандарт безопасности для карточных платежей
PDH	*Plesiochronous Digital Hierarchy*	Сеть плезиохронной цифровой иерархии
PE	*Provider Edge*	Провайдерский граничный коммутатор
PLP	*Packet-Layer Protocol*	Протокол пакетного уровня
PMD	*Polarization Mode Dispersion*	Поляризационная модовая дисперсия
PoE	*Power over Ethernet*	Питание по линии *Ethernet*
PON	*Passive Optical Network*	Пассивная оптическая сеть
POP	*Point of presence*	Точка присутствия
POP3	*Post Office Protocol 3*	Протокол 3 получения почты с сервера
POST	*Power On Self Test*	Процедура тестирования после включения
PPP	*Point to Point Protocol*	Протокол канального уровня точка-точка
PRI	*Primary Rate Interface*	Интерфейс первичного цифрового канала
PVC	*Permanent Virtual Circuit*	Постоянный виртуальный канал
PVC	*Polyvinyl chloride*	Поливинилхлоридная оболочка
PVID	*Port Identifier VLAN*	Идентификатор порта виртуальной сети
QoS	*Quality of Service*	Качество услуг
RADIUS	*Remote Authentication in Dial-In User Service*	Протокол для реализации аутентификации, авторизации
RAM	*Random-Access Memory*	Оперативное запоминающее устройство
RARP	*Reverse Address Resolution Protocol*	Обратный протокол разрешения адресов
RIP	*Routing Information Protocol*	Дистанционно-векторный протокол маршрутизации
RSTP	*Rapid Spanning Tree Protocol*	Быстрый протокол покрывающего дерева
RU	*Rack Unit*	Единица стандартной высоты

		компонента сети
SAP	*Service Advertising Protocol*	Протокол объявления служб
SDH	*Synchronous Digital Hierarchy*	Синхронная цифровая иерархия
SFP	*Small Form factor Pluggable module*	Малогабаритный конвертер интерфейса
SLIP	*Serial Line Internet Protocol*	Канальный последовательный протокол
SNMP	*Simple Network Management Protocol*	Простой протокол управления сетью
SOHO	*Small Office/Home Office*	Сеть малого или домашнего офиса
SPID	*Service Profile IDentifier*	Идентификатор профиля службы
SRAM	*Static Random-Access Memory*	Статическое ОЗУ
SRM	*Switch Resource Management*	Управление ресурсами коммутатора
SSH	*Secure Shell*	Безопасная оболочка
STA	*Spanning Tree Algotithm*	Алгоритм покрывающего дерева
STP	*Spanning Tree Protocol*	Протокол покрывающего дерева
SVC	*Switched Virtual Circuit*	Коммутируемый виртуальный канал
TCI	*Tag Control Information*	Тэг управляющей информации
TCP	*Transport Control Protocol*	Транспортный протокол управления передачей
TDM	*Time Division Multiplexing*	Временное разделение каналов
TFTP	*Trivial FTP*	Упрощенный протокол передачи файлов
TIA	*Telecommunications Industry Association*	Ассоциация телекоммуникационной индустрии;
TPID	*Tag Protocol Identifier*	Тэг протокольного идентификатора
UBR	*Unspecified Bit Rate*	Трафик с неопределенной скоростью
UDP	*User Datagram Protocol*	Протокол пользовательских дейтаграмм
UNI	*User Network Interface*	Сетевой интерфейс пользователя
UTP	*Unshielded Twisted Pair*	Неэкранированная витая пара
VBR	*Variable Bit Rate*	Трафик с переменной скоростью
VC	*Virtual Channal*	Виртуальный канал

VCI	*Virtual Channal Identifier*	Идентификатор виртуального канала
VID	*VLAN Identifier*	Идентификатор виртуальной локальной сети
VIP	*Versatile Interface Processor*	Многоцелевой интерфейсный процессор
VLAN	*Virtual LAN*	Виртуальная локальная сеть
VoIP	*Voice over IP*	IP-телефония
VP	*Virtual Path*	Виртуальный путь
VPI	*Virtual Path Identifier*	Идентификатор виртуального пути
VPN	*Virtual Private Network*	Виртуальная частная сеть
VTP	*VLAN Trunking Protocol*	Протокол магистральных каналов виртуальных локальных сетей
WAN	*Wide Area Networks*	Глобальная сеть
WWW	*World Wide Web*	Всемирная гипермедиа информационная служба

ВВЕДЕНИЕ

Компьютерные сети играют одну из важнейших ролей в деятельности современных предприятий и организаций. С помощью компьютерных сетей предприятия и организации информируют о своей хозяйственной деятельности, получают заказы и проводят финансовые операции, филиалы осуществляют связь с центральным офисом, сотрудники обмениваются информацией друг с другом, получают доступ к ресурсам внутренних и внешних серверов и т.д. и т.п.

Замедление работы сети существенно сказывается на темпе работы предприятия (организации), а выход из строя магистрального коммуникационного оборудования или сервера предприятия может привести к полной остановке деятельности отдельного подразделения или всей организации или предприятия.

Надежность функционирования компьютерной сети и ее производительность закладывается на этапе ее проектирования, а поддержание высокой производительности на протяжении всего жизненного цикла сети обеспечивается грамотной эксплуатацией и администрированием компьютерной сети. Поэтому в процессе обучения студентов по направлениям «Информационные системы и технологии», «Информационные технологии и компьютерные системы» и «Информатика и управление в технических системах» вопросам проектирования сетей уделяется значительное внимание, как во время теоретической подготовки, так и в рамках курсового проектирования.

Целью курсового проектирования является углубление теоретических знаний в области архитектуры компьютерных сетей и приобретение практических навыков проектирования и моделирования локальных сетей предприятий различного масштаба. Поэтому перед приступлением к процессу проектирования студент должен глубоко изучить основные теоретические положения построения компьютерных сетей, изложенные в [17,22,24,26,27,33] и базовые принципы проектирования локальных и глобальных сетей, которые достаточно подробно освещены в специализированной литературе [1,2,3, 5,10-13,17,20,21,28,31,34,35,39].

В результате проектирования компьютерной сети студент вначале должен определить количество и месторасположения активного и пассивного сетевого оборудования, разработать логическую структуру локальной компьютерной сети, произвести, по необходимости, ее сегментацию, выполнить расчет кабельной системы, произвести обоснованный выбор коммуникационного оборудования, разработать мероприятия по защите сети, составить сценарии конфигурации оборудования. На следующем этапе необходимо проверить работоспособность спроектированной сети путем моделирования ее функционирования на компьютере. Процедура моделирования включает создание топологии сети в редакторе моделирующей

программы (например, Packet Tracer), конфигурацию оборудования с учетом технического задания и проверку функционирования сети.

После коррекции по результатам моделирования топологии и программы конфигурации необходимо начертить электрическую схему соединений компонентов сети или составить таблицу соединений оборудования.

В курсовом проекте предусмотрено ряд групп вариантов компьютерных сетей различной сложности.

Первая группа — минимальная сложность. Организация, для которой необходимо спроектировать сеть, размещается на одном этаже. Количество рабочих мест не более 100. Все пользователи располагаются в помещениях по функциональному признаку: бухгалтерия; кадровая служба; служба главного механика; служба информационной поддержки; отдел снабжения; управления и т.п. Информационное взаимодействие между службами минимальное. Выход в сеть Интернет разрешен только руководству организации, руководителю кадровой службы и работникам отдела снабжения.

Вторая группа — средняя сложность. Количество этажей здания, занимаемой службами организация не более 6. Количество рабочих мест не более 300. Работники, относящиеся к одной и той же службе, размещаются в различных помещениях и на различных этажах. Информационное взаимодействие между службами минимальное. Выход в сеть Интернет разрешен только руководству организации, руководителю кадровой службы, работникам отдела снабжения и одному сотруднику каждой из служб.

Третья группа — повышенная сложность. Предприятие имеет ряд филиалов, расположенных в различных городах. Количество этажей здания, занимаемой службами организация не более 16. Количество рабочих мест не более 1000. Работники, относящиеся к одной и той же службе, размещаются в различных помещениях и на различных этажах. Информационное взаимодействие между филиалами осуществляется по каналам глобальных сетей (FTTx, FR, ATM). Выход в сеть Интернет разрешен только руководству организации, руководителю кадровой службы, работникам отдела снабжения и сотрудникам каждой из служб по особому списку.

При проектировании ЛКС предприятия топология сети определяется преимущественно схемой его территориального размещения и организационной структурой предприятия, количеством структурных подразделений и компьютеров в них, а также местом возможного размещения центрального и промежуточного распределительных пунктов (наличием, количеством и месторасположением соответствующих помещений). В связи с этим проектировщик ограничен возможностью изменения пространственного расположения распределительных пунктов и рабочих станций, а, следовательно, и возможностью варьирования длин кабельных линий.

В процессе проектирования локальной вычислительной сети разработчику необходимо решить следующие задачи:

1. Выяснить, на какое количество пользователей должна быть рассчитана сеть и для каких прикладных задач она предназначена.
2. Определить топологию сети и метод доступа для пользователей.
3. Выбрать подходящее активное и пассивное аппаратное обеспечение: типы коммутаторов, маршрутизаторов, распределительных шкафов, типы и количество кабеля и т.д.
4. Разработать схему электрических соединений компонентов компьютерной сети и рассчитать длины кабелей, входящих в ее состав.
5. Составить сценарии конфигурирования коммуникационного оборудования, при котором обеспечивается надежное и безопасное функционирование сети в соответствии с поставленными требованиями.
6. Выполнить моделирование спроектированной сети в одном из пакетов моделирования (Packet Tracer, Boson, NS-2 или др.) и проверить правильность ее конфигурации.

От правильного решения этих и многих других задач зависит работоспособность сети, скорость и помехоустойчивость передачи данных, затраты на создание и эксплуатацию сети.

Проектирование сети должно осуществляться на основе государственных и отраслевых нормативов и стандартов [40-44]. В случае отсутствия некоторых национальных стандартов, следует использовать международные рекомендации и стандарты в данной области.

В данном учебном пособии приводятся примеры проектирования локальных сетей на основе телекоммуникационных устройств преимущественно корпораций Cisco с конфигурацией с командной строки. Особенностью устройств корпорации Cisco является использование большого количества проприетарных (собственной разработки) телекоммуникационных протоколов. Поэтому в пособии также рассмотрены примеры создания компьютерных сетей на базе коммутаторов D-Link и Huawei, в которых используются преимущественно стандартные телекоммуникационные протоколы. Следует отметить, что способ конфигурации сетевых устройств с использованием интерфейса командной строки CLI (*Command Line Interface)* является более сложным, по сравнению с конфигурацией посредством графического интерфейса, однако, он требует от студента более глубоких знаний процессов, протекающих в компьютерных сетях, что способствует формированию специалиста более высокого класса.

Руководителем курсового проектирования может быть задана другая аппаратная платформа реализации проектируемой сети, либо выбор аппаратной реализации может быть предоставлен самому студенту.

Автор глубоко признательны рецензентам, профессору кафедры информационных технологий и компьютерных систем СевГУ, д-ру техн. наук Апраксину Ю.К. и заведующему кафедрой передачи дискретных сообщений и метрологии Сибирскго государственного университета телекоммуникаций и информатики проф., д-р техн. наук Шувалову В.П., за доброжелательную критику и полезные замечания, которые способствовали улучшению книги.

Часть 1. Общие принципы проектирования компьютерных сетей уровня предприятия

1. Локальные компьютерные сети предприятий и взаимодействие их с глобальными сетями

1.1. Обобщенная структура компьютерной сети предприятия

Структура сети предприятия (организации) зависит от числа его сотрудников, использующих сетевые компьютеры, схемы размещения и размера занимаемой площади, количества структурных подразделений, наличия филиалов, их количества и удаленности от головного предприятия (центрального офиса), а также ряда других факторов. В общем случае физическую структуру объединенной (корпоративной) компьютерной сети крупного предприятия, расположенного в одном или нескольких многоэтажных зданиях с рядом филиалов в других местах населенного пункта или регионах, можно представить в виде структурной схемы, изображенной на рисунке 1.1.

В состав сети, как центрального офиса, так и филиалов предприятия входят компьютерные сети (КС) рабочих групп, расположенные на разных этажах здания и объединенные посредством этажного (промежуточного) узла коммутации $УК_{пр}$ в сеть структурного подразделения (отдела, цеха, службы). В свою очередь сети подразделений посредством главного (центрального) узла коммутации $УК_{гл}$ объединяются в сеть головного предприятия. Аналогичную или несколько упрощенную структуру имеют и дочерние предприятия или филиалы.

Сеть головного предприятия (и его филиалов) обычно территориально располагается в одном или нескольких зданиях, расположенных на сравнительно небольшом расстоянии друг от друга (≈ 2 км). В качестве среды для передачи сигналов данных используются преимущественно проводные либо волоконно-оптические линии связи (ВОЛС), принадлежащие самой организации. В ряде случаев применяются и беспроводные линии. Сети предприятий по общепринятой классификации являются локальными. В них используются преимущественно технологии Ethernet, реже Token Ring или FDDI.

Пользователи сети совместно (по очереди) используют среду передачи. Доступ к среде осуществляется либо случайным образом (сети Ethernet) по способу CSMA/CD (множественный доступ с передачей несущей и обнаружением коллизий), либо регулируется путем передачи кадров со свободным или занятым маркером (сети Token Ring и FDDI).

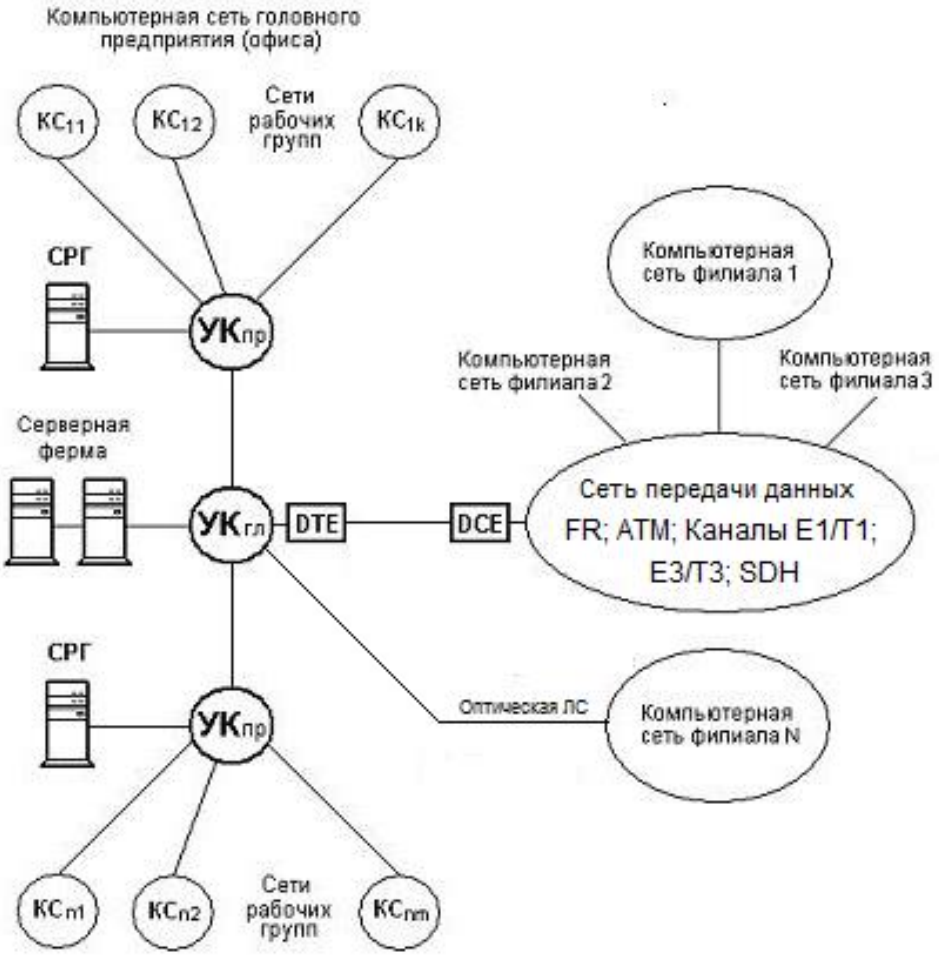


Рисунок 1.1 Обобщенная структурная схема объединенной сети крупного предприятия

Выход в Интернет и связь с доченими предприятиями (филиалами) происходит посредством глобальной (распределенной) сети передачи информации общего пользования с коммутацией каналов или коммутацией пакетов. К таким сетям относятся.

1. Сеть плезиохронной цифровой иерархии PDH (Рекомендация ITU-T G.703), в состав которой входят основной цифровой канал со скоростью передачи сигналов 56 и 64 кбит/с; цифровые каналы типа T1 или E1 со скоростями передачи 1544 и 2048 кбит/с соответственно; цифровые каналы типа T3 или E3 со скоростями передачи 44,736 и 34,368 Мбит/с соответственно, а также цифровые каналы более высокого уровня иерархии.

2. Сеть каналов синхронной цифровой иерархии (SDH), основным каналом которой является цифровой канал со скоростью передачи 155,52 Мбит/с, а также каналы более высоких уровней иерархии со скоростями передачи 622 Мбит/с, 2,5 и 10 Гбит/с.

3. Цифровая сеть с коммутацией пакетов Frame Relay (FR), позволяющая транслировать кадры со скоростью передачи сигналов 1544 и 2048 кбит/с.

4. Асинхронная сеть передачи сообщений с коммутацией пакетов (ATM), позволяющая передавать данные со скоростями 155, 622 и 2500 Мбит/с.

Кроме этого головное предприятие или его филиалы могут соединяться с другими филиалами посредством выделенных физических линий — проводных или оптических.

Взаимодействие оборудования сети предприятия с распределенной глобальной сетью происходит между оконечным оборудованием данных **DTE** (*Data Terminal Equipment*) и оборудование канала данных **DCE** (*Data Circuit Terminating Equipment*). Обычно DTE представляет собой персональный компьютер, рабочую станцию или шлюз (маршрутизатор), а DCE является аппаратурой канала данных, осуществляющей преобразование форматов данных сети пользователя (предприятия) в форму, используемую в каналах связи глобальной сети. В цифровых сетях Frame Relay и ATM функции DCE выполняются интерфейсными модулями коммутаторов этих сетей. Интерфейсы DTE/DCE являются стыком, на котором ответственность за передачу потока данных переходит от абонента глобальной сети к провайдеру. Обмен данными в интерфейсе DTE/DCE преимущественно выполняется на канальном уровне по протоколу синхронной последовательной передачи V.35.

Наиболее часто в качестве интерфейсов глобальных сетей используются последовательные порты. Практически все эти порты могут выступать как в качестве DTE- так и в качестве DCE-порта. Отличительной особенностью этих интерфейсов является то, что DCE-интерфейс обеспечивает сигналы синхронизации, которые необходимы для синхронной передачи по шине. В документации к коммуникационному устройству обычно указывается, к какому типу относится порт — DTE или DCE.

Связь компьютера или маршрутизатора с цифровой выделенной линией осуществляется с помощью пары устройств, обычно выполненных в одном корпусе или же совмещенных с маршрутизатором. К таким устройствами относятся: *устройство обслуживания данных* (УОД) и *устройство обслуживания канала* (УОК). В англоязычной литературе эти устройства называются соответственно **DSU (***Data Service Unit*) и **CSU** (*Channel Service Unit*). DSU преобразует униполярные сигналы, поступающие от DTE в биполярные (обычно по интерфейсу RS-232C, RS-449 или V.35). Кроме этого DSU выполняет всю синхронизацию, формирует кадры каналов T1/E1 и осуществляет выравнивание загрузки канала. Устройство CSU реализует более узкие функции, преимущественно созданием оптимальных условий передачи в линии связи. Эти устройства, как и модуляторы-демодуляторы, часто обо-

значаются одним словом DSU/CSU (рисунок 1.2) [17,18]. Роль такого устройства при сопряжении маршрутизатора с выделенной линией выполняет xDSL- или оптический модем.

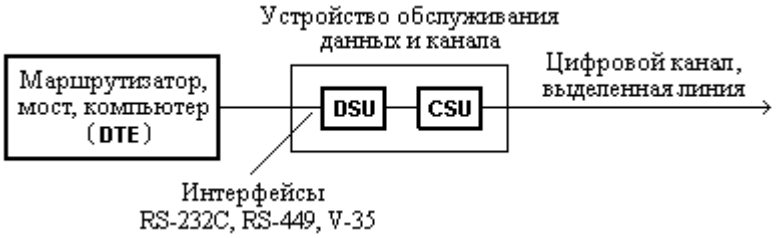


Рисунок 1.2 — Использование DSU/CSU для подключения к цифровой выделенной линии

Нередко под устройством DSU/CSU понимают более сложные устройства, которые кроме согласования интерфейсов выполняют функции мультиплексора потоков T1/E1. В состав такого устройства может входить модуль мультиплексирования низкоскоростных потоков речевых и компьютерных данных в канал 64 Кбит/с или в несколько таких каналов (речевые данные при этом обычно компрессируется до скорости 8-16 Кбит/с).

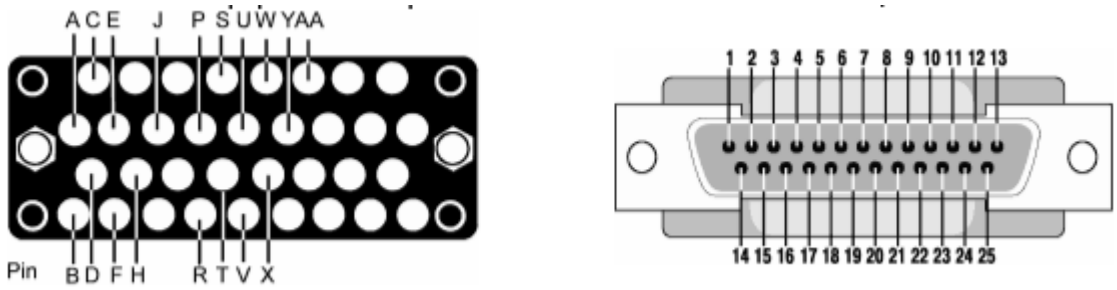
Для осуществления транспортирования кадров локальной сети по каналам глобальной сети выполняется процедура включения (*инкапсуляции*) блоков данных в кадры, характерные для глобальной сети. В процессе инкапсуляции ко входному кадру, имеющему собственный заголовок, добавляется заголовок, а в некоторых сетях и хвостовик кадра в соответствии с используемым в конкретной глобальной сети форматом. Содержащаяся в них дополнительная служебная информация позволяет беспрепятственно транспортировать данные между любыми точками (портами) глобальной сети. На оконечном узле глобальной сети служебные поля изымаются и получателю выдаются кадры, идентичные поступившим в глобальную сеть. То есть, глобальная сеть является "прозрачной" для кадров локальной сети.

Для согласования интерфейса оконечного оборудования с каналом внешней сети производится настройка параметров (*конфигурация*) подключаемого порта. Сначала задается тип канала, а затем порт конфигурируется на применение необходимого протокола инкапсуляции. В современном коммуникационном оборудовании эта процедура выполняется путем задания инструкций в командной строке или выбора соответствующего пункта меню. В процессе проектирования сети студент должен обосновано выбрать параметры конфигурации, определить их численные значения и разработать скрипты конфигурации активного оборудования.

В устройствах DTE и DCE, работающих с высокими скоростями, обычно используется интерфейс V.35. Сначала этот интерфейс предназначался для передачи данных между DTE и DCE со скоростями от 48 до 100

кбит/с. Затем скорость обмена была повышена до 45 Мбит/с (поток Т3). С увеличением скорости передачи длина соединительного кабеля между DTE и DCE уменьшается.

Стандартом МККТТ V.35, регламентирующим параметры этого интерфейса, допускается два типа устройств — сбалансированные (передача по двум витым парам с волновым сопротивлением 120 Ом) и несбалансированные (передача по двум коаксиальным кабелям с волновым сопротивлением 75 Ом). В общем случае интерфейс V.35 использует прямоугольные 4-рядные разъемы типа М34. Из наличных 34 контактов задействованы лишь 20. Поэтому вместо разъемов М34 допускается также применение 25-контактных разъемов типа DB-25. Внешний вид разъемов М34 и DB-25 интерфейса V.35 показан на рисунке 1.3,а и б соответственно [8].



а) б)

Рисунок 1.3 – Внешний вид разъемов М34 (а) и DB-25 (б) интерфейса V.35

Контакты разъема М34 имеют буквенное, а разъема DB-25 — цифровое обозначение сигналов, поступающим по соответствующим цепям. В таблица П.1.1 приведено описание цепей и соответствие контактов для двух типов интерфейсных разъемов.

Интерфейс RS-449 позволяет осуществлять обмен данными между DTE и DCE на более высоких скоростях. Передача данных осуществляется дифференциальными сигналами по симметричным цепям. Для соединения устройств используется 37-контактный разъем.

1.2. Структурные уровни локальных сетей

При проектировании компьютерных сетей для достижения наилучших результатов по производительности, надежности, управляемости и масштабируемости используется модульный и иерархический подход. Такой прием позволяет в будущем наращивать сеть путем добавления новых блоков, не затрагивая остальные компоненты сетевой инфраструктуры. Для упрощения процессов разработки и обслуживания крупных корпоративных компьютер-

ных сетей компания Cisco предложила разбивать их на три иерархических уровня [9, 18, 20], на каждом из которых выполняются специфические сетевые функций (рисунок 1.4). Каждый уровень задает правила и порядок выполнения определенных функций. Однако эти уровни являются логическими и не обязательно согласованы с физическими устройствами, т.е. три уровня не обязательно предполагают три различных устройства.

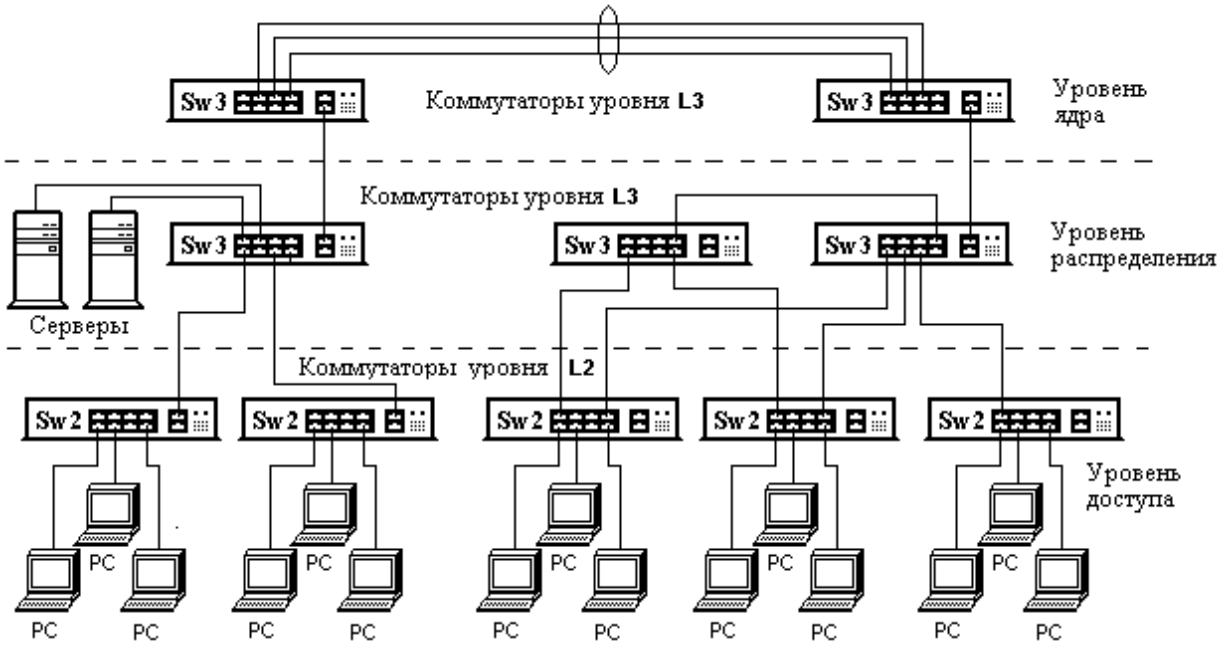


Рисунок 1.4 — Иерархическая структура локальных сетей

Нижняя ступень иерархии получила название **«уровень доступа»** (*Access layer*). Коммутаторы уровня доступа функционируют на втором (канальном) уровне эталонной модели OSI и предоставляют пользователям порты 10/100 Ethernet, образуют изолированные подсети рабочих групп пользователей. На этом уровне реализовано управление пользовательскими рабочими станциями и рабочими группами при обращении к ресурсам объединенной сети. Каждый коммутатор уровня доступа соединяется, как правило, каналами Gigabit Ethernet с одним или двумя коммутаторами уровня распределения. Подключение к двум коммутаторам рапределения служит для повышения надежности сети.

Следующей ступенью иерархии структуры сети является **уровень распределения** (*Distribution layer*). Уровень распределения, который иногда называют уровнем рабочих групп, служит связующим звеном между уровнями доступа и ядра. Основные функции уровня распределения состоят в маршрутизации, фильтрации и доступе к региональным сетям, а также (если необходимо) в определении правил доступа пакетов к уровню ядра (базовому уровню). Поэтому на данном уровне устанавливаются коммутаторы,

функционирующие на третьем (сетевом) или третьим и четвертом (сетевом и прикладном) уровнях. На уровне распределения осуществляется соединение рабочих групп компьютеров пользователей с уровнем распределения, перенаправление трафика к удаленным службам, контроль (из уровня распределения) за доступом и политиками доступа и др. На этом же уровне реализуется переход от одной технологии к другой (например, от 100Base-TX к 1000Base-T), объединение полос пропускания низкоскоростных каналов доступа в высокоскоростные магистральные каналы.

На самом верху иерархии располагается **магистральный уровень** или **ядро сети** — (*Core layer*). Этот уровень отвечает за быструю и надежную пересылку больших объемов трафика между узлами уровня распределения. Задача ядра сети — высокоскоростная коммутация трафика. Для повышения скорости обмена линии связи между узлами уровня ядра объединяются в магистраль. Устройства, входящие в состав ядра сети, выполняют следующие функции [17,18]:

- высокоскоростной маршрутизации/коммутации трафика;
- резервирования на уровне аппаратуры и каналов;
- разделения нагрузки по параллельным каналам;
- быстрого переключения между основным и резервным каналами;
- эффективного использования полосы пропускания соединений.

Ядро сети строится из модулей, образованных однотипными высокопроизводительными устройствами, с обеспечением аппаратного резервирования. В качестве таких устройств зачастую используются маршрутизаторы. Построение ядра сети на базе маршрутизаторов сокращает также время простоя сети, как в случае отказа аппаратного (за счет гибких схем резервирования), так и в случае программных ошибок или ошибок оператора (за счет разнообразных механизмов поиска неисправностей). Коммутаторы уровня ядра устанавливаются в аппаратной (серверной), где также, как правило, располагаются все сетевые ресурсы: серверы (файл-серверы, серверы приложений, почтовые серверы и т.п.), маршрутизатор доступа в Internet и т.п. Эти коммутаторы формируют единую высокопроизводительную информационную магистраль предприятия.

Более новая классификация корпоративных сетей [Обзор прод] предполагает и четвертый уровень, в который входит серверный блок (серверная ферма **—** *Server Farm*). На этом уровне используются высокоскоростные коммутаторы 3–7 уровней.

1.3. Выбор структуры сети для предприятий различного масштаба

Если компьютерная сеть проектируется для малого предприятия (офисная сеть), располагающимся в одном или нескольких помещениях на одном этаже здания, количество компьютеров на котором равно порядка 10 и требуется выход в Интернет, то в качестве логической структуры целесообразно взять "плоскую" структуру сети, изображенную на рисунке 1.5.

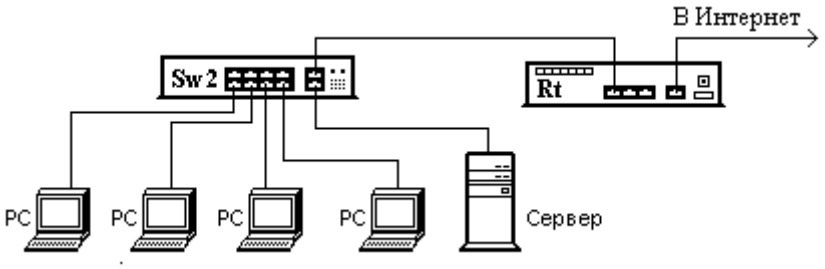


Рисунок 1.5 — Структура "плоской" сети

Такие сети получили название **SOHO** (*Small Office/Home Office*) — сети малого или домашнего офиса. Плоская структура означает, что нет необходимости использовать маршрутизатор для объединения различных физических сетей. Для объединения достаточно использовать сетевые коммутаторы (свичи). Узлом сети является коммутатор второго уровня Sw2, а соединение с сетью Интернет осуществляет маршрутизатор Rt. Рабочие станции PC подключаются к портам коммутатора, к ним же подсоединяются сервер(ы) и маршрутизатор. При выборе коммутатора следует предусмотреть наличие одного или двух свободных портов для последующего возможного расширения сети и подключения дополнительных серверов. Если в качестве Sw2 взят программируемый коммутатор, то можно компьютеры организации разделить на изолированные виртуальные сети VLAN.

Кроссовое помещение для сети малого предприятия, как правило, не выделяется, а коммуникационное оборудование устанавливается в специальном подвесном коммуникационном шкафу или просто крепится к стене. С целью обеспечения безопасности коммуникационное оборудование и сервер следует все же устанавливать в закрываемом на замок коммуникационном шкафу.

Плоскую сеть можно логически разделить на независимые подсети путем выделения каждой из подсетей своего сетевого IP-адреса. Такое решение позволяет заметно повысить пропускную способность сетевых сегментов. К каждой подсети целесообразно отнести компьютеры, относящиеся одной и той же службе: бухгалтерии, отдела маркетинга, службы снабжения и т.п. Для направления пакетов в свои подсети в качестве узла применяется маршрутизатор или коммутатор третьего уровня Sw3 (рисунок 1.6).

Как видно из рисунка в этой сети организовано три подсети. Пользо-

ватели каждой из подсетей имеют возможность обмениваться информацией с группой внутренних серверов (серверной фермой). Выход в сеть Интернет обеспечивается маршрутизатором Rt. Внутренние серверы и подсети защищены от внешнего доступа программным межсетевым защитным экраном, установленным на маршрутизаторе.

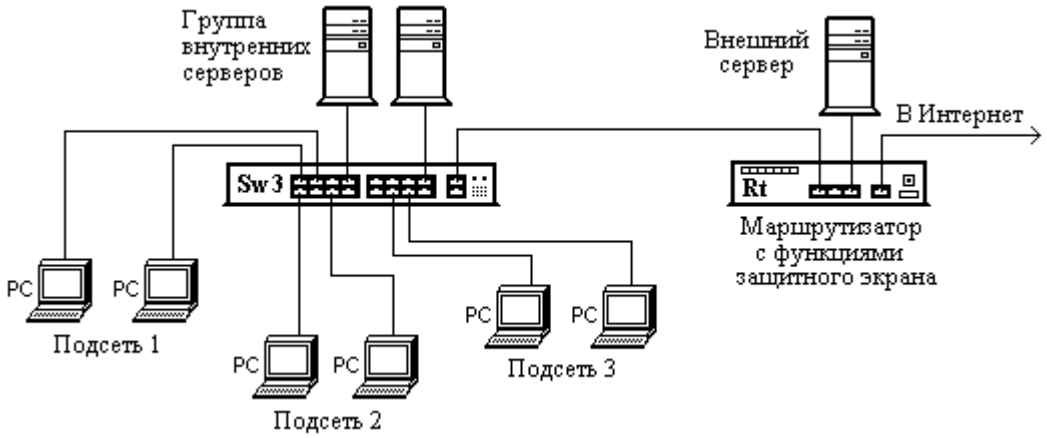


Рисунок 1.6 — Компьютерная сеть с разделением на подсети

Пользователи Интернета могут получить свободный доступ к внешнему серверу данной организации. Для организации, размещающейся в многоэтажном здании и занимающей на каждом этаже несколько комнат, рекомендуется иерархическая структура сети, изображенная на рисунке 1.7.

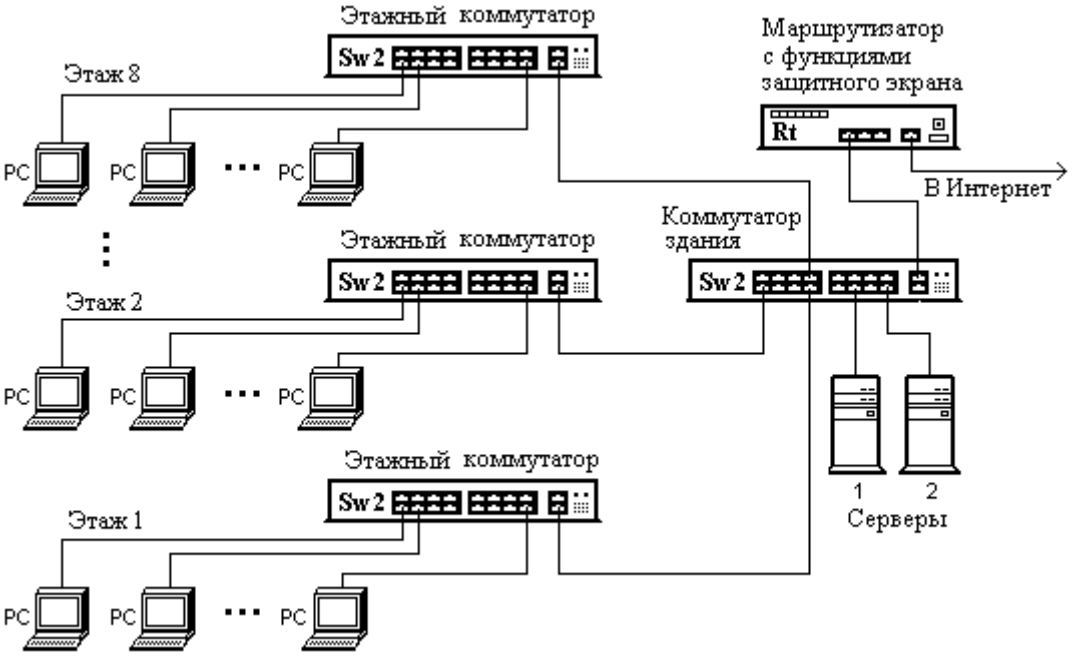


Рисунок 1.7 – Иерархическая структура сети с этажными коммутаторами

В такой сети на каждом этаже устанавливается один или несколько коммутаторов, располагаемых в специальных помещениях — распределительных пунктах этажа. При небольшом количестве компьютеров на этаже возможно использование одного распределительного пункта на 2-3 этажа. Кабель от каждой коммуникационной розетки заводится в кроссовое помещение этажа и заканчивается коммуникационной розеткой, закрепляемой на специальной раме с розетками разъема RJ-45 — патч-панеле. Подключение каждого из кабелей к коммутатору выполняется патч-кордами. Коммутатор здания, маршрутизатор и серверное оборудование устанавливаются в распределительном пункте здания.

В случае если предприятие имеет один или несколько филиалов, располагаемых в других частях населенного пункта или в других городах, а связь с ними будет осуществляться по каналам глобальных сетей (Frame Relay, ATM, кабельным и оптическим линиям связи), то структура компьютерной сети центрального офиса организации имеет вид, изображенный на рисунке 1.8.

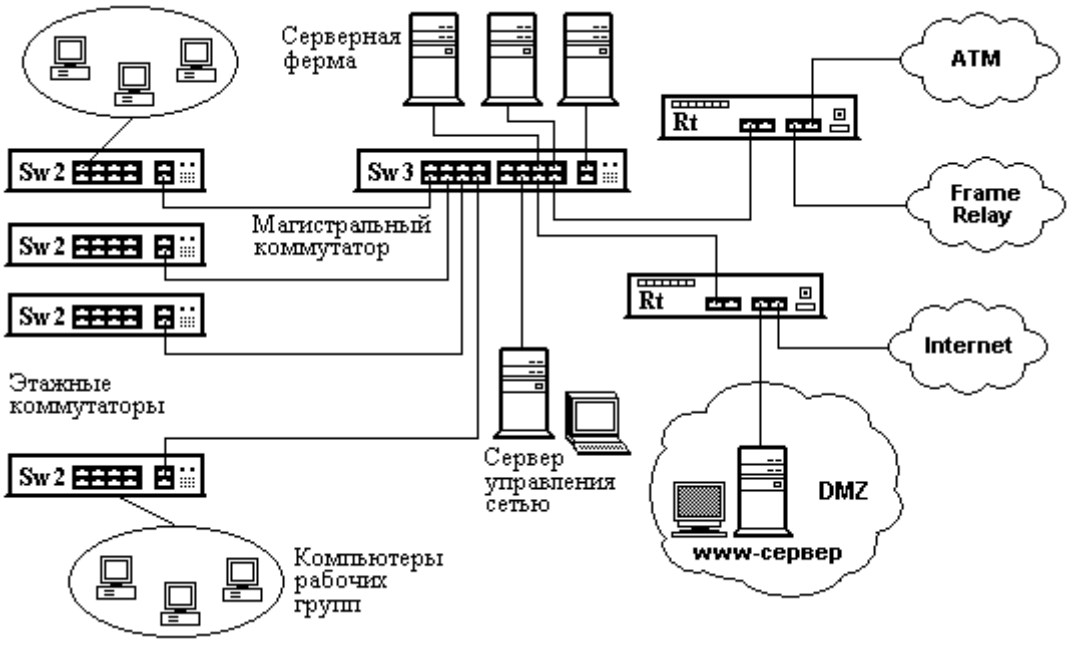


Рисунок 1.8 — Структура корпоративной компьютерной сети предприятия с филиалами в других населенных пунктах

Для защиты корпоративной сети Web-сервер организации устанавливается в "демилитаризованной зоне" DMZ, которая отделяется от сети незащищенной Интернет межсетевым защитным экраном, выполненным в виде самостоятельного устройства или устанавливаемым на маршрутизаторе. Все серверы организации объединяются в группу — "серверную ферму", располагаемую в распределительном пункте здания.

Примеры реализации сетей предприятий различного масштаба можно найти в сети Интернет, например [http://telecomsite.ru/project/nets/project142/].

1.4. Взаимодействие локальных сетей с глобальной сетью

Для объединения локальных сетей, разделенных значительными географическими расстояниями широко используются выделенные линии (линии телефонной сети общего пользования, цифровые линии на основе xDSL, оптические линии связи, первичные цифровые каналы E1, E2 и др.), а также каналы глобальных сетей типа Frame Relay, ATM. Архитектура глобальных сетей и форматы кадров достаточно подробно освещены в [17,21,28,33]. В этом подразделе будут кратко рассмотрены только особенности каналов глобальных сетей, которые необходимы для осознанного выполнения процедур конфигурации коммуникационного оборудования.

Чтобы установить сетевое соединение с удаленными станциями на них должно быть инсталлировано соответствующее сетевое программное обеспечение, включающее, например, службу передачи файлов FTP, службу эмуляции терминала Telnet и др., стеки сетевых и транспортных протоколов (IP/TCP или IPX/SPX), протоколы канального уровня (PPP или SLIP). Пакеты протоколов верхних уровней для передачи их по каналам данных инкапсулируются в кадры канального уровня, формат которых регламентируется протоколами SLIP или PPP.

Существуют два типа трактов передачи данных, используемых в компьютерных сетях: двухточечные выделенные линии и коммутируемые каналы глобальных цифровых сетей. Каждый тип соединения при передаче данных по каналам распределенной сети использует для инкапсуляции протокол 2-го (канального) уровня. Поэтому для каждого последовательного интерфейса маршрутизатора необходимо задать тип конфигурации 2-го уровня. Выбор протокола инкапсуляции зависит от используемой технологии глобальной сети и от типа коммуникационного оборудования. Ниже рассматриваются особенности реализации различных протоколов канального уровня и их конфигурирования. Следует заметить, что некоторые из этих протоколов являются морально устаревшими и в современных компьютерных сетях применяются сравнительно редко. В настоящем пособии эти протоколы, наряду с современными, включены в техническое задание на учебное проектирование для увеличения количества вариантов.

1.4.1. Протокол PPP

Выделенные линии, также называемые *арендованными линиями (leased lines),* позволяют постоянно пользоваться связью. При проектировании сети передачи данных выделенные линии обычно обеспечивают соединение ко-

нечного пользователя с провайдером, связь между локальными сетями, а также магистральное соединение между сетями или подсетями. Для транспортирования пакетов более высокого уровня по двухточечной выделенной линии (соединение типа "точка-точка") применяется в настоящее время в основном протокол инкапсуляции кадров PPP (*Point to Point Protocol*) [3,6,18]. Соединения обычно осуществляются с использованием синхронных последовательных портов маршрутизаторов; при этом используется скорость передачи до 2 Мбит/с (поток E1).

Преимуществом протокола PPP по сравнению с его предшественником SLIP является то, что он позволяет работать с несколькими протоколами сетевого уровня, включая протоколы IP, IPX и AppleTalk. Это означает, что в рамках одного PPP-соединения могут передаваться потоки данных различных сетевых протоколов (IP, Novell IPX и т. д.), а также данные протоколов канального уровня локальной сети. Протоколом PPP предусмотрено выполнение следующих функций:

- конфигурирования и проверки качества канала;
- согласования параметров канала;
- аутентификации пользователей;
- мультиплексирования сетевых протоколов;
- обнаружения ошибок;
- сжатия заголовков.

Способ реализации этих функций определяется тремя отдельными протоколами.

1. Протокол HDLC (*High-Level Data Link Control*), регламентирующий процедуру инкапсуляции датаграмм при передаче по последовательным PPP-соединениям.
2. Расширенный протокол управления линией связи LCP (*Link Control Protocol*), определяющий способ конфигурирования и тестирования физического соединения.
3. Протокол управления сетью NCP (*Network Control Protocol*), предназначенный для установления и управления различными сетевыми протоколами.

В момент установления связи через PPP соединение PPP-драйвер вначале отправляет кадры LCP для конфигурирования и (при необходимости) тестирования линии связи. На некоторых каналах может возникнуть необходимость подтверждения вызывающим устройством своей подлинности. В таком случае запускается процедура аутентификации, которая выполняется в соответствии с проколами аутентификации PAP (*Password Authentication Protocol*) или CHAP (*Challenge Handshake Authentication Protocol*). Аутентификации по обоим протоколам осуществляется путем запроса имени и пароля инициатора соединения и сравнения этой пары идентификаторов с записями, находящимися в базе данных запрашиваемой стороны, или на специ-

альном сервере безопасности RADIUS. Основным различием протоколов PAP и CHAP является то, что протоколом PAP предусмотрена передача пароля в нешифрованном виде, а протоколом CHAP – в зашифрованном. Поэтому протоколом PAP следует пользоваться только в случае, если это единственный способ аутентификации, который поддерживает удаленное устройство.

После установления связи и успешной аутентификации PPP-драйвер посылает NCP-кадры для изменения и/или настройки параметров одного или более сетевых протоколов. По завершению этой процедуры сетевые пакеты получают возможность быть переданными через установленное соединение. Оно будет оставаться настроенным и активным до тех пор, пока определенные LCP или NCP кадры не закроют соединение, или до тех пор пока не произойдет какое-нибудь внешнее событие, которое приведет к потере соединения (например, сработал таймер отсутствия активности или произошло вмешательство пользователя).

1.4.2. Протокол HDLC

HDLC представляет собой протокол канального уровня, созданный на базе использовавшегося ранее для инкапсуляции протокола управления синхронным каналом данных (*Synchronous Data Link Control*). HDLC-инкапсуляция также является используемым по умолчанию протоколом инкапсуляции для последовательных каналов между маршрутизаторами Cisco.

Реализация этого протокола в сетях Cisco является очень простой. В нем не используется механизм окна и контроль потока, допускаются только соединения типа "точка-точка". В адресном поле все биты всегда равны единице. Кроме того, после управляющего поля вставлен 2-байтовый код производителя; это означает, что тип HDLC-кадров, используемых в Cisco сетях, несовместим с оборудованием других производителей. Однако, если на обоих концах выделенной линии расположены маршрутизаторы или серверы доступа, работающие с программным обеспечением операционной системы Cisco (*Cisco Internetwork Operating System software*, IOS), то для инкапсуляции обычно применяется протокол HDLC. Поскольку методы инкапсуляции протокола HDLC не являются стандартными, для устройств, которые не используют программное обеспечение Cisco, необходимо использовать протокол PPP. Несмотря на соответствие стандарту ISO, различные программные реализации протоколов HDLC, приобретенные у разных производителей, могут оказаться несовместимыми друг с другом, поскольку каждый производитель может выбрать свой способ реализации этого протокола.

1.4.4. Протокол и интерфейс сети Frame Relay

Одной из распространенных технологий глобальных сетей является сеть с ретрансляцией кадров **Frame Relay** (FR). Сеть FR состоит из ряда FR-коммутаторов (SW-FR), соединенных цифровыми каналами связи (рисунок 1.9). Локальные сети предприятия подключаются к FR-коммутаторам через маршрутизаторы, интерфейсы которых должны инкапсулировать передаваемые пакеты в кадры сети Frame Relay. Очевидно, что параметры интерфейсов маршрутизатора должны быть согласованы с параметрами сети FR.

В сетях FR предусмотрено использование электрических и оптических линий связи и высококачественного цифрового оборудования. За счет применения упрощенного механизма формирования кадров без коррекции ошибок, Frame Relay может отправлять информацию канального уровня намного быстрее, чем это происходит в других типах сетей. Frame Relay является стандартным протоколом канального (второго) уровня с установлением виртуальных соединений, позволяющим работать сразу с несколькими виртуальными каналами, в которых используется инкапсуляция по методу HDLC. Frame Relay является более эффективным протоколом, чем протокол X.25, для замены которого он и был разработан [25,27]. Он может использоваться как в частных сетях, так и в сетях, предоставляемых провайдерами.

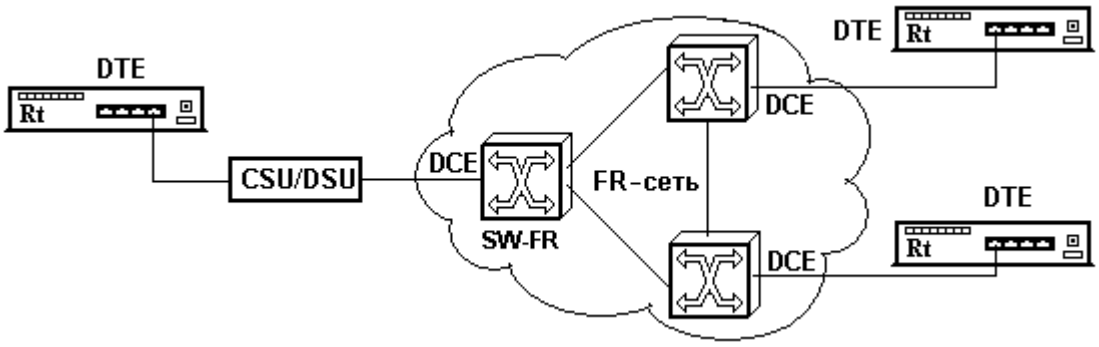


Рисунок 1.9 — Связь маршрутизаторов ЛВС с сетью Frame Relay

Frame Relay обеспечивает передачу данных со скоростями 56 Кбит/с, 64 Кбит/с или 1,544 и 2,048 Мбит/с. На рисунке 1.3 показан пример связи маршрутизаторов локальных сетей с сетью ретрансляции кадров Frame Relay через устройство передачи данных (CSU/DSU) и посредством цифровой выделенной линии.

В сетях Frame Relay обычно DTE представляет собой маршрутизатор, а DCE является коммутатором FR. Маршрутизаторы отправителя и получателя соединяются с коммутаторами Frame Relay выделенными линиями, называемыми линиями доступа (*Access Link*). Для передачи данных между

оконечными устройствами сеть Frame Relay образует виртуальный канал (*Virtual Circuit*), через который осуществляется ретрансляция кадров.

Существуют два типа виртуальных каналов: коммутируемые виртуальные каналы SVC (*Switched Virtual Circuit*) и постоянные виртуальные каналы PVC (*Permanent Virtual Circuit*). Каналы SVC используются в звеньях данных, в которых требуется спорадическая передача сообщений между оконечными устройствами DTE по сети FR. В связи с тем, что каналы являются временными SVC, то перед передачей данных требуются применение процедур установления и завершения соединения.

Постоянные виртуальные каналы PVC предоставляются пользователям, которым требуется осуществлять регулярный и продолжительный обмен данными между оконечными устройствами по сети FR. При создании PVC в качестве идентификатора конкретного канального соединения применяется идентификационный номер **DLCI** (*Data-Link Connection Identifier*). Номер DLCI является локальным идентификатором между DTE и DCE, описывающим логическую связь между устройствами отправителя и получателя. Номера DLCI задаются провайдерами службы *Frame Ralay* и могут принимать значения от 0 до 1023. Соответствие номеров DLCI для каждой пары взаимодействующих через сеть FR маршрутизаторов обеспечивают коммутаторы сети FR.

С целью обеспечение совместимости версий протоколов Frame Relay от различных поставщиков консорциумом Cisco совместно с рядом других компаний было разработано расширение, позволяющее устройствам межсетевого взаимодействия оптимально обмениваться данными в сети Frame Relay. Это расширение, получившее название «интерфейс локального управления LMI (*Local Management Interface*)», позволяет DTE-устройствам сети *Frame Relay* (например, маршрутизаторам) общаться с DCE-устройствами и производить обмен служебной информацией, которая используется для передачи межсетевого трафика по глобальной сети Frame Relay. Сообщения интерфейса LMI предоставляют информацию о текущих значениях DLCI, их характере (локальные они или глобальные) и о статусе виртуальных каналов. Существует три варианта протокола LMI, разработанные соответственно корпорацией Cisco, американским институтом стандартизации ANSI и международным телекоммуникационным союзом ITU – стандарт Q933-A. Они отличаются форматами заголовков и номерами служебных идентификаторов. Поэтому, чтобы выполнить конфигурацию последовательного интерфейса маршрутизатора для работы с протоколом Frame Relay необходимо задать интерфейсу тип инкапсуляции, присвоить интерфейсу идентификатор DLCI и, при необходимости, задать интерфейсу тип LMI (cisco, ansi или q933a). Примеры конфигурации интерфейсов маршрутизатора приведены в подразделе 6.3.

Несмотря на то, что технология Frame Relay является одной из наиболее распространенных в современных сетях, популярность ее постепенно уменьшается в связи с появлением конкурирующих технологий, в частности технология ATM и виртуальных частных сетей VPN (*Virtual Private Network*) на основе каналов глобальной сети Интернет и на основе мультипротокольной коммутации меток MPLS (*Multiprotocol Label Switching*).

1.4.6. Протокол и интерфейс сети ATM

Одной из новых технологий объединения локальных сетей является высокопроизводительная технология коммутации и мультиплексирования **с** асинхронным способом передачи данных **ATM** (*Asynchronous Transfer Mode)*. Она основана на передаче данных в виде кадров (ячеек) фиксированного размера длиной 53 байта, из которых 5 байтов используется под заголовок. Сеть ATM состоит из коммутаторов ATM (DCE) и оконечных устройств ATM (DTE). Коммутаторы сети SW соединяются между собой через узловые интерфейсы **NNI** (*Network Node Interface*). Узловые интерфейсы оснащены преимущественно интерфейсами STM-1 (скорость передачи 155 Мбит/с) или **STM-4** (622 Мбит/с). Также имеется возможность использовать интерфейсы **STM-16** со скоростью передачи 2,5 Гбит/с.

Локальные сети LAN подключаются через пограничный маршрутизатор к узлу ATM через пользовательские интерфейсы **UNI** (*User Network Interface*). У маршрутизаторов имеется широкий выбор канальных интерфейсов на основе Ethernet или PDH- и SDH-технологий с электрическими и оптическими сигналами в диапазоне скоростей от 2 до 155 Мбит/с (рисунок 1.10).

Конфигурация соответствующего интерфейса сводится всего лишь к указанию вида инкапсуляции и идентификаторов виртуального канала VCI и виртуального пути VPI. Как и в сети Frame Relay, в ATM используются виртуальные каналы для создания и адресации соединений с другими устройствами ATM. В ней виртуальные каналы также подразделяются на постоянные виртуальные каналы (PVC) и коммутируемые виртуальные каналы (SVC). Оконечные устройства передают данные коммутаторам ATM, которые разбивают данные на ячейки и передают эти ячейки по сети. Передача ячеек в сети с асинхронным способом передачи ATM осуществляется по виртуальным каналам VC (*Virtual Channel*), группа которых образует виртуальный путь VP (*Virtual Path*). Виртуальный путь — это совокупность каналов, которые коммутируются в сети ATM на основе одного идентификатора VPI (*Virtual Path Identifier*). Виртуальный канал в сетях ATM идентифицируется парой идентификаторов виртуального пути VPI и виртуального канала VCI (*Virtual Channal Identifier*). При этом

VPI определяет единицу коммутации — виртуальный путь, а VCI — идентифицирует уникальное соединение в группе виртуальных каналов. Нумерация VPI и VCI носит только локальный характер. В сетях ATM виртуальные пути объединяются в более крупные единицы — пути передачи, состоящих из нескольких виртуальных путей.

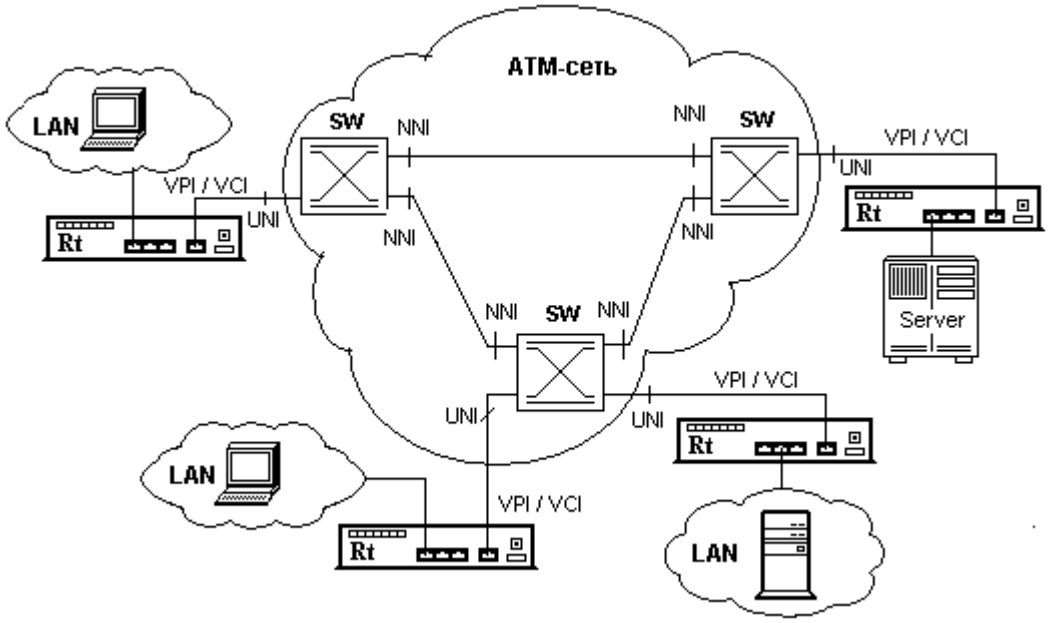


Рисунок 1.10 – Связь локальной сети с глобальной сетью ATM

В ATM определено пять классов трафика [23,27], отличающихся следующими качественными характеристиками (таблица 1.2):

- типом трафика, характеризующим допустимое отклонение скорости передачи: трафики с постоянной CBR (*Constant Bit Rate*), переменной VBR (*Variable Bit Rate*), доступной ABR (*Available Bit Rate*) или неопределенной UBR (*Unspecified Bit Rate)* скоростью;
- требованием к наличию или отсутствию непрерывной синхронизации данных между приемником и передатчиком;
- типом протокола, передающего свои данные через сеть ATM, — с установлением соединения или без установления соединения;
- наличием или отсутствием контроля ошибок.

Передача с постоянной скоростью CBR не предусматривает контроля ошибок, управления трафиком или какой-либо другой обработки данных. Класс CBR пригоден для работы с мультимедийной информацией реального времени. Передача с доступной скоростью ABR предназначена для работы в условиях быстрых вариаций трафика. Система связи гарантирует некоторую пропускную способность, но в течение короткого времени может выдержать и большую нагрузку. Этот класс предусматривает наличие обратной связи

между приёмником и отправителем, которая позволяет в случае необходимости понизить загрузку канала. Класс UBR пригоден для передачи IP-пакетов. В этом случае не гарантируется безошибочная передача, а также возможны потери в случае перегрузки тракта.

Таблица 1.2

Характеристики классов трафика сети ATM

Основные характеристики классов трафика ATM					
Класс QoS	1	2	3	4	5
Класс обслуживания	A	B	C	D	x
Тип трафика	CBR	VBR	VBR	ABR	UBR
Тип уровня ATM	AAL1	AAL2	AAL3/4	AAL3/4	AAL5
Синхронизация	Требуется		Не требуется		
Скорость передачи	Постоянная	Переменная			
Режим соединения	С установлением			Без установления	
Пример использования	(E1, T1)	Видео	аудио	Передача данных	

В ATM-сетях используется два различных типа адресации: адресация на основе стандарта ЕЛ64 (схема адресации, похожая на телефонные номера) и адресация с использованием адресов точек доступа к сетевой службе в открытых системах NSAP (*Network Service Access Point*). Схема адресации E.164 была разработана в ITU-T, а метод адресации, основанный на NSAP, был предложен ATM-форумом. Обычно адресация в соответствии со схемой E.164 используется в ATM-сетях общего пользования, предоставляемых операторами телекоммуникационных услуг, а NSAP-адресация применяется в частных ATM-сетях, например, в сетях, обеспечивающих связь ATM-коммутаторов с устройствами межсетевого взаимодействия.

Инкапсуляция сообщений протоколов верхних уровней сети ATM в ячейки ATM нужного формата происходит на уровне адаптации AAL (*ATM Adaptation Layer*), который содержит набор протоколов AAL1-AAL5. Каждый протокол уровня AAL определяет способ обработки пользовательского трафика определенного класса. На начальных этапах стандартизации каждому классу трафика был предписан свой протокол AAL, в соответствии с которым принимались в конечном узле пакеты от протокола верхнего уровня и заказывались с помощью соответствующего протокола нужные параметры трафика и качества обслуживания для данного виртуального канала. При развитии стандартов ATM такое однозначное соответствие между классами трафика и протоколами уровня AAL исчезло, и в настоящее время разрешается использовать для одного и того же класса трафика различные протоколы уровня AAL.

1.5. Широкополосный доступ по протоколу Ethernet на основе волоконно-оптических технологий FTTx

Благодаря чрезвычайно широкой полосе пропускания волоконно-оптические линии (ВОЛС) становятся в настоящее время основной транспортной средой для передачи данных мультимедийных сообщений в магистральных и городских сетях связи. Волоконно-оптическими линиями соединены между собой практически все крупные Интернет-узлы. Повсеместное внедрение таких линий на всех участках передачи цифровой информации позволило существенно увеличить качество обслуживания клиентов телекоммуникационных сетей и предложить им новые услуги, такие как доставку видео по заказу, трансляцию телевизионных каналов и видеотелефонию.

Большинство корпоративных сетей (предприятий, банков, крупных компаний), на настоящее время уже осуществляют доступ к телекоммуникационным услугам по волоконно-оптическим сетям. Подключение к провайдеру или оператору связи часто имеет вид «точка-точка» (от помещения клиента проложена оптическая линия связи до узла оператора, предоставляющего услуги). В то же время офисы малых предприятий, а также абоненты жилого сектора до сих пор используют цифровые абонентские линии (xDSL) и гибридные волоконно-коаксиальные линии (услуги от операторов кабельного телевидения), главным недостатком которых является ограниченная пропускная способность.

Тракты высокоскоростного доступа на основе волоконно-оптических технологий называют общим термином FTTx (*Fiber To The* x – волокно до точки x). Это означает, что оптоволоконный кабель проложен от узла связи до определенного места (точка "x"), а связь с абонентом осуществляется по медной паре, хотя это не исключает прокладку ВОЛС непосредственно до абонентского устройства.

Существует несколько разновидностей линий (технологий) FTTx, отличаются главным образом тем, насколько близко к пользовательскому терминалу подходит оптический кабель:

- FTTN (*Fiber To The Node*) — оптоволокно до сетевого узла, расположенного на расстоянии около 1 км от абонента;
- FTTC (*Fiber To The Curb*) — оптоволокно до распределительного шкафа, расположенного в микрорайоне, квартале или у группы домов на расстоянии около 500 м от абонента;
- FTTB (*Fiber To The Building*) — оптоволокно до здания, при максимальном удалении абонентов от точки окончания ВОЛС до 100 м;
- FTTH (*Fiber To The Home*) — оптоволокно в дом (подразумевается индивидуальный дом, коттедж, квартира либо офис абонента.

На настоящее время наибольшее распространение получили две технологии:

FTTB – волокно до здания (подразумевается многоквартирный дом) в котором точка окончания ВОЛС расположена не дальше 100 м от абонента, далее к абоненту прокладывается медный кабель.

FTTH – волокно заводится непосредственно в квартиру либо офис предприятия. Медные линии связи при этом не используются.

В США и Японии развертывание сетей FTTH в основном производится на базе технологии пассивной оптической сети PON (*Passive Optical Network*). В Европе обычно применяются топологии «точка-точка» и «кольцо» с использованием технологии *Ethernet* (*Ethernet FTTH*), сети PON FTTH встречаются реже. *Ethernet* как базовую технологию на участке доступа выбрано по причине того, что практически весь трафик данных генерируется и терминируется в сетях Ethernet/IP. Поэтому применение данной технологии на всех участках телекоммуникационной сети приводит к повышению эффективности доставки трафика.

Для продвижения технологий широкополосного абонентского доступа на базе Ethernet стандарт IEEE 802.3ah, получивший название «Ethernet на первой миле» (*Ethernet in the First Mile*, EFM). В качестве сред передачи были выбраны медные витые пары и оптическое волокно.

1.5.1. Доступ на базе пассивной оптической сети

Пассивная оптическая сеть PON (*Passive Optical Network*) не содержит каких-либо активных компонентов, а разветвление оптического сигнала осуществляется с помощью пассивных разветвителей оптической мощности — сплиттеров. Благодаря этому снижается стоимость системы доступа и уменьшается объема сетевого управления. В пассивной оптической сети PON (рисунок 1.11) реализуется схема взаимодействия «точка-много точек» (P2MP — P*oint-to-Multipoint*), в которой по одному оптическому волокну передаются данные множества каналов (32 или 64), которые на приемной стороне распределяются между соответствующими абонентами.

Сплиттер являются пассивными устройства, в них отсутствуют какие-либо электронные устройства и не используются оптические передатчики, в связи с чем для них не требуется подача электропитания. По этой причине мощность сигнала на выходах сплиттера будет ниже мощности входного сигнала. В связи с этим разработчики должны принимать во внимание баланс по мощности при определении числа выходных линий и дальности связи. Место расположения оборудования оператора связи или провайдера, к которому возможно подключение волоконно-оптической линии, получило название точки присутствия POP (*Point of Presence*). Обычно это узел связи

или центр данных, либо отдельная единица коммуникационного оборудования, вынесенная ближе к месту концентрации потенциальных клиентов.

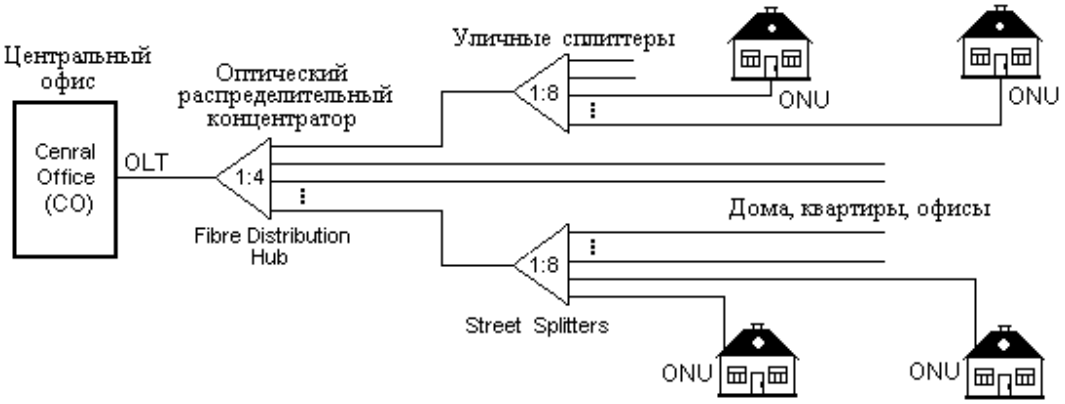


Рисунок 1.11 – Доступ по схеме точка-многоточка на базе пассивной оптической сети FTTH

В связи с тем, что провайдер сети зачастую указывает стоимость своих услуг именно в точке присутствия, а полная стоимость сетевой инфраструктуры включает стоимость линий связи от точки присутствия до клиентского оборудования и затраты на их обслуживание, то месторасположение POP имеет важное значение при проектировании сети. Передача пакетов в пассивной оптической сети FTTx регламентируется обычно протоколом Ethernet, в связи с чем такая сеть обозначается сокращенно как EPON (*Ethernet Passive Optical Network*) или GEPON (*Gigabit Ethernet Passive Optical Network*).

По терминологии PON передача пакетов в пассивных оптических сетях осуществляется между оптическим линейным терминалом OLT (*Optical Line Terminal*) — EPON-коммутатором, расположенным в центральном офисе CO (*Central Office*) провайдера и оптическим сетевым блоком ONU (*Optical Network Unit*), размещаемым либо на стороне пользователя (архитектуры (FTTH — *Fiber To The Home* и FTTB — *Fiber to The Building*), либо в месте разветвления (архитектура FTTC — *Fiber To The Curb*). Многопортовый коммутатор OLT оснащен группой оптических разъемов типа SC и несколькими слотами слотами SFP, совмещенными с разъемами RJ-45. Один порт EPON-коммутатора (OLT) позволяет подключить до 32-х EPON-модемов (ONU) на расстояниях до 20 км и скорости до 1 Гбит/с.

К недостаткам пассивных оптических сетей относится сложность или невозможность масштабирования сети по причине практически полного использования пропускной способности ВОЛС группой абонентов, а также сложность тестирования и обнаружения неисправностей. Кроме того, в связи с тем, что одной линии передаются сообщения многих пользователей, для

обеспечения конфиденциальности информации необходимо шифровать передаваемые данные.

1.5.2. Доступ на базе активной оптической сети

В активной оптической сети доступа AON (*Actsive Optical Network*) для распределения оптического сигнала применяются активные сетевые устройства (коммутаторы, маршрутизаторы, мультиплексоры). Благодаря этому пакеты, отправляемые телекоммуникационным устройством, расположенным в точке присутствия POP (*Point of Presence*), попадают непосредственно тому пользователю, которому они адресованы, т.е. устанавливается двухточечное соединение P2P (). Наибольшее распространение в сетях AON получил протокол Ethernet, а сами сети стали называться «активными оптическими Ethernet-сетями» или Ethernet FTTH (EFTTH).

Достаточно широко в активных оптических сетях доступа применяется также топология сети Ethernet типа «звезда». Для ее реализации используются выделенные одномодовые оптические линии (обычно одномодовые, одноволоконные линий с передачей кадров Ethernet по технологии 100BASE-BX или 1000BASE-BX) от каждого оконечного устройства к точке присутствия POP, где происходит их подключение к коммутатору (рисунок 1.12). Для передачи пакетов в двух направлениях применяется частотное разделение каналов.

Оконечные устройства могут находиться в отдельных жилых домах, квартирах или многоквартирных домах, на цокольных этажах которых располагаются коммутаторы. От коммутаторов проводятся линии связи (ВОЛС, симметричные или коаксиальные медные кабели) ко всем квартирам.

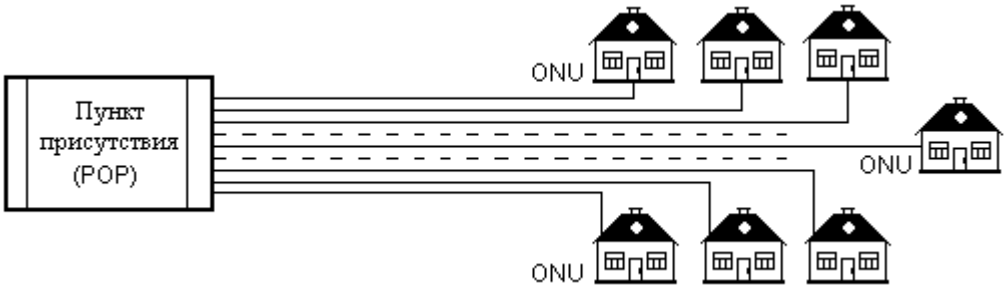


Рисунок 1.12 – Схема организации сети доступа FTTH «точка-точка»

Преимуществами сетей PON «точка-точка» является удобное подключение и простая идентификация оптических портов, гибкость структуры и лёгкость тестирования и обнаружения неисправностей. К недостаткам такой топологии следует отнести большое количество ВОЛС на магистральном

сегменте, высокая стоимость развёртывания сети, малая пригодность на участках с большим сосредоточением конечных пользователей.

1.5.3. Интерфейсы сетей PON

В сетях PON применяются как электрические, так и оптические интерфейсы. Оптические интерфейсы для EPON аналогичны используемым в традиционных оптических сетях. Как и стандартный Gigabit Ethernet, EPON имеет номинальную битовую скорость в линии 1250 Мбит/с и схему линейного кодирования 8B/10B. В одноволоконной сети EPON применяется волновое мультиплексирование WDM на длинах волн 1490 нм для прямого потока и 1310 нм — для обратного потока. Окно 1550 нм резервируется для добавления других услуг (кабельного телевидения или частных каналов). Физический уровень EPON PMD (*Physical Medium Dependent*) предусматривает два класса интерфейсов: класс 1 для малых расстояний (до 10 км при коэффициенте разветвления 1:16) и класс 2 для больших расстояний (до 20 км при коэффициенте разветвления 1:16). Это позволяет создавать оптимальные по стоимости сети PON с большим диапазоном расстояний и коэффициентов разветвления.

В сетях Gigabit и 10 Gigabit Ethernet применяются оптические интерфейсы (рисунок 1.13) на основе оптических соединителей типа LC/dual LC (а) и SC (б), а режим работы (дуплекс или полудуплекс) определяется модулем медиаконвертера типа SFP (*Small Form factor Pluggable module*).

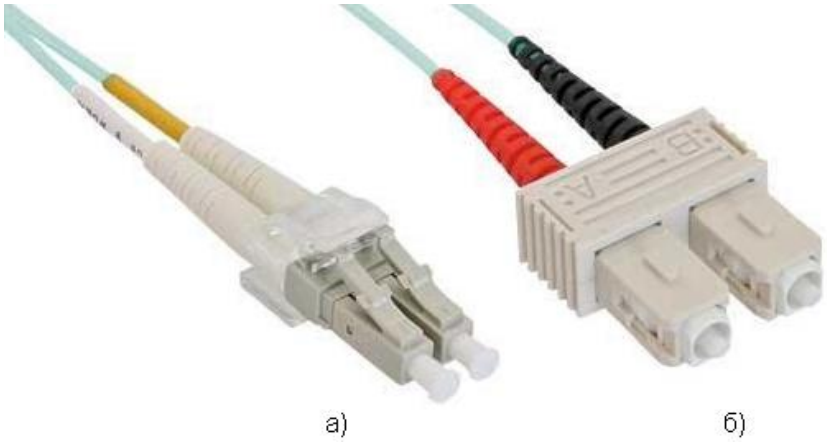


Рисунок 1.13 – Общий вид оптических дуплексных соединителей

Применение оптического разъема типа LC позволяет добиться высокой плотности монтажа в коммутационной панели или шкафу. Наконечник Разъема выполнен из керамического материала диаметром 1,25 мм. Фиксация разъема происходит за счет прижимного механизма — защелки, которая

исключает непредвиденное разъединение. Тип SC разъема оптического коннектора используется как для многомодового волокна, так и одномодового. Наконечник коннектора выполнен из керамики, а его диаметр равен 2,5 мм. Корпус коннектора изготовлен из пластика. Фиксация коннектора осуществляется поступательным движением с защелкиванием.В качестве электрического интерфейса в Gigabit Ethernet для дуплексного или полудуплексного режима работы используются соединители типа 8P8C (другое название RJ45).

Скорость передачи, параметры линейного кодирования и другие характеристики в PON регламентируются стандартом IEEE 802.3ah, который определяет:

- скорость передачи 1 Гбит/с;
- линейное кодирование 8B/10B;
- WDM мультиплексирование с длиной волны прямого потока 1490 нм (1550 нм — кабельное ТВ) и длиной волны обратного потока 1310 нм;
- уровень ошибок по битам (BER) — 10^{-12};
- интерфейсы класса 1 со стороны OLT — 1000BASE-PX10-D и 1000BASE-PX10-U со стороны ONT;
- интерфейсы класса 2 со стороны OLT — 1000BASE-PX20-D и 1000BASE-PX20-U со стороны ONT;
- максимальное допустимое расстояние от OLT до ONT для EPON класса 1 — 10 км и EPON класса 2 — 20 км.

Стандартом предусмотрена возможность использование коррекции ошибок для увеличения числа узлов, подключенных к одному фидерному волокну.

2. Планирование сетей, распределение и преобразование адресов

2.1. Разработка логической структуры сети

Логическая структура компьютерной сети представляет собой схему, на которой изображены все рабочие станции (PC) сети, узлы коммутации и распределения информации, а также все логические связи, по которым осуществляется обмен информацией между компонентами сети.

При построении компьютерной сети рекомендуется использовать иерархическую звездную топологию [22,23]. В этом случае кабели от каждой из телекоммуникационных розеток заканчиваются на телекоммуникационном распределительном пункте этажа – «кроссовой». Здесь же зачастую устанавливается коммуникационное и серверное оборудование. С помощью специальных соединительных пач-кабелей осуществляется постоянное соединение (*кроссирование*) кабелей с коммуникационным оборудованием (концентраторами, коммутаторами, маршрутизаторами), которое реализует требуемую топологию сети. В кроссовом помещении может осуществляться соединение нескольких коммутаторов между собой для формирования иерархической структуры. Если же рабочей группе требуется повышенная информационная безопасность или нужно дисковое пространство, выделение которого на головном сервере предприятия представляется нецелесообразным, то в этом случае для рабочей группы следует устанавливать отдельный сервер, который выполняет также функции сервера приложений.

Для обеспечения более высокой пропускной способности и безопасности информации целесообразно осуществлять логическую структуризацию сети — разбиения ее на более мелкие части (сегменты) с локализованным трафиком. Структуризация позволяет повысить производительность, безопасность, гибкость и управляемость сети [17,19]. Уменьшение размера сегмента снижает нагрузку на него и в результате возрастает его пропускная способность. Повышение гибкости сети поясняется тем, что в результате сегментации каждый из новых сегментов может быть адаптирован к специфическим потребностям рабочей группы или отдела. Безопасность данных в сегментированной сети можно повысить путем применения различных фильтров на мостах или коммутаторах. В результате этого возможно контролировать доступ пользователей к сетевым ресурсам.

При разработке логической схемы сети необходимо также учитывать порядок взаимодействия серверов и пользователей локальной сети с глобальными сетями. Для разделения внутренней и публичной сетей целесообразно ввести д**емилитаризованную зону DMZ** (*Demilitarized Zone*). Своеобразность DMZ заключается в том, что эта часть сети не входит непосредственно ни во внутреннюю, ни во внешнюю сеть, и доступ к ней может осу-

ществляться только по заранее заданным правилам межсетевого экрана [15]. На практике DMZ выполняется как отдельная IP-подсеть, вынесенная в самостоятельный сегмент сети, который физически либо с помощью технологии виртуальных сетей отделен от внутренний локальной сети предприятия. В DMZ-зону можно включить всего один компьютер, указав принадлежность его IP-адреса к DMZ-зоне.

При больших размерах сети для ограничения взаимодействия отделов между собой целесообразно использовать технологию виртуальных сетей – VLAN. Для обеспечения быстрой маршрутизации между VLAN рекомендуется применять технологию Layer 3 switching.

2.2. Размещение серверов в локальной сети

Серверы в локальной сети предприятия играют важнейшую роль. Они предоставляют всем или большинству пользователей сетевые услуги, а также доступ к сетевым ресурсам.

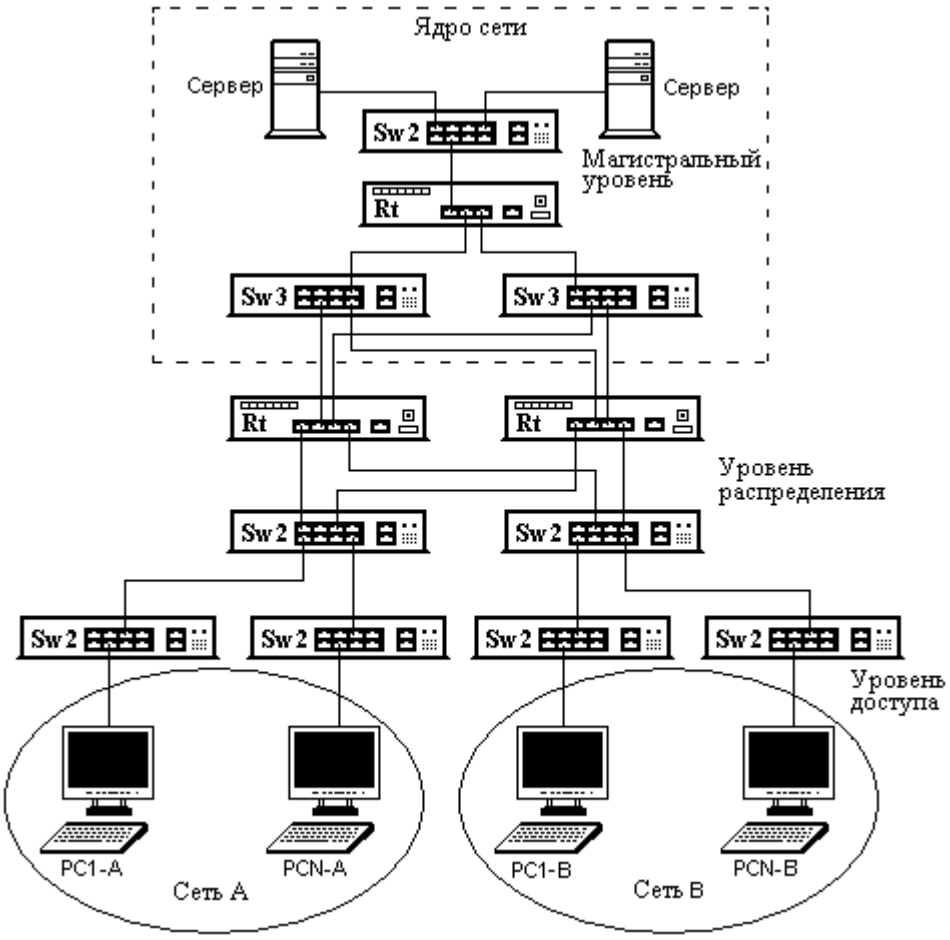


Рисунок 2.1 – Схема централизованного подключения серверов

Различают два типа серверов: централизованные (*Enterprise Servers*) и распределенные серверы [31,32]. Централизованные серверы обслуживают всех или большую часть пользователей сети (например, E-Mail сервер). Распределенные серверы предоставляют услуги определенной группе пользователей. Их называют также серверами рабочих групп, или просто локальными серверами. В связи с тем, что между серверами и сетью циркулируют большие информационные потоки, то место подключения серверов к сети непосредственно влияет на ее производительность. При централизованном использовании сервера он подключается непосредственно к магистрали сети (рисунок 2.1). В связи с этим информационные потоки к серверу и от него проходят через маршрутизатор и коммутаторы ядра сети, что при высокой интенсивности запросов может привести к перегрузке магистрального канала сети.

Сервер рабочей группы обычно подключается к подсети, состоящей из клиентов, которым предоставляет услуги данный сервер (рисунок 2.2).

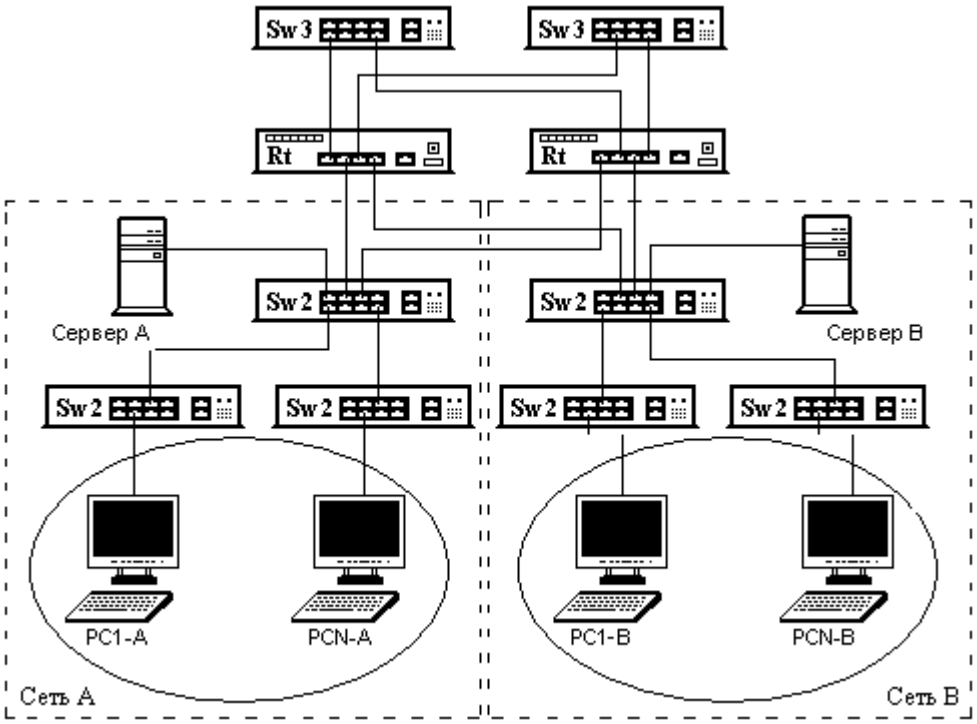


Рисунок 2.2 – Схема распределенного подключения серверов

Использование распределенных серверов позволяет локализировать трафик в пределах одного или нескольких сегментов и тем самым существенно уменьшить циркулирующий в сети трафик Применение того или иного типа серверов имеет свои преимущества и недостатки. Наиболее рациональным решением является использование в проектируемой сети обоих типов серверов. Там где можно локализировать трафик в одном или не-

скольких сегментах сети, следует устанавливать локальный сервер рабочей группы. Серверы приложений, к которым требуется доступ от многих или всех пользователей, следует включать по схеме централизованного сервера.

2.3. Деление сети на логические сегменты

Для разделения информационных потоков компьютеров различных служб организации, относительно редко взаимодействующих друг с другом, возможности сокрытия структуры организации со стороны незащищенной сети, администраторы осуществляют структуризацию своей сети, т.е. разделяют ее на несколько независимых логических сегментов —подсетей. Подсеть представляет собой подмножество сети, не пересекающееся с другими подсетями, входящими в ее состав.

Сегментация позволяет уменьшить число пользователей на один сегмент, снизить объем широковещательного трафика и тем самим повысить производительность сети в целом [18,21,30]. Каждый сегмент большой сети Ethernet также использует метод доступа CSMA/CD, но функционирует как отдельная независимая **подсеть**. По разделяемой среде сегмента циркулирует трафик компьютеров, подключенных только к данной среде. Благодаря этому пропускная способность среды делится между компьютерами, которые непосредственно соединены с ней. Обычно в подсеть включают компьютеры, выполняющие однотипные задачи (бухгалтерия, служба главного механика, отдел сбыта и т.п.), или входящие в одну административную единицу (отдел, лаборатория). Такую совокупность компьютеров называют **рабочей группой.**

Сегментация сети может осуществляться на основе коммутаторов или маршрутизаторов.

2.3.1. Виртуальные локальные сети VLAN

Разделение локальной сети на независимые сегменты может осуществлять сетевой коммутатор (*Swtch*). **Коммутатор** представляет собой мультипроцессорный мост, способный независимо транслировать кадры между всеми парами своих портов. Благодаря этому коммутаторы, разделяя локальную сеть на подсети, делят единый коллизионный домен на отдельные поддомены, свободные от коллизий. Коммутатор создает соединение между своими портами по принципу "точка-точка". Поэтому компьютеры, подключенные к этим портам, имеют в своем распоряжении пропускную способность (10, 100, 1000 или 10000 Мбит/с), которую способны обеспечить соответствующие порты коммутатора.

В результате деления компьютерной сети на логически изолированные сегменты коммутатором формируются виртуальные локальные сети ***VLAN***

(*Virtual LAN*). Виртуальной локальной сетью называется совокупность узлов некоторой компьютерной сети, трафик которой, в том числе широковещательный, на канальном уровне полностью изолирован от трафика других узлов этой сети [10,17,31]. Это означает, что передача кадров между разными виртуальными сетями на основании MAC-адреса невозможна.

Основное назначение технологии *VLAN* – недопущение трафика из одной сети в другую. Это делается либо с целью увеличения реальной пропускной способности сегментов сети, или с целью защиты от несанкционированного доступа. Виртуальные сети возможно создавать на основе коммутаторов из групп пользователей, основываясь на их задачах, а не по физическому расположению в сети. *VLAN* могут быть построены на базе одного или нескольких коммутаторов [2,10,12,32].

Виртуальные сети на основе одного коммутатора создаются в небольших организациях, в которых рабочие группы состоят из 2…6 компьютеров. В таких сетях применяется механизм *группирования портов* коммутатора. На рисунке 2.3 показано, как компьютерная сеть одной организации, содержащей два файл-сервера ФС и 8 рабочих станций, разделена на три виртуальные сети.

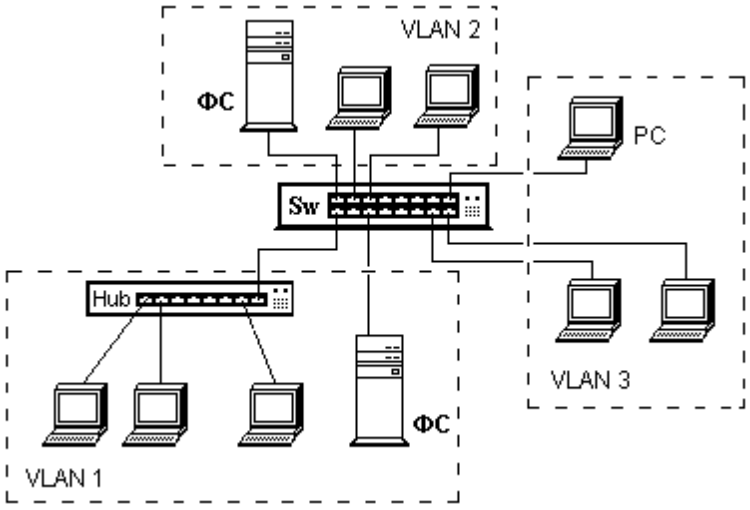


Рисунок 2.3 – Виртуальные сети, построены на основе одного коммутатора

При использовании механизма группировании портов каждый порт программным образом назначается одной из виртуальных сетей. Обмен данными в таком случае будет осуществляться только между указанными портами. Порт можно приписать нескольким виртуальным сетям, однако, в случае требований повышенной безопасности это действие исключается. Достоинством VLAN на базе портов является высокий уровень управляемости и безопасности. К недостаткам такого вида сетей следует отнести необходи-

мость физического переключения устройств при изменении конфигурации отдельных сетей. Другим способом создания виртуальных сетей на базе одного коммутатора является группирование MAC-адресов, при котором каждый физический адрес приписывается той или иной виртуальной сети.

На рисунке 2.4 показана схема реализации двух виртуальных локальных сетей VLAN 1 и VLAN 2, созданных на основе двух коммутаторов [33]. На рисунке узлы, относящиеся к VLAN 1, заштрихованы.

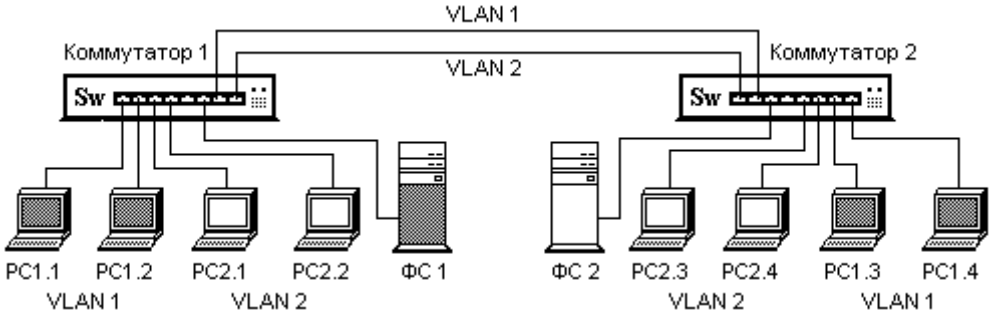


Рисунок 2.4 – Виртуальные сети на основе двух коммутаторов

При использовании механизма группирования портов между коммутаторами должно быть установлено столько связей (выделено портов), сколько виртуальных сетей они поддерживают. Это приводит к повышению расходов кабелей на создание сетей. Группирование MAC-адресов по виртуальным сетям избавляет от необходимости связывать коммутаторы посредством нескольких кабелей. В таком случае распределение кадров по сетям выполняется коммутаторами на основе MAC-адресов, являющихся признаком принадлежности к конкретной виртуальной сети. К недостаткам VLAN, созданных на базе MAC-адресов относятся дополнительные затраты времени на ручную установку MAC-адресов всех устройств сети и распределение их по соответствующим виртуальным сетям, VLAN. При добавлении рабочей станции или замене сетевой карты её MAC-адрес необходимо заново добавлять в таблицу коммутации. Кроме того, возникают проблемы с доступом мобильных клиентов с гостевыми подключениями.

Способы создания VLAN во многом определяются возможностями коммутаторов, с помощью которых строятся виртуальные сети. С каждым годом эти возможности расширяются. В настоящее время существуют коммутаторы и программные средства, которые позволяют создавать VLAN на сетевом уровне, на базе протоколов и на базе правил. Виртуальные ЛВС сетевого уровня дают возможность администратору связать трафик для того или иного протокола в соответствующей виртуальной сети. Администратор может самостоятельно выбрать поля в заголовках кадров, по которым будет определяться принадлежность к виртуальной сети, и загрузить подготовленные правила во все коммутаторы сети.

Виртуальная локальная сеть на базе правил — наиболее мощная реализация VLAN, позволяющая администратору использовать любые комбинации критериев для создания виртуальных сетей. После того, как правила загружены во все коммутаторы, они обеспечивают организацию VLAN на основе заданных администратором критериев. Поскольку в таких сетях кадры постоянно анализируются коммутаторами на предмет соответствия заданным критериям, принадлежность пользователей к виртуальным сетям может меняться в зависимости от текущей деятельности пользователей.

2.3.2. Виртуальные сети с магистральной связью

Для уменьшения количества связей между коммутаторами, на которых сконфигурированы несколько виртуальных сетей, используется одна магистральная линия (рисунок 2.5). По терминологии Cisco такое соединение называется транковым (*Trunk*). В магистральной линии мультиплексируются кадры, принадлежащие различным VLAN.

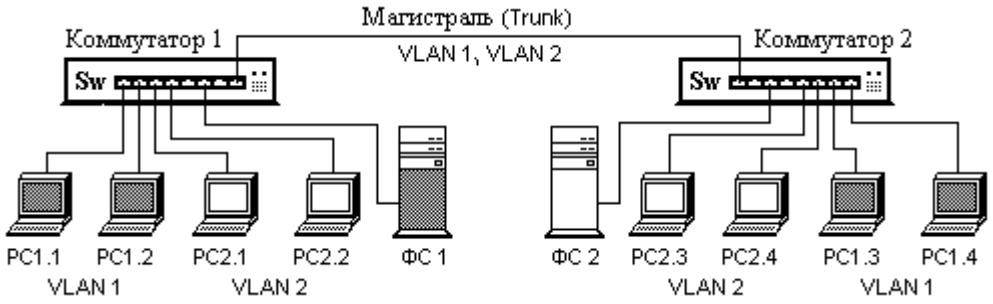


Рисунок 2.5 — Связь коммутаторов магистральной линией

Разделение (демультиплексирование) входящих кадров производится на основании идентификаторов виртуальных сетей, которые включаются (инкапсулируются) в кадры Ethernet. Способ маркировки виртуальных сетей и формат Ethernet-кадров регламентируется международным стандартом **IEEE 802.1Q**. Корпорация Cisco разработала собственный протокол маркирования VLAN, который получил название «межкоммутаторный канал» ISL (*Inter Switch Link*). Коммутаторы Cisco поддерживают оба протокола.В соответствии со стандартом IEEE 802.1Q к кадру Ethernet добавлен специальный маркер виртуальной сети (*Tag*) размером в четыре байта. Эти 32 теговых бита содержат информацию о принадлежности кадра Ethernet к конкретной VLAN и о его приоритете. Процедура добавления информации о принадлежности к 802.1Q VLAN в заголовок кадра называют маркированием кадра (*Tagging*), а извлечение маркера — *Untagging*.

Очевидно, что изменение структуры кадра Ethernet влечет за собой возникновение серьезных проблем, так как нарушается совместимость со

всеми традиционными устройствами Ethernet, ориентированными на старый формат кадра. Это связано с тем, что данные 802.1q размещаются перед полем с информацией о длине полезной нагрузки (или типе протокола). Традиционное сетевое устройство в процессе анализа заголовка не обнаружит эту информацию на обычном месте. На его месте располагается "маркер" виртуальной сети (рисунок 2.6). Новое поле состоит из тэга (маркера) протокольного идентификатора **TPID** (*Tag Protocol Identifier*) и тега управляющей информации **TCI** (*Tag Control Information*). Поле TPID имеет длину два байта и содержит фиксированный код 0x8100, который информирует, что кадр содержит тег протокола 802.1Q/802.1P. Поскольку это число больше максимальной длины кадра *Ethernet* (1500), то сетевые карты *Ethernet* будут интерпретировать его как тип, а не как длину кадра. Структура полей TCI изображена в нижней части рисунка 2.6

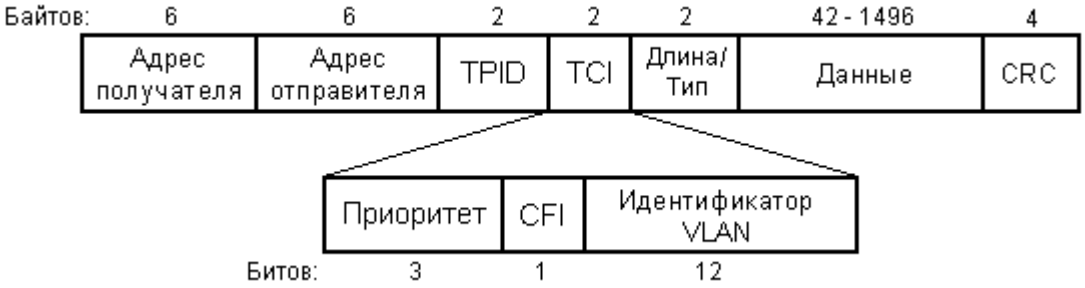


Рисунок 2.6 - Формат кадра Ehternet с меткой виртуальной сети

Трехбитовое поле "**Приоритет**" позволяет задавать 8 уровней приоритета передаваемых кадров и тем самым выделять *трафик реального времени*, *трафик со средними требованиями* и трафик, для которого *время доставки не критично*. Это открывает возможность использования сети Ethernet для задач управления и обеспечения качества обслуживания (QoS) при транспортировке мультимедийных данных. Наивысший уровень приоритета имеют кадры управления сетью, следующий приоритет задается кадрам передачи голосового трафика, а следующий, более низкий уровень, установлен для видеоданных. Остальные уровни предназначены для маркировки данных с разными требованиями по задержке доставки пакетов.

Однобитовое поле **CFI** (*Canonical Format Indicator*) зарезервировано для обозначения кадров сетей других типов (Token Ring, FDDI), передаваемых по магистрали Ethernet. В настоящее время его функцией (CFI=1) является указание того, что в поле данных содержится кадр сети *Token Ring* (Стандарт IEEE 802.5).

Поле "**Идентификатор VLAN**" VID (*VLAN Identifier*) длиной 12 бит определяет, какой виртуальной сети принадлежит кадр. 12-битовое поле позволяет коммутаторам разных производителей создавать до 4096 общих

виртуальных сетей. Обычно виртуальные сети VID0 и VID4095 резервируются.

Каждый физический порт коммутатора имеет параметр, называемый идентификатор порта VLAN (PVID). Этот параметр используется для того, чтобы определить, в какую VLAN коммутатор направит входящий немаркированный кадр с подключенного к порту сегмента, когда кадр нужно передать на другой порт (внутри коммутатора в заголовки всех немаркированных кадров добавляется идентификатор VID, соответствующий PVID порта, на который они были приняты). Этот механизм позволяет одновременно существовать в одной сети устройствам с поддержкой и без поддержки стандарта IEEE 802.1Q.

Коммутаторы, поддерживающие протокол IEEE 802.1Q, должны хранить таблицу, связывающую идентификаторы портов PVID с идентификаторами VID сети. При этом каждый порт такого коммутатора может иметь только один PVID и столько идентификаторов VID, сколько VLAN поддерживает данная модель коммутатора. Если на коммутаторе не настроены VLAN, то все порты по умолчанию входят в одну VLAN с PVID=1.

Решение о продвижении кадра внутри виртуальной локальной сети принимается на основе трех следующих видов правил:

1) правила входящего трафика (*ingress rules*) — классификация получаемых кадров относительно принадлежности к VLAN.
2) правила продвижения между портами (*forwarding rules*) — принятие решения о продвижении или отбрасывании кадра.
3) правила исходящего трафика (*egress rules*) — принятие решения о сохранении или удалении в заголовке кадра тега 802.1Q перед его передачей.

Правила входящего трафика выполняют классификацию каждого получаемого кадра относительно принадлежности к определенной VLAN, а также могут служить для принятия решения о приеме кадра для дальнейшей обработки или его отбрасывании на основе формата принятого кадра.

Классификация кадра по принадлежности VLAN осуществляется следующим образом:

- если кадр не содержит информацию о VLAN (немаркированный кадр), то в его заголовок коммутатор добавляет тег с идентификатором VID, равным идентификатору PVID порта, через который этот кадр был принят;
- если кадр содержит информацию о VLAN (маркированный кадр), то его принадлежность к конкретной VLAN определяется по идентификатору VID в заголовке кадра, а значение тега в нем не изменяется.

Активизировав функцию проверки формата кадра на входе, администратор сети может указать, кадры каких форматов будут приниматься коммутатором для дальнейшей обработки. Большинство типов управляемых

коммутаторов позволяют, либо обоих типов кадров — маркированных и немаркированных. Внутри коммутатора все кадры являются маркированными!

В соответствии с правилами продвижения между портами осуществляется принятие решения об отбрасывании или передаче кадра на порт назначения на основе его информации о принадлежности конкретной VLAN и MAC-адреса узла-приемника.

Если входящий кадр маркированный, то коммутатор определяет, является ли входной порт членом той же VLAN, путем сравнения идентификатора VID в заголовке кадра и набора идентификаторов VID, ассоциированных с портом, включая его PVID. Если нет, то кадр отбрасывается. Этот процесс называется входной фильтрацией (Ingress Filtering) и используется для сохранения пропускной способности внутри коммутатора путем отбрасывания кадров, не принадлежащих той же VLAN, что и входной порт, на стадии их приема. Если кадр немаркированный, входная фильтрация не выполняется. Затем определяется, является ли порт назначения членом той же VLAN. Если нет, то кадр отбрасывается. Если же выходной порт входит в данную VLAN, то коммутатор передает кадр в подключенный к нему сегмент сети.

Правила исходящего трафика определяют формат исходящего кадра — маркированный или немаркированный. Если выходной порт является немаркированным (*Untagged*), то он будет извлекать тег 802.1Q из заголовков всех выходящих через него маркированных кадров. Если выходной порт настроен как маркированный (*Tagged*), то он будет сохранять тег 802.1Q в заголовках всех выходящих через него маркированных кадров.

Формат кадра проприетарного протокола ISL корпорации Cisco с инкапсулированной информацией о виртуальной сети показан на рисунке 2.7. В ISL-заголовок входит ряд полей, в частности [2,3,6]:

- 40-битный широковещательный адрес, указывающий, что данный кадр имеет инкапсуляцию ISL;
- 4-битовый индикатор сети отправителя, причем код 0 — это сеть *Ethernet*, 1 — FR, 2 — FDDI, 3 — ATM;
- MAC-адрес отправителя;
- указатель длины данных (16 битов);
- номер сети VLAN-отправителя, которой принадлежит исходный блок (15 битов);
- номер порта коммутатора-отправителя;

ряд других полей.

Коммутатор, отправляя кадр через магистральный интерфейс (порт), функционирующий в соответствии с протоколом ISL, присоединяет к исходному блоку данных ISL-заголовок и указывает его принадлежность к сети VLAN-отправителя. Управление виртуальными локальными сетями по умолчанию осуществляется через VLAN1 (*Default VLAN*). Поэтому при конфигурировании коммутатора, как минимум, один порт должен относиться к

VLAN1, чтобы можно было управлять коммутатором. Все остальные порты коммутатора могут быть назначены другим виртуальным сетям.

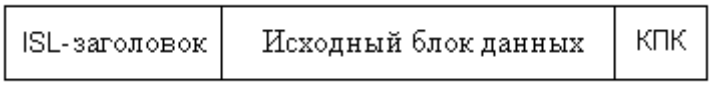


Рисунок 2.7 – Формат инкапсулированного ISL-кадра

Передача пакетов между виртуальными сетями может быть осуществлена только через маршрутизатор. Поэтому, чтобы виртуальные сети могли обмениваться между собой пакетами каждой VLAN при конфигурировании должен быть назначен IP-адрес с соответствующей маской.

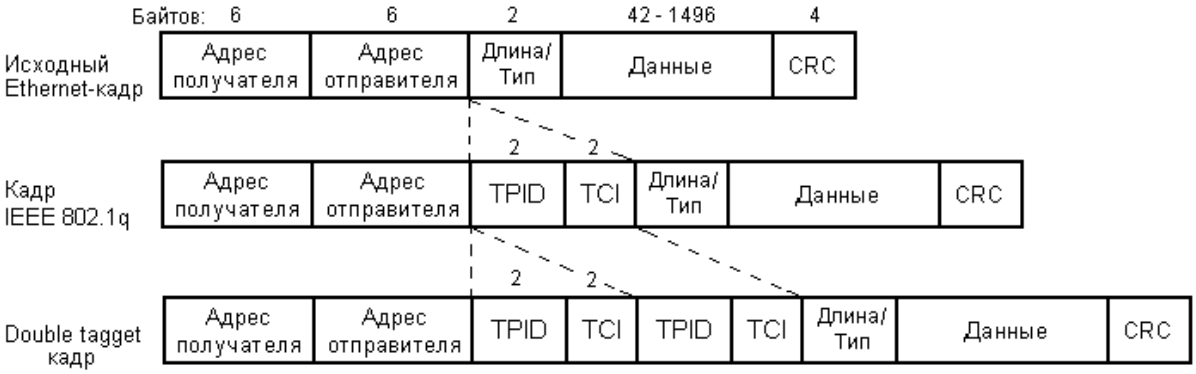


Рисунок 2.8 – Форматы кадров по стандартам IEEE 802.1Q и IEEE 802.1ad

Дальнейшим расширением стандарта IEEE 802.1Q стал стандарт IEEE 802.1ad, которым была введена функция **Q-in-Q** — двойной виртуальной сети (*Double VLAN*). Она позволяет добавлять в маркированные кадры *Ethernet* второй тег IEEE 802.1Q. Благодаря функции Q-in-Q провайдеры могут использовать их собственные уникальные идентификаторы VLAN (называемые *Service Provider* VLAN ID или SP-VLANID) при оказании услуг пользователям, в сетях которых настроено несколько VLAN. Это позволяет сохранить используемые пользователями идентификаторы VLAN (Customer VLAN ID или CVLAN ID), избежать их совпадения и изолировать трафик разных клиентов во внутренней сети провайдера. На рисунке 2.8 изображены форматы обычного кадра Ethernet, кадра Ethernet с тегом 802.1Q и кадра Ethernet с двумя тегами 802.1Q.

2.3.3. Логические сегменты на основе маршрутизаторов

Создание независимых подсетей, как отмечалось выше, пожет быть выполнено на основе маршрутизаторов. **Маршрутизатор** — это устройство,

распределяющее пакеты по сети с помощью информации сетевого уровня. При этом основной задачей маршрутизатора является нахождение наилучшего (оптимального) пути прохождения пакета по сети от источника до получателя [13,18,30,31]. Критерием оптимальности служит некоторая метрика (скорость передачи пакетов, время задержки, количество узлов на маршруте, стоимость доставки и т.п.).

Так как маршрутизаторы работают на третьем уровне эталонной модели, то они исполняют больше функций, по сравнению с мостами и коммутаторами. Они, подобно мостам, дают возможность расширить сеть и позволяют ограничивать домены коллизий. Кроме этого маршрутизаторы предотвращают распространение широковещательных сообщений в сети, что позволяет создавать отдельные широковещательные домены. Блокировка распространения широковещательных сообщений маршрутизаторами определяет границы **широковещательного домена** — области, за пределы которой не выходят широковещательные сообщения, генерируемые компьютерами сети.

Маршрутизаторы способны соединять сегменты с абсолютно разными схемами упаковки данных в пакеты и доступа к среде, им часто доступны несколько путей. При отказе одного из маршрутизаторов или части его портов, данные будут передаваться по другим маршрутизаторам. Используя сведения о загруженности участков сети и о стоимости пути, маршрутизатор выбирает оптимальный путь.

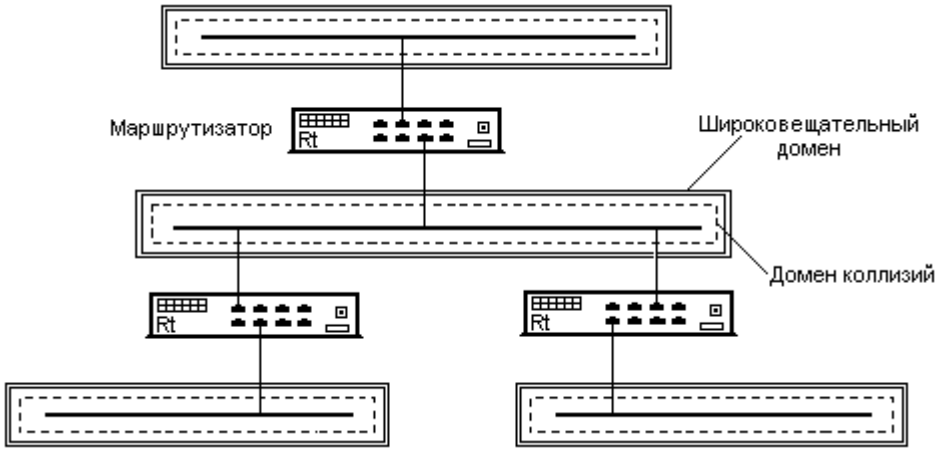


Рисунок 2.9 – Разделение сети на домены посредством маршрутизаторов

На рисунке 2.9 изображена сеть, построенная на основе маршрутизаторов, и показаны границы доменов коллизий (штриховая линия) и широковещательных доменов (двойная линия). Разделение сегментов с помощью маршрутизаторов приводит к тому, что в сети создается несколько широковещательных доменов, а каждый сегмент принадлежит отдельной подсети. В связи с этим принципы функционирования рабочих станций в сети с марш-

рутизаторами отличаются от принципов работы в сетях, объединенных с помощью мостов.

В сетях с мостами и повторителями рабочие станции передают кадры так же, как если бы отправитель и получатель находились в одном домене коллизий.

2.4. Распределение и трансляция сетевых адресов

2.4.1. Агрегирование адресов

Выбор и планирование адресов является одним из важнейших этапов проектирования локальных корпоративных сетей. Нерациональное распределение адресов может привести к затруднениям при масштабировании спроектированной сети, а также к появлению сбоев в работе крупномасштабных сетей. Принимая решение о выделении сетевых адресов, необходимо учитывать две основные цели адресации:

- уменьшение размеров таблицы маршрутизации;
- уменьшение расстояния, на которое может распространяться информация об изменении топологии сети.

Наиболее эффективным средством, позволяющим достичь обе эти цели, является агрегирование (объединение) адресов (*addresses aggregation*) [20].

Агрегирование (объединение) адресов — это замена нескольких смежных адресов IP-сетей на один обобщающий адрес с более короткой сетевой маской, указывающий на то же самое адресное пространство. Суть объединения сетевых адресов заключается в том, что вместо нескольких адресов сетей более низкого уровня в таблицу маршрутизации вышестоящего маршрутизатора заносится сетевой укороченный адрес, являющийся общей частью (префиксом) адресов нижележащих сетей. Для пояснения этого принципа рассмотрим пример некоторой сети, изображенной на рисунке 2.10. Маршрутизаторы уровня доступа **A, B, C** и **D** осуществляют пересылку пакетов в сети с ответствующими адресами: 172.16.4.0/24, 172.16.5.0/24, 172.16.6.0/24 и 172.16.7.0/24. Нетрудно заметить, что адреса сетей отличаются двумя младшими битами третьего октета. Для доставки пакетов к этим сетям все выше расположенные маршрутизаторы E, F, G и H должны содержать соответствующие записи о достижимости данных сетей в своих маршрутных таблицах. А чем выше расположен маршрутизатор, тем более громоздкая его таблица маршрутизации и тем больше времени требуется для завершения процесса сходимости.

Стабильность сети, как известно [20,31], в значительной степени зависит от количества маршрутизаторов, участвующих в процессе модификации

таблиц маршрутизации, который инициируется при появлении каких-либо изменений в сети.

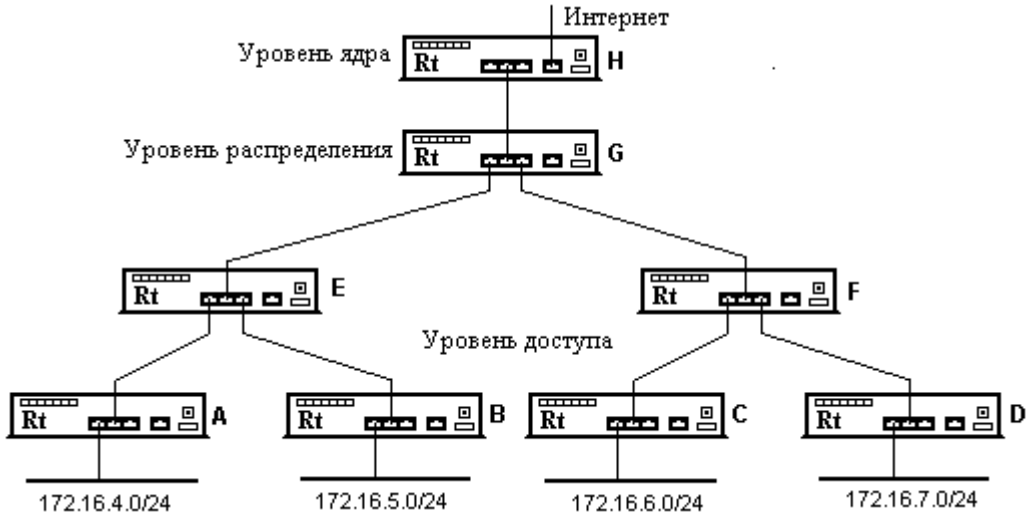


Рисунок 2.10 – Пример фрагмента локальной сети предприятия

Поэтому для ускорения процесса сходимости нужно замаскировать вышестоящему маршрутизатору **H**, непосредственно не связанному с уровнем доступа, сведения об изменении топологии на уровне доступа. В таком случае маршрутизатору **H** не придется производить пересчет своей таблицы маршрутизации при отказе каналов, ведущих к сетям 172.16.4.0/24 – 172.16.7.0/24. Такую маскировку можно осуществить путем объединения маршрутов 172.16.4.0/24 – 172.16.7.0/24 в один маршрут 172.16.4.0/22. Как видно из этой записи, маска префикса сети сместилась на два бита влево, т.е. она выделяет теперь префикс, который является общим для всех четырех сетей уровня доступа. Следовательно, процесс объединения адресов осуществляется администратором путем измерения маски сети. Обратите внимание, что агрегирование (объединение) адресов возможно только при использовании бесклассовой междоменной маршрутизации CIDR!

При выборе участка сети, на котором должно выполняться агрегирование, следует предоставлять полную информацию о топологии только на тех участках сети, где это действительно необходимо. Так вместо того, чтобы выдавать устройствам ядра полные адреса отдельных подсетей и рабочих станций, маршрутизаторы уровня распределения должны объединять каждую группу адресов уровня доступа путем укорачивания префикса и предоставлять ядру информацию об агрегированных маршрутах.

Маршрутизаторы уровня доступа также не должны обладать информацией обо всех специфических пунктах назначения сети. Единственная информация, которая действительно нужна маршрутизатору уровня доступа, это данные, достаточные для принятия решения о направлении трафика на один (или два) подключенных к данному сегменту маршрутизаторов уровня

распределения. В большинстве случаев маршрутизаторам уровня доступа достаточно сведений об одном маршруте, так называемом маршруте по умолчанию или стандартном маршруте.

Наиболее рациональным участком в иерархической сети для проведения агрегирования является уровень распределения. Поэтому, прежде чем передать уровню ядра сведения о достижимости мест назначения, маршрутизаторы уровня распределения должны произвести агрегирования адресов назначения. Это позволит ограничить область распространения сведений об изменениях топологии сети одним лишь локальным участком уровня распределения. Агрегирование, осуществляемое на уровне распределения по отношению к маршрутизаторам уровня доступа, позволяет существенно уменьшить объем информации, обрабатываемой маршрутизаторами.

Рассмотрим примеры агрегирования маршрутной информации, передаваемой с уровня распределения на ядро и уровень доступа для сети, изображенной на рисунке 2.11 [21]. Маршрутизатор уровня распределения М5, объединяющий маршрутизаторы уровня доступа М1-М4 и маршрутизатор ядра М6, получает следующие сетевые адреса с уровня доступа (таблица 2.1). Как видно из двоичной записи, общим префиксом для всех адресов являются первые три октета. При объединении этих адресов в один два младших бита сетевого адреса можно перенести на адрес хоста. Поэтому сетевая маска должна выделять 24 бита общего префикса.

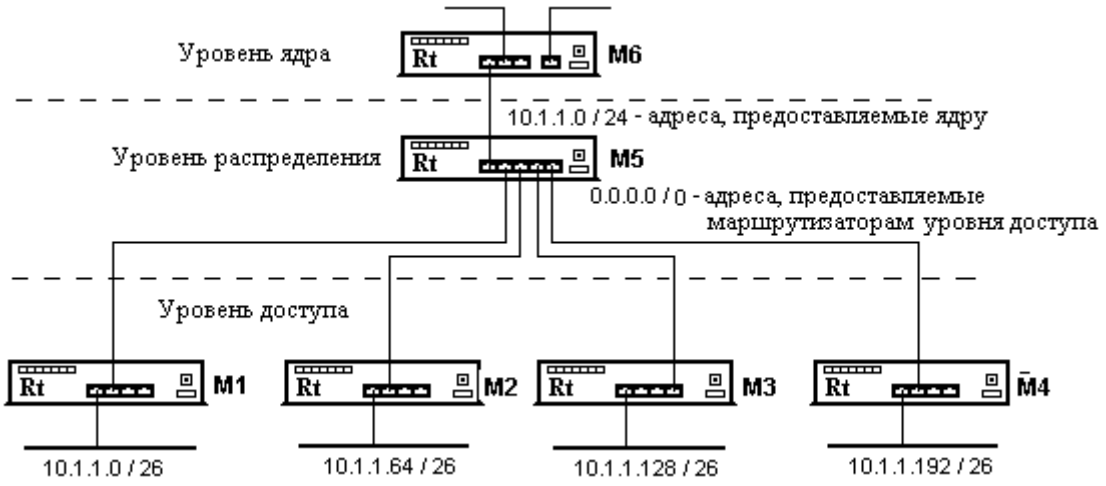


Рисунок 2.11 – Рассылка маршрутной информации в направление ядра и устройств уровня доступа

Для пакетов, отправляемых маршрутизаторами уровня доступа во внешнюю сеть, имеется только один путь. Поэтому в процессе агрегирования адресов, все записи таблиц маршрутизации узлов М1-М4 объединяются в одну – 0.0.0.0/0. Этот адрес называют стандартным маршрутом или маршрутом по умолчанию.

Таблица 2.1

Адреса сетей в десятичной и двоичной записи

Номера сетей	Десятичная запись IP-адреса	Двоичная запись IP-адреса
1	10.1.1.0 / 26;	00001010. 00000001. 00000001. 00000000
2	10.1.1.64 / 26;	00001010. 00000001. 00000001. 01000000
3	10.1.1.128 / 26;	00001010. 00000001. 00000001. 10000000
4	10.1.1.192 / 26;	00001010. 00000001. 00000001. 11000000

2.4.2. Распределение и планирование адресов

При распределении набора сетевых адресов между подсетями корпоративной сети могут быть использованы следующие способы выделения адресов [21].

- **Последовательный**. У провайдера имеется достаточное количество адресов и он из имеющегося списка выделяет их для адресации вновь создаваемых сетей в порядке поступления заявки.
- **Структурный**. Каждому структурному подразделению организации выделяется собственное пространство адресов.
- **Географический.** Региональным отделениям или филиалам организации, расположенным географически в разных местах, выделяется собственное пространство адресов.
- **Топологический.** Адрес подсети зависит от точки подключения к общей сети предприятия. В некоторых случаях может совпадать с географическим распределением адресов.

Последовательный способ являлся самым распространенным в первых корпоративных сетях, что объясняется его простотой и долговременной стабильностью структуры сети. В процессе роста масштабов сети, оказывалось, что подсети, располагаемые на общих магистральных участках, имели адреса, существенно отличающиеся друг от друга. По этой причине весьма проблематичным стало реализовать объединение адресов таких подсетей. В связи с этим резко увеличивались размеры таблиц маршрутизации и нарушалась устойчивость работы сети.

Структурный способ позволяет в некоторой степени проводить агрегацию адресов подсетей, однако рост масштабов сети также ограничен. При географическом способе адресное пространство распределяется в соответствии с пространственным расположением сегментов сети. Во многих случаях этот способ распределения адресов дает возможность объединения адресов, однако малопригоден для проведения эффективной оптимизации маршрутной информации.

Наиболее эффективным способом распределения адресов, гарантирующим возможность агрегирования маршрутов, является распределение адресов в зависимости от принадлежности к маршрутизатору, к которому подсоединена подсеть, т.е. по топологическому признаку. Конфигурация маршрутизаторов при этом оказывается достаточно проста, а топология сети остается достаточно стабильной на протяжении значительного временного промежутка. Единственный недостаток топологического способа распределения – сложность определения по имени (адресу) принадлежности рабочей станции или подсети без знания топологии всей сети.

Этот недостаток минимизируется при комбинировании топологического принципа с другими способами распределения адресов. Так, например, учитывая, что IP-адрес состоит из четырех октетов, два левых октета можно предоставить для географической адресации сети, а третий октет – для адресации по структурному принципу.

При распределении пространства возможных адресов необходимо учитывать следующие особенности:

- каждое устройство или интерфейс должны иметь уникальный ненулевой номер;
- адрес, состоящий из единиц, зарезервирован для IP-широковещания в сети;
- нулевое значение адреса в поле хоста означает "эта сеть" или "сам кабель сегмента сети" (например, 172.16.0.0).

Кроме этого, следует зарезервировать адреса для различных сетевых служб, частности, для:

- станции SNMP-управления;
- корпоративного DHCP-сервеар и WINS-сервера;
- почтового SMTP-сервера;
- DNS-сервера;
- WWW-и HTP-сервера;
- Серверов защиты информации (Syslog, TACACS+, RADIUS-серверов и др.).

2.4.3. Трансляция частных адресов в сети

Одной из проблем, возникающей в процессе проектирования корпоративных сетей, является нехватка глобальных (внешних) IP-адресов, как по причине их ограниченного количества, так и в связи с их высокой стоимостью. Решение этой проблемы состоит в использовании во внутренних сетях предприятия частных адресов и применении процедуры трансляции сетевых адресов для преобразования внутренних (частных) адресов в публичные (зарегистрированные), разрешенные к использованию в глобальной сети Ин-

тернет [12,17,23,28]. Ниже приведены частные адреса, используемые в 4-й версии протокола IP:

10.0.0.0 … 10.255.255.255 – одна сеть класса A;
172.16.0.0 … 172.31.255.255 - 16 сетей класса B;
192.168.0.0 … 192.168.255 255 – 256 сетей класса C.

Существуют статический и динамический способы трансляции адресов NAT (*Network Address Translation*). При статическом способе задается взаимно однозначное соответствие между внутренними локальными (частными) и внешними (глобальными) адресами. Очевидно, что количество зарегистрированных внешних адресов, выделенных данной организации провайдером, должно соответствовать количеству внутренних. Программный модуль, реализующий процедуру NAT функционирует на маршрутизаторе.

При динамическом способе трансляции организации выделяется один или группа (пул) зарегистрированных внешних IP-адресов. В данном способе устанавливается динамическое соответствие между внутренними локальными и внешним(и) адресом (адресами), но отображение внутренних адресов на внешние может меняться в зависимости от наличия в пуле свободного зарегистрированного адреса. В этом случае реальный IP-адрес выделяется для узла лишь на время его работы в сети.

Одним из видов реализации динамической трансляции является так называемый **перегруженный NAT** *(Overload),* который отображает несколько внутренних адресов в единственный внешний IP-адрес, используя различные порты. Его называют также **PAT** (*Port Address Translation*).При таком способе каждый компьютер в частной сети транслируется в тот же самый адрес, но с различным номером порта. Модуль NAT поддерживает таблицу, где каждому соединению с Internet ставится в соответствие внешний IP-адрес и номер порта.

При использовании NAT маршрутизатор, подсоединяющий локальную сеть к Internet, имеет два IP-адреса (рисунок 2.9). Один, внутренний (*Inside local*), со стороны LAN, который выбирается из адресного пространства, выделенного для частных сетей, и второй, внешний (*Outside local*) — со стороны Internet, предоставляемый оператором (провайдером) услуг Internet. Интерфейс, к которому подключена локальная сеть, называется внутренним интерфейсом (Inside), а к которому подключена внешняя сеть, например сеть Интернет провайдера, называется внешним (Outside). Следовательно, интерфейс на рисунке 2.12 *FastEthernet*0 (Fa0) — это *Inside* интерфейс, а последовательный интерфейс S0 — *Outside*.

После получения пакета от клиента локальной сети с запросом на соединение с компьютером внешней сети маршрутизатор, после определения пути следования и проверки пакета, сохраняет внутренний IP-адрес компьютера и номер порта в своей таблице трансляции. Затем маршрутизатор заменяет немаршрутизируемый частный IP-адрес компьютера отправителя

(например, 192.168.1.1) IP-адресом маршрутизатора (170.30.210.1), а исходный порт компьютера отправителя заменяет неким случайным номером порта (выбранным за пределами диапазона стандартных номеров портов) и сохраняет его в таблице трансляции адресов для этого отправителя. Далее модуль NAT вносит в свою таблицу запись, которая приводит в соответствие внутренний IP-адрес и номер порта компьютера ЛВС номеру порта, присвоенному в этой сессии.

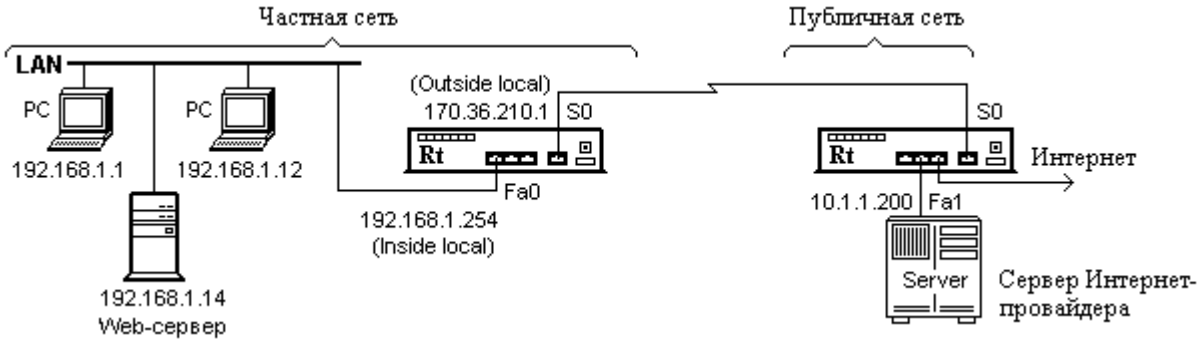


Рисунок 2.12 – Иллюстрация процедуры трансляции адресов

Генерируя новый номер порта, NAT-модуль может выбирать любое число, которого нет в NAT-таблице. В связи с тем, что поле номера порта состоит из 16 бит, протокол NAT может поддерживать более 60 000 одновременных соединений с единственным разрешенным IP-адресом маршрутизатора. Таким образом, NAT может представлять тысячи компьютеров внутренней сети только одним внешним IP-адресом.

Перед разработкой сценариев трансляции адресов администратор сети должен четко представлять себе, чего он пытается достичь с помощью процедуры NAT?

1. Разрешить доступ в Интернет внутренним пользователям?
2. Разрешить доступ из Интернета к внутренним устройствам (например, почтовому серверу или Web-серверу)?
3. Перенаправить трафик TCP на другой порт или адрес TCP?
4. Применить NAT во время сетевых переключений (например, после изменения IP-адреса сервера и до обновления всех клиентов необходимо, чтобы все необновленные клиенты могли получать доступ к серверу через исходный IP-адрес, а обновленные клиенты получали доступ к серверу через новый адрес)?
5. Использовать NAT, чтобы позволить перекрывающимся сетям связываться друг с другом?

Так, если требуется предоставить доступ в Интернет внутренним пользователям, но у администратора нет достаточного количества допустимых адресов, то можно воспользоваться одним публичным адресом или пулом публичных адресов.

3. Проектирование структурированной кабельной системы сети

3.1. Структура универсальной кабельной системы

3.1.1. Состав и назначение подсистем

Компьютерная сеть крупного предприятия структурно представляет собой совокупность рабочих станций, узлов коммутации и распределения информации, соединенных между собой линиями передачи цифровых и мультимедийных данных. Для обеспечения эффективного обмена информацией между пользователями сети, рабочими станциями и узлами коммутации и распределения, а также узлов между собой, целесообразно использовать универсальную коммуникационную среду. Такую среду образует *структурированная кабельная система* (СКС) [22,24]. СКС представляет собой универсальную телекоммуникационную инфраструктуру здания или комплекса зданий, которая предназначена для передачи сигналов всех типов, включая речевые, информационные и видеоизображения. Правила построения СКС регламентируются рядом международных и отечественных стандартов [41-44]. По рекомендациям стандарта структурированную кабельную систему следует устанавливать при количестве рабочих станций в компьютерной сети свыше 50. Структурированная кабельная система строится таким образом, чтобы каждый интерфейс (точка подключения к системе) обеспечивал доступ ко всем ресурсам сети. СКС может быть развернута не во всем здании, а на отдельном этаже (части этажа), занимаемым некоторой организацией.

Целесообразность использования структурированной кабельной системы обусловлена высоким качеством и надежностью передачи различной информации по линиям СКС, удобством эксплуатации компьютерной сети, длительным жизненным циклом. Внедрение СКС создает основу для повышения эффективности профессиональной деятельности предприятия/организации, снижения эксплуатационных расходов, улучшения взаимодействия внутри компании и качества обслуживания клиентов.

На рисунке 3.1 изображена обобщенная схема структурированной кабельной системы компьютерной сети крупной организации (предприятия). Универсальная кабельная система имеет иерархическую структуру "звезда". Фактическая топология сети определяется пространственным расположением и размерами здания или группы зданий (кампуса), занимаемых предприятием.

В состав типовой СКС входят следующие подсистемы и элементы:

- внешние магистральные кабели комплекса зданий (кампуса);

- распределительный пункт кампуса (РПК);
- внутренние магистральные (вертикальные) кабели зданий;
- распределительные пункты зданий (РПЗ);
- этажные (горизонтальные) кабели;
- распределительные пункты этажей (РПЭ);
- точки перехода (ТП), между различными типами кабелей;
- телекоммуникационные розетки (ТР).

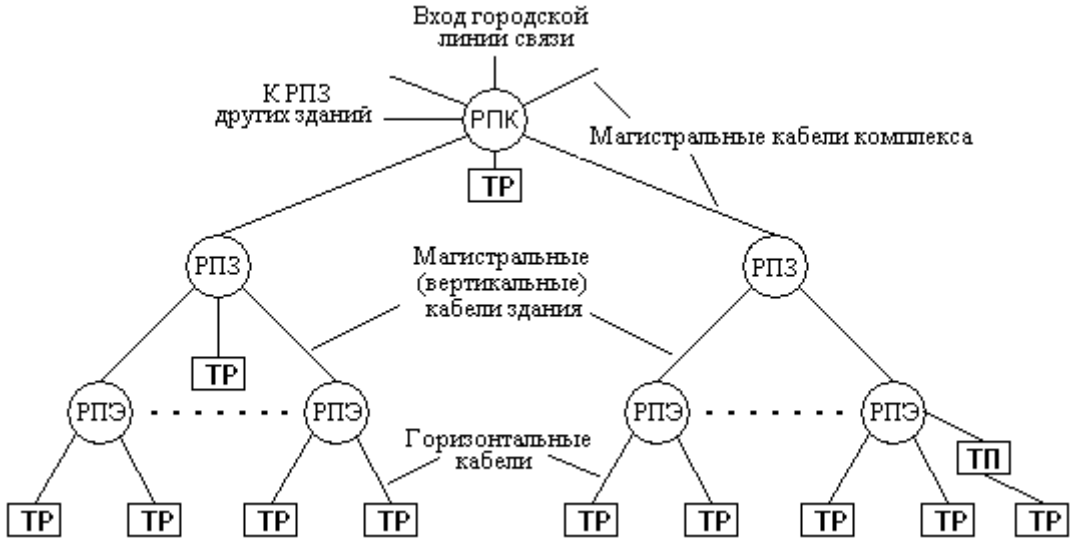


Рисунок 3.1 – Обобщенная схема структурированной кабельной системы комплекса зданий

На нижнем уровне иерархии СКС располагаются телекоммуникационные розетки ТР, к которым подсоединяются рабочие станции пользователей сети, а зачастую и индивидуальные телефонные аппараты, входящие в состав рабочего места сотрудника предприятия. Телекоммуникационные розетки рабочих мест, расположенные в помещениях одного этажа здания, соединяется соответствующими индивидуальными многопарными электрическими или оптическими кабелями с коммутационным устройством, установленным на распределительном пункте этажа РПЭ. Такие этажные соединительные кабели получили названия "горизонтальных", так как они прокладываются в горизонтальном направлении и обычно не пересекают границы этажа.

В ряде случаев на пути от ТР до РПЭ необходимо соединение однородных, с электрической точки зрения, кабелей, различающихся конструктивным исполнением, например, круглого и плоского кабелей (последний используется для прокладки под ковровым покрытием). Место соединения таких кабелей называется точкой перехода (ТП). При построении горизонтальной проводки допускается использование только одной точки перехода на весь горизонтальный тракт.

Распределительные пункты этажей соединяются группой кабелей с распределительным пунктом здания РПЗ, который, за исключением редких случаев, является единственным на все здание. Кабели, соединяющие РПЭ с распределительным пунктом здания, относят к внутримагистральным. В связи с тем, что они располагаются в пространстве обычно вертикально, их называют "вертикальными". Кабели вертикальной подсистемы фактически соединяют между собой отдельные этажи здания. Подсистема внутренних магистралей может отсутствовать в случае расположения СКС только на одном этаже.

Если предприятие занимает несколько зданий, расположенных на ограниченной территории, то для объединения их в единую сеть применяется подсистема внешних магистральных кабелей. На практике эта подсистема преимущественно строится по звездной или кольцевой топологии, центром которой выступает распределительный пункт комплекса задний (кампуса) РПЗ, являющийся главным распределительным пунктом предприятия. Очевидно, что при размещении СКС только в одном здании подсистема внешних магистралей отсутствует. В зданиях с большими размерами часто к подсистеме внешних магистралей относят кабели, имеющие протяженность свыше 500 метров, хотя фактически они и не выходят за пределы здания.

СКС в сравнении с раздельными информационными и телефонными сетями имеет ряд преимуществ:

- интегрированная кабельная система позволяет передавать сигналы данных и мультимедийных приложений;
- обеспечивает работу нескольких поколений компьютеров и сетевых устройств;
- предусматривает использование любого стандартного сетевого оборудования;
- реализует большой диапазон скоростей передачи данных от 100 Кбит/с для речевых приложений до 10 000 Мбит/с – для информационных и мультимедийных приложений;
- допускает одновременное использование нескольких разнотипных сетевых протоколов;
- обеспечивает снижение цен на стандартные конструктивные элементы и комплектующие;
- позволяет реализовать свободу перемещения пользователей в пределах всей рабочей области с сохранением доступа и персональных данных (адресов, внутренних и внешних телефонных номеров, паролей, прав доступа, классов обслуживания и т.д.);
- имеет большую надежность;
- позволяет сократить трудозатраты на обслуживание сети благодаря простоте эксплуатации и администрирования;
- упрощает администрирование сети за счет того, что все линии и интерфейсы указаны в технической документации, благодаря чему рабо-

та организация не зависит от сотрудника с монопольными знаниями соединений сети.

К недостаткам использования СКС относится то, что при ее проектировании и реализации требуется заложить избыточность количественных и качественных параметров системы, что связано с существенными единовременными затратами.

3.1.2. Фазы проектирования СКС

Процесс проектирования СКС разделяется на две основные фазы: архитектурная и телекоммуникационная [22]. Основными задачами архитектурной фазы проектирования являются определение оптимальной общей структуры СКС и адаптация отдельных помещений и конструкций здания на уровне строительных решений под специфические требования кабельной проводки, коммутационного оборудования и технических помещений СКС.

Архитектурная фаза проектирования осуществляется на этапе разработки проекта нового или реконструируемого здания. На этой фазе в строительный проект закладываются кабельные стояки, помещения кроссовых и аппаратных с соответствующими системами инженерного обеспечения их параметров, определяются трассы и способы прокладки кабелей как внутри, так и снаружи здания (кабельная канализация, воздушные линии). Основными исходными данными для данного этапа проектирования являются:

• форма, этажность, архитектурные, планировочные и другие особенности и геометрические характеристики здания или их комплекса, а также прилегающей территории;

• строительные и другие нормативные документы на проектирование служебных помещений систем телекоммуникаций и кабельных трасс;

• нормативная документация по СКС (ведомственные руководящие технические материалы и государственные стандарты);

• дополнительные требования заказчика.

Работы по сбору исходной информации и собственно проектированию на архитектурной фазе проводятся специализированными проектными организациями с учетом требований подрядчика, который будет реализовывать СКС. В некоторых ситуациях при наличии соответствующих лицензий, опыта выполнения работ и штата проектировщиков подрядчик частично или полностью берет проектные работы этой фазы на себя.

Телекоммуникационная фаза проектирования начинается по окончании архитектурной, либо после завершении капитальных строительно-монтажных работ. На данной фазе проектирования разрабатывается конкретная структура СКС, составляется перечень необходимого оборудования, планы его размещения и т.д. К проектированию на телекоммуникационной фазе привлекаются организации, специализирующиеся на создании СКС и работающие в области системной интеграции (проектирование, установка

оборудования, настройка, ремонт и обслуживание сетей). Эти же компании силами собственных сотрудников или привлеченных субподрядчиков достаточно часто выполняют также большую часть монтажных и пусконаладочных работ, которые по времени, как правило, проводятся одновременно с отделкой внутренних помещений или сразу же после ее завершения. Основными исходными данными, необходимыми для практической реализации телекоммуникационной фазы проектных работ, являются:

• результаты обследования здания и прилегающей территории или их проектная документация, выполненная на архитектурной фазе проектирования;

• нормативно-техническая документация по СКС (стандарты);

• дополнительные требования заказчика, например количество и размещение рабочих мест, количество розеточных модулей и телекоммуникационных розеток на рабочем месте, требования к пропускной способности, надежности, безопасности и т.д.

Учебное проектирование СКС ограничивается только телекоммуникационной стадией. На этой стадии выполняется выбор типов и расчет параметров и количества компонентов, необходимых для создания кабельной системы. Для этого следует разделить СКС на более мелкие составляющие, в состав которых рекомендуется [22,24,44] отнести:

1) подсистему рабочего места;
2) горизонтальную подсистему;
3) магистрали кабельной системы;
4) подсистему кабелей коммуникационного оборудования;
5) подсистему администрирования.

Результаты расчетов по каждой из подсистем целесообразно представить в табличной форме. На последующих этапах эти данные используются в качестве исходной информации для проектирования следующих подсистем. Форма таблиц выбирается разработчиком по своему усмотрению.

Какой-либо расчет электрических и оптических характеристик в подавляющем большинстве случаев не производится, так как заданный уровень параметров формируемых трактов гарантируется применяемой элементной базой, соблюдением требований стандартов и правил монтажа.

3.1.3. Требования и рекомендации по размещению распределительных пунктов

Распределительные пункты СКС образуют узлы локальной сети, на которых устанавливается коммутационное, сетевое и серверное оборудование. На них заводятся окончания горизонтальных и магистральных линий, которые для удобства использования соединяют с контактами разъемов коммутационных панелей (патч-панелей) или кроссовых панелей. Территориально

распределительные пункты этажей, зданий и комплекса размещают в специальных технических телекоммуникационных помещениях. В общем случае они делятся на аппаратные и кроссовые. *Аппаратной* называется помещение, в котором, наряду с групповым коммутационным оборудованием СКС, располагается сетевое оборудование коллективного пользования масштаба предприятия (серверные фермы, маршрутизаторы и коммутаторы). Предъявляемые к аппаратным комнатам требования несколько выше, чем к остальным телекоммуникационным помещениям, поскольку оборудование, устанавливаемое в них, является более сложным (например, УАТС или серверы). В аппаратной может находиться более одного распределительного пункта. Обычно, если телекоммуникационное помещение служит для размещения двух и более распределительных пунктов, его считают аппаратной. Аппаратные, как правило, оборудуются фальшполами, системами пожаротушения, кондиционирования и контроля доступа.

Кроссовые представляет собой помещения, в которых размещаются промежуточные распределительные пункты этажей (РПЭ). В них устанавливается коммутационное оборудование СКС, сетевое и другое вспомогательное оборудование, обслуживающее обычно ограниченную группу пользователей. При этом уровень оснащения кроссовой оборудованием инженерного обеспечения является более низким по сравнению с аппаратной.

В аппаратной размещается, как правило, распределительный пункт здания и /или распределительный пункт комплекса зданий. В кроссовых помещениях располагаются кроссовые этажей, здания или комплекса. Аппаратная может быть совмещена с кроссовой здания (КЗ). В этом случае ее сетевое оборудование может подключаться непосредственно к коммутационному оборудованию СКС. Если аппаратная расположена отдельно, то ее сетевое оборудование подсоединяется к локально расположенному коммутационному оборудованию или к обычным информационным розеткам, аналогичным розеткам рабочих мест.

Для установки в аппаратных и кроссовых помещениях коммутационных панелей, кроссов и сетевого оборудования служат напольные или настенные телекоммуникационные шкафы, либо телекоммуникационные стойки.

Распределительный пункт может занимать часть шкафа или несколько шкафов. На каждом этаже здания рекомендуется устанавливать один распределительный пункт этажа. Если офисная площадь этажа превышает 1000 квадратных метров, следует предусмотреть дополнительный РПЭ. При выборе места расположения распределительных пунктов целесообразно руководствоваться следующими принципами:

- РПЗ можно совместить с одним из РПЭ на том же самом этаже;
- РПЭ должен быть на каждом этаже здания;

- РПЭ следует располагать максимально близко к стоякам, по которым прокладываются кабели подсистемы внутренних магистралей СКС; в идеальном случае каналы стояка проходят непосредственно через него;
- для облегчения соблюдения режима контроля доступа комната, выделенная для распределительного пункта, не должна быть проходной или совмещаться с другими производственными помещениями, желательно, чтобы в ней отсутствовали окна;
- с целью минимизации длины кабелей и соответственно стоимости горизонтальной подсистемы следует располагать РПЭ как можно ближе к геометрическому центру обслуживаемой рабочей зоны.

На рисунке 3.2 показана обобщенная схема локальной компьютерной сети одного здания, построенной на основе структурированной кабельной системы.

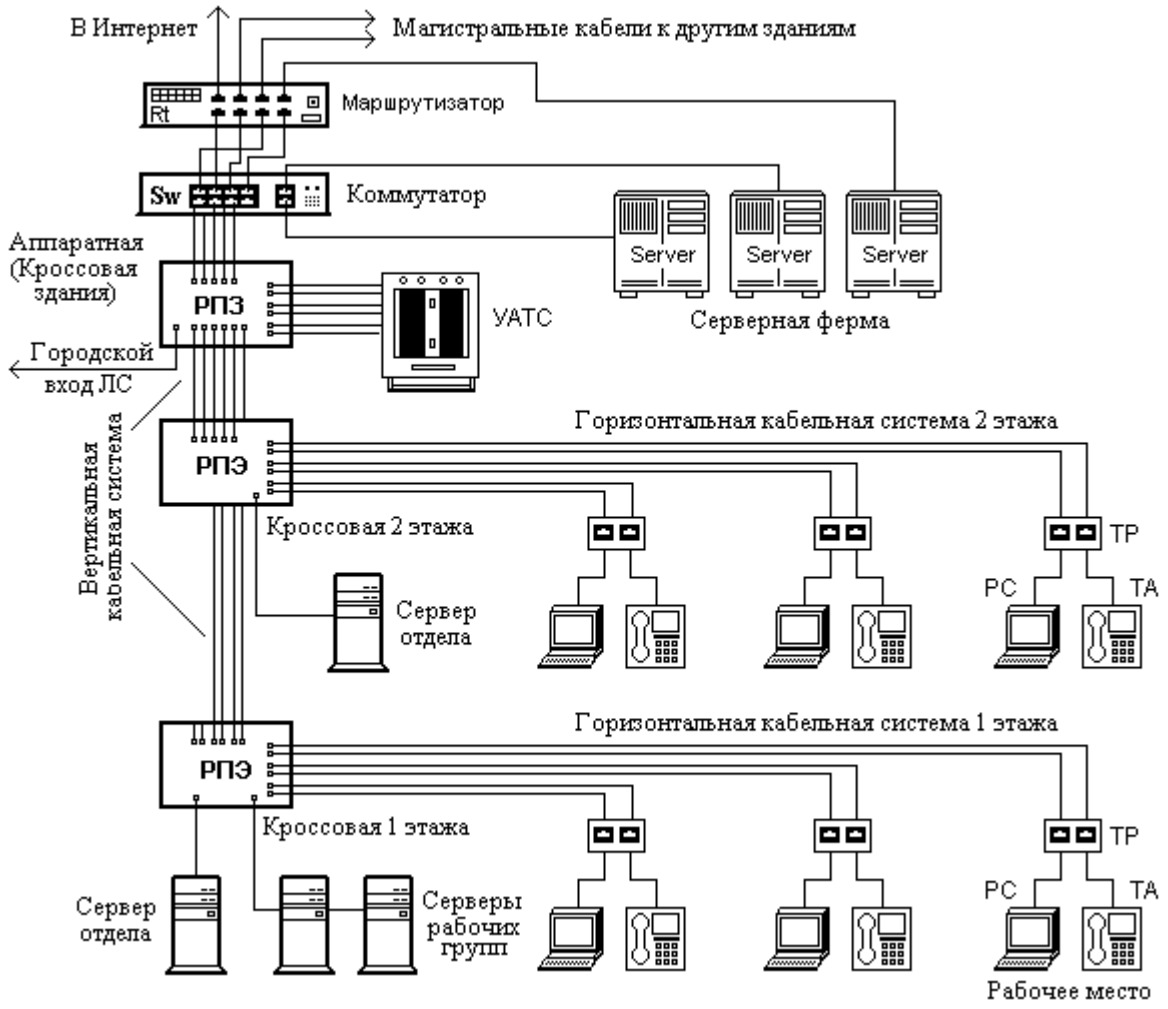


Рисунок 3.2 — Локальная компьютерная сеть предприятия на основе структурированной кабельной системы

Кабель городского ввода заводится в распределительный пункт комплекса, при наличии последнего. Если же такой пункт отсутствует, или совмещен распределительным пунктом здания главного офиса, то городской ввод осуществляется в распределительный пункт здания РПЗ. В этот пункт сходятся кабели внешних магистралей, соединяющие с ним отдельные РПЗ, а также внутренние магистральные кабели, соединяющие с распределительным пунктом здания кроссовые этажей.

В помещении кроссовой этажа устанавливается активное сетевое оборудование, которое, как правило, обслуживает только ограниченную группу пользователей (обычные и коммутирующие концентраторы рабочих групп, выносные блоки телефонных станций и т.д.). К кроссовым этажей горизонтальными кабелями подключены модули телекоммуникационных розеток рабочих мест.

3.1.4. Размещение серверов и требования к серверному помещению

Одним из важнейших моментов успешного проектирования компьютерной сети предприятия является учет особенностей функционирования серверов и их размещения в сети.

Серверы предоставляют доступ пользователям к файлам, осуществляют управление печатью, обеспечивают почтовую связь и службы приложений, таких как обработка текстов, СУБД и пр. В настоящее время каждый сервер обычно выделяется для выполнения одной функции, например, функции почтового или файлового сервера. Серверы обычно не используются в качестве рабочих станций и работают под управлением специализированных операционных систем, таких как NetWare, Windows Server, UNIX и Linux.

Серверы разделяют на две отдельные группы: **серверы предприятия** (*enterprise servers*) и **серверы рабочих групп** (*workgroup servers*). Сервер предприятия поддерживает всех пользователей сети, предоставляя им различные службы, такие как электронная почта или служба доменных имен (DNS).

Сервер рабочей группы обслуживает определенную группу пользователей и реализует такие службы, как обработка текстов, совместный доступ к файлам, работа с конкретным приложением, то есть функции, которые могут понадобиться только некоторым группам пользователей. Обычно сервер рабочей группы — это сервер с умеренной производительностью, который обслуживает до 20 пользователей. Такой сервер выполняет ряд задач малого бизнеса. Основной функцией данного сервера является хранение файлов сотрудников с разграничением доступа.

При выборе сервера для рабочей группы необходимо учитывать масштабируемость сервера, т.е. возможность его дальнейшей модернизации, в связи с возможным ростом организации, а также аппаратных требований, накладываемых производителями программного обеспечения.

В крупных компьютерных сетях предприятий и корпораций серверы часто объединяют в серверные группы (фермы), которые располагаются в специально оборудованных помещениях. Основными особенностями серверных ферм является обеспечение распределенного выполнения приложений, применение кластерных решений, вынесение дисковых подсистем из серверов во внешние защищенные стойки. На серверной ферме должны быть установлены следующие системы:

- бесперебойного питания;
- резервного копирования данных;
- антивирусной защиты;
- регистрации и сигнализации попыток внешних и внутренних атак;
- кондиционирования;
- автоматического пожаротушения;
- защиты от вредного электромагнитного излучения др.

Размещение серверов в логической структуре сети связано с расположением пользователей, имеющих к этому серверу доступ. По этой причине место подключения сервера значительно влияет на структуру потока данных в распределенной сети. Поэтому серверы рабочих групп следует размещать в промежуточных узлах коммутации, по возможности ближе к пользователям, использующим приложения этих серверов. При расположении серверов рабочих групп близко к пользователям поток данных будет проходить по каналам сети прямо к промежуточному узлу, не затрагивая других пользователей в этом сегменте. В качестве серверов рабочих групп могут быть использованы серверные компьютеры настольного типа, хотя предпочтение следует отдавать серверам стоечного исполнения.

Серверы предприятия следует размещать в специально выделенном помещении, в котором располагается главный узел коммутации. В качестве серверов необходимо выбирать специализированные компьютеры серверного исполнения, конструктивно выполненные для установки в коммуникационный шкаф. Доступ в помещение, где располагются серверы должен быть строго ограничен.

Таким образом, на начальной стадии проектирования нужно разделить файловые серверы проекта на серверы предприятия и серверы рабочих групп, а затем разместить их в сети согласно ожидаемому характеру потока данных пользователей и исполняемым функциям.

Серверная комната — помещение, занимаемое крупным телекоммуникационным и/или серверным оборудованием. Серверная комната относится к помещениям специального назначения и считается средством обслуживания здания или кампуса, предназначенными для выполнения телекоммуникационных функций.

Стандартом (ANSI/TIA-569A) сформулированы следующие основным требования к серверным помещениям [41]:

- наличие не менее одной двойной электрической розетки с заземлением на каждые 3 погонных метра любой стены серверного помещения, либо 2 планки розеток подключенных на различные фидеры для каждой коммутационной стойки;
- серверная комната должна располагаться в стороне от источников электромагнитного излучения;
- использовать для освещения серверной комнаты лампы накаливания или галогенные лампы, для снижения количества электромагнитных помех;
- устанавливать фальшпол или систему кабельнесущих лотков.
- система кондиционирования должна обеспечивать поддержку температуры в диапазоне от 18 до 24 ^{0}C и относительную влажность от 30 до 50 %;
- минимальный допустимый размер серверной комнаты — 12 м^2;
- серверная комната должна быть соединена с главным электродом системы заземления здания кондуитом (металлической трубой) калибром 1,5 дюйма (диаметр 41 мм);
- требуемая минимальная высота потолка серверной комнаты должна составлять не менее 2,5 м.

3.1.5. Расположение телекоммуникационных розеток

Часть помещения, где пользователи работают с терминальным (телекоммуникационным, информационным, речевым) оборудованием относят к рабочей области. Эта область не относится к горизонтальной подсистеме СКС. Функциональным элементом горизонтальной подсистемы СКС является телекоммуникационный разъем (ТР). Рабочие места оснащаются розеточными модулями, включающими два или более телекоммуникационных разъема (розетки). Подключение оборудования рабочей области выполняют абонентскими кабелями. Абонентские (сетевые) кабели находятся за рамками СКС, однако они позволяют создавать каналы, параметры которых определяются стандартами СКС. К СКС относят коммутационные кабели (перемычки), используемые для соединений между портами панелей либо контактами кроссов.

Телекоммуникационные разъемы конструктивно располагаются в розеточном модуле, по два ТР в модуле. Розеточные модули разрешается располагать на стене, полу или в другой точке рабочей области помещения. При этом следует обеспечить удобство доступа ко всем разъемам. Следует принимать во внимание, что высокая плотность ТР повышает гибкость системы и облегчает изменения телекоммуникационных ресурсов рабочих мест. Рекомендуется устанавливать два телекоммуникационных разъема на каждые 5 м^2 используемой площади [22,24,42]. Допускается установка разъемов одиночно или группами, однако каждое рабочее место должно иметь не менее

двух разъемов. На каждом рабочем месте необходимо предусмотреть, по крайней мере, одну телекоммуникационную розетку, установленную на симметричном кабеле 100 Ом или 120 Ом (предпочтение отдается кабелям 100 Ом). К другой розетке можно подключать симметричный, либо оптоволоконный кабель.

Согласно указаниям стандарта высота установки телекоммуникационной розетки, определяемая как расстояние от основного пола до центра лицевой пластины, должна составлять от 375 мм до 1220 мм. Телекоммуникационные розетки должны размещаться на одной высоте с силовыми, причем расстояние между силовыми и информационными розетками не должно превышать 1 м (рисунок 3.3).

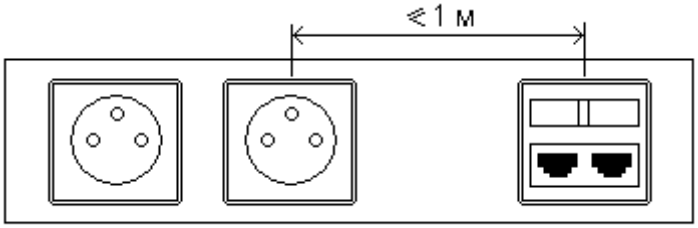


Рисунок 3.3 — Допустимое расстояние между силовой и телекоммуникационной розетками

На практике находят применение следующие основные разновидности установки телекоммуникационных розеток в рабочих помещениях пользователей:

- с использованием декоративных коробов;
- с использованием настенного корпуса;
- по скрытой схеме в толще стены;
- в подпольных лючках и коробках;
- с использованием посадочных мест специализированной мебели.

3.2. Выбор и расчет кабелей для реализации СКС

3.2.1. Классы информационных приложений и категории кабелей

В соответствии с международными стандартом ISO/IEC 11801 [42] все виды приложений, которые могут обмениваться данными по витым медным парам, подразделяет на 7 классов: A, B, C, D, E, F G (таблица 3.1). Класс A относится к низшему, а класс — G к высшему виду приложений. Для приложений каждого класса определяется соответствующий класс линии связи, который задает предельные электрические частотные характеристики линии, необходимые для нормальной работы приложений соответствующего и более низкого класса.

Кабели улучшенной категории 5 (категория 5+, или категория 5e) с верхней граничной частотой нормировки параметров до 100 МГц. Категория 5e нормирует ряд параметров, соблюдение которых обеспечивает возможность работы сверхвысокоскоростного приложения *Gigabit Ethernet*.

Приложения класса E и компоненты СКС категории 6 имеют нормируемые характеристики до частоты 250 МГц. Выбор именно такого частотного диапазона гарантируемых параметров был обусловлен требованием обеспечения поддержки функционирования дуплексных *Gigabit Ethernet.* Класс F и компоненты категории 7 рассчитаны на частоты до 600 МГц. Выбор последнего значения в первую очередь обусловлен широким распространением аппаратуры ATM со скоростью передачи 622 Мбит/с, а также необходимостью поддержки передачи сигналов многоканального аналогового телевидения с верхней граничной частотой 550 МГц.

Таблица 3.1

Классы приложений и категории проводных кабельных линий

Класс приложений	**Скорость передачи данных / максимальная частота спектра сигнала**	**Категория кабеля**
A	Низкая или речевые сообщения / 100 кГц	–
B	Средняя / 1 МГц	–
C	Высокая / 16 МГц	3
D	Очень высокая / 100 МГц	5; 5e
E	Очень высокая / 250 МГц	6
F	Сверхвысокая / 600 МГц	7
G	Сверхвысокая / 1200 МГц	8

Для построения трактов категории 6 используются кабели всех типов (экранированные и неэкранированные). В качестве соединителя применяется в основном модульный разъем. Линии категории 7 при современном состоянии уровня техники могут быть реализованы только на кабеле с экранированными парами [22,24].

Следует отметить, что кабели и разъемы различных категорий могут быть установлены в пределах подсистемы и/или кабельной линии, но передающие рабочие характеристики тракта будут определяться категорией худшего элемента.

Для оптоволоконных кабелей стандартом нормируются общее затухание линии связи. Максимальное затухание не должно превышать значений, указанных в таблице 3.2 для выделенных оптических окон (длин волн). Кроме этого затухание в оптических линиях, объединяющих несколько подсистем (например, горизонтальную и магистральную), не должно превышать 11 дБ для оптического волокна 62,5/1125 мкм и 8/125 мкм для номинальных рабочих волновых диапазонов. Значения затуханий, приведенные в таблице 2.2, установлены для оптоволоконных линий в каждой подсистеме для

наихудших условий монтажа разъемов с помощью сплайсов (механических соединителей) на каждом конце каждой подсистемы.

Таблица 3.2

Допустимые затухания в оптоволоконных подсистемах

Подсистема	**Длина линии, м**	**Затухание, дБ**			
		Одномодовый		**Многомодовый**	
		1310 нм	1550 нм	850 нм	1300 нм
Горизонтальная	100	2.2	2.2	2.5	2.2
Магистраль здания	500	2.7	2.7	3.9	2.6
Магистраль комплекса	1500	3.6	3.6	7.4	3.6

При наличии коротких оптоволоконных линий следует учесть возможность перегрузки приемника мощным сигналом и предусмотреть возможность снижения уровня излучаемого сигнала в передатчике.

3.2.2. Выбор типов кабелей

Одним из важнейших требований, предъявляемых к структурированной кабельной системе (СКС), является ее надежность. Надежность СКС в свою очередь определяется составляющими компонентами сети, к которым относятся: кабель связи, разъемы и устройства сопряжения, коммутационные панели. Для повышения надежности СКС необходимо принять следующие меры:

- вертикальную разводку желательно выполнять оптоволоконным кабелем, который является нечувствительным к электромагнитным помехам, а также обеспечивает гальваническую развязку СКС;
- кабели следует прокладывать в лотках и на подвесах, за фальшпотолком и в кабельных каналах (коробах) — т.е. в труднодоступных для пользователей и сторонних лиц местах;
- для ввода кабелей в коммуникационные шкафы или проводки их через потолочные перекрытия следует использовать жесткий или гибкий металлический или неметаллический канал круглого сечения (трубу), называемый кондуит (*Conduit)*;
- подключение компьютеров и другого оборудования осуществлять сменными легко заменяемыми коммутационными шнурами (патч-кордами).

В локальных компьютерных сетях используются как проводные неэкранированные UTP- и экранированные STP-кабели, так и оптоволоконные. Для горизонтальной кабельной системы разрешается применять кабель

STP с двумя витыми парами и волновым сопротивлением 150 Ом. Для кабеля UTP стандарт требует прокладки кабеля с четырьмя витыми парами и волновым сопротивлением 100 Ом.

При применении оптоволоконного кабеля стандартом регламентируется использования кабеля с диаметром сердцевины 62,5/125 мкм с двумя многомодовыми световодами.

Стандарт EIA/TIA-568B определяет, что в телекоммуникационной панели (патч-панели) горизонтальной кабельной системы для создания соединения с кабелем UTP категории 5 должен использоваться 8-контактный гнездовой разъем типа RJ-45, имеющий прорези с цветовым кодированием. Для создания электрического соединения проводники запрессовываются в эти прорези.

В таблице 3.3 представлена степень применимости оптического кабеля с волокном диаметром 62,5/125 мкм и 50/125 мкм соответственно. Из таблицы видно, что оба типа волокна (62,5 и 50 мкм) могут быть использованы во всех подсистемах кабельной проводки: горизонтальной, вертикальной и между зданиями в территориальных сетях со скоростью передачи данных до 155 Мбит/с, как с коротковолновыми, так и длинноволновыми источниками света.

Таблица 3.3

Степень применимости оптоволоконного кабеля

Тип волокна	**Скорость передачи Мбит/с**	**Протяженность линии (длина волны 850 нм)**			**Протяженность линии (длина волны 1300 нм)**		
		Горизонтальная проводка (< 100 м)	Магистральная проводка (< 300 м)	Проводка между зданиями (≥ 300 м)	Горизонтальная проводка (< 100 м)	Магистральная проводка (< 300 м)	Проводка между зданиями (≥ 300 м)
Волокно диаметром 62,5 мкм	≤ 155	Да	Да	Да	Да	Да	Да
	≤ 1000	Да	Нет		Да	Да	Нет
	≤ 10000	Нет			Нет		
Волокно диаметром 50 мкм	≤ 155	Да	Да	Да	Да	Да	Да
	≤ 1000	Да	Да	Нет	Да	Да	Нет
	≤ 10000	Нет			Нет		
Одномодовое волокно	≤ 155	Нет			Нет	Не рекомендуется	
	≤ 1000	Нет			Нет	Да	Да
	≤ 10000	Нет			Нет	Да	Да

Однако при выборе типа оптического кабеля следует учитывать, что излучатели оптических сигналов с длиной волны 1300 нм и используемые с ними в комплекте электронные компоненты намного дороже, чем для сигналов с длиной волны 850 нм. Многомодовый кабель с диаметром волокна 62,5 мкм может также использоваться и в приложениях, в которых требуются гигабитные скорости, но в этом случае он применим с некоторыми ограничениями. Такой кабель применим как в горизонтальной, так и в вертикальной проводке однако в вертикальной проводке его разрешается устанавливать лишь в случае использования источников с длиной волны 1300 нм.

3.2.3. Ограничения длин коммуникационных кабелей

Обобщенная кабельная система компьютерной сети состоит из трех кабельных подсистем (рисунок 3.4):

- магистральной подсистемы территории (комплекса);
- магистральной подсистемы здания;
- горизонтальной подсистемы этажа.

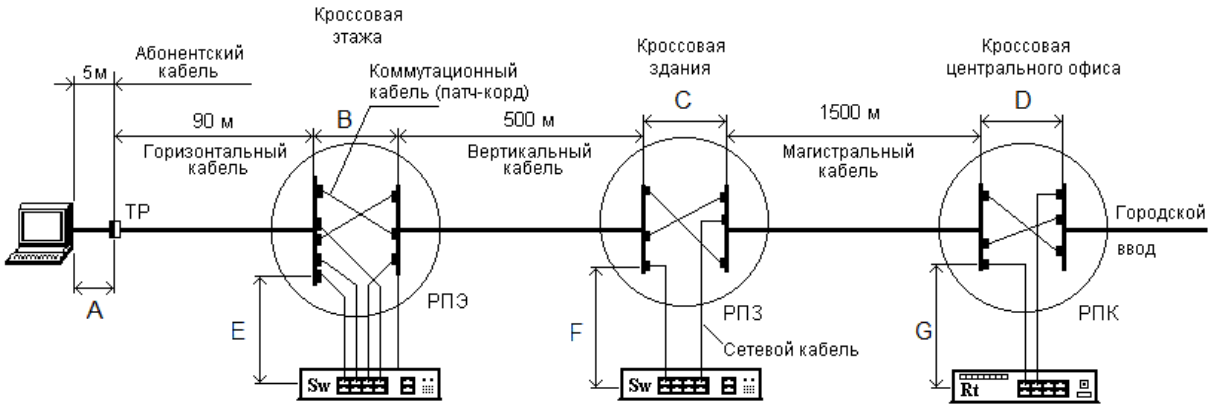


Рисунок 3.4 – Максимальные размеры участков структурированной кабельной системы

Магистральная кабельная подсистема комплекса прокладывается от главного распределительного пункта (РП) комплекса до распределительных пунктов здания, обычно расположенных в разных зданиях. Подсистема состоит из: магистральных кабелей (МК) территории, механического окончания кабелей (в главном распределительном пункте и в распределительных пунктах этажа), кроссовых соединений в главном распределительном пункте. Кабели подсистемы могут соединять распределительные пункты здания между собой.

Магистральная (вертикальная) кабельная подсистема здания простирается от распределительного пункта здания до этажных распределительных пунктов (РПЭ). Подсистема состоит из магистральных кабелей здания, механического окончания кабелей (в распределительном пункте здания и в распределительных пунктах этажей), кроссовых соединений в распределительном пункте здания. Кабели подсистемы не должны иметь точек перехода, а медные кабели выполняются без сращивания.

Горизонтальная кабельная подсистема простирается от распределительного пункта этажа до телекоммуникационных разъемов на рабочих местах. Она включает горизонтальные кабели, механическое окончание кабелей (разъемы) в РПЭ, коммутационные соединения в РП этажа и

телекоммуникационные разъемы. Все пары и волокна телекоммуникационного разъема должны быть подключены к его контактам.

Стандартами ISO/IEC и TIA/EIA [41] устанавливаются ограничения на максимальные длины кабелей и соединительных шнуров горизонтальной и магистральных подсистем. На рисунке 3.4 изображена схема ветви структурированной кабельной системы с допустимыми размерами отрезков кабелей на отдельных ее участках.

Общая длина абонентских (A), коммутационных (B) и сетевых кабелей (E), образующих канал горизонтальной подсистемы не должна превышать 10 метров, а длина коммутационных кабелей в РП здания (C) и РП комплекса (D) — не более 20 метров. Длина сетевых кабелей в РП здания (F) и РП комплекса (G) — не более 30 метров. Соблюдение указанных длин строго рекомендуется, однако не является требованием, поскольку абонентские и сетевые кабели находятся за рамками международного, европейского и американского стандартов.

Наибольшая длина кабеля горизонтальной подсистемы установлена равной 90 м. Стандартизация именно этого значения произведена исходя из возможностей витой пары как направляющей системы электромагнитных колебаний передавать сигналы наиболее массовых (на момент принятия стандартов) высокоскоростных приложений типа Fast Ethernet.

Максимальная длина кабеля подсистемы внутренних магистралей по рекомендации ISO/IEC 11801международной организации по стандартом ISO/IEC ограничена величиной 500 м. Этим же стандартом установлено, что подсистема внешних магистралей, которая объединяет отдельные здания, может включать в себя кабели максимальной длиной 1,5 км. Дополнительно оговаривается, что максимальная длина магистральных кабелей между кроссовой этажа и кроссовой внешних магистралей не может превышать 2000 м (500 м кабеля внутренней и 1500 м кабеля внешней магистрали) при условии применения коммутационных и оконечных шнуров стандартной длины. В случае использования одномодового оптического кабеля указанное значение может быть увеличено до 3000 м при длине кабеля внешней магистрали 2500 метров.

При проектировании и монтаже СКС следует избегать соединения в одном тракте компонентов с различным волновым сопротивлением. Также не разрешается соединять в пределах одной кабельной линии оптические волокна с различными диаметрами сердцевины. В случае необходимости соединения разнородных линий следует применять медиаконверторы.

3.2.4. Определение величины расхода кабеля

При расчете длины горизонтального кабеля учитываются следующие положения. Каждый телекоммуникационный разъем (TP) связывается с коммутационным оборудованием в кроссовой этажа одним кабелем. Кабели

прокладываются по кабельным каналам в обязательном порядке прямолинейно или с углом поворота не более 90°. Трасса рассматривается как пространственный объект, то есть при ее анализе в обязательном порядке принимаются во внимание спуски, подъемы, переходы на разные уровни и т.д. каналов для прокладки кабеля. Некоторое увеличение фактической величины расхода за счет неровностей укладки, невозможности полного использования кабеля из стандартных упаковок и необходимости выполнения процедур подключения кабеля к телекоммуникационным разъемам учитывается введением определенных поправочных коэффициентов.

Требуемое количество кабеля рассчитывается с использованием эмпирического метода [22], основанного на предположении, что рабочие места распределены по обслуживаемой площади равномерно. Средняя длина ($L_{ср}$) кабельных трасс вычисляется по формуле:

$$L_{ср} = (L_{max}+L_{min})/2, \quad (3.1)$$

где L_{min} и L_{max} – соответственно длины кабельной трассы от точки размещения кроссового оборудования до телекоммуникационного разъема самого близкого и самого далекого рабочего места, посчитанные с учетом технологии прокладки кабеля, всех спусков, подъемов, поворотов и особенностей здания. Величины L_{min} и L_{max} рассчитываются путем построения профилей кабельных трасс по плану здания и помещений, в которых размещается организация.

В процессе определении длины трасс необходимо добавить технологический запас величиной 10% от $L_{ср}$ и запас X для процедур разводки кабеля в распределительном узле и телекоммуникационном разъеме. С учетом сделанных дополнений формула нахождения общей длины кабельных трасс L принимает вид:

$$L= (1{,}1L_{ср}+X)\, N_{р}\,, \quad (3.2)$$

где $N_{р}$ – количество розеток на этаже.

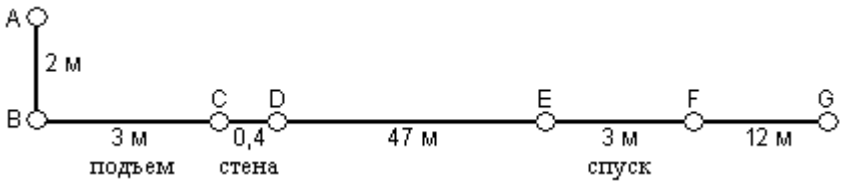


Рисунок 3.5– Кабельная трасса горизонтальной подсистемы

При расчете длины кабеля рекомендуется начертить трассу прохождения кабеля от телекоммуникационного разъема (точка A) до розетки пачпанели коммуникационного шкафа (точка G) с учетом подъемов и спусков, толщин стен и перекрытий. Пример такого чертежа показан на рисунке 3.5.

3.2.5. Расчет габаритных размеров декоративного кабельного короба

Существует два способа прокладки кабелей — скрытый и открытый. Для скрытой прокладки используют конструкцию стен, полов, потолков: кабельные каналы в полах и стенах, фальшполы и подвесные потолки. С целью защиты кабеля при прохождении его через стену или потолочное перекрытие применяется металлическая труба — **кондуит.** Процесс изготовления кабельных каналов для скрытой проводки является достаточно трудоемким и используется преимущественно в строящихся зданиях.

При открытой прокладке кабельных пучков применяются проволочные сетчатые лотки, пластиковые короба и желоба. Выбор способа прокладки зачастую осуществляется по рекомендации Заказчика. На практике наиболее распространенным вариантом реализации кабельных каналов являются пластиковые короба. Если прокладка кабеля выполняется в декоративных коробах, то необходимо определить его габаритные размеры и общее количество. При расчетах диаметр горизонтального кабеля категории 5е принимается равным 5,2 мм, что соответствует площади поперечного сечения кабеля $S_{каб}$=21,2 мм^2.

Коэффициент использования площади принимается равным k_i = 0,5, а коэффициент заполнения — средним по стандарту TIA/ EIA-569-A и равным k_z = 0,45. При такой степени заполнения существенно упрощается эксплуатация кабельной системы и становится возможной при необходимости установка дополнительных ТР с прокладкой новых кабелей в существующих декоративных коробах. В случае острой необходимости иногда допускается увеличение этого параметра, но не выше максимального значения, установленного стандартом. В случае необходимости укладки в коробе и силового кабеля, следует выбирать многосекционный (минимум двухсекционные) короб. При этом также необходимо просчитать требуемые габариты секции короба для такого кабеля.

Таким образом, требуемое сечение короба определяется по формуле [22]

$$S_{крб} = (\sum S_{jкаб}) / (k_i k_z). \qquad (3.3)$$

После определения суммарного сечения кабелей выбирается стандартный тип короба с сечением, не меньше рассчитанного. На практике наиболее широко используются секции короба стандартной длины 2 м и сечением 40×16 мм, 60×16 мм и 75×20 мм, которые позволяют выполнять монтаж корпусов информационных и силовых розеток рядом с коробом на поверхности стены.

При монтаже кабельного канализационного оборудования, кроме собственно короба, требуется еще ряд вспомогательных элементов: соединители, заглушки, уголки. Для уменьшения затрат на рутинную работу по расчету потребного количества короба и вспомогательных элементов также целе-

сообразно воспользоваться услугами одной их бесплатных специализированных автоматизированных систем проектирования локальных вычислительных сетей, например *Netwizard*.

3.3. Выбор коммуникационного и кроссового оборудования

3.3.1. Кроссовое оборудование

Кроссовое оборудование служит для долговременного соединения (кроссирования) пар медных проводов, в частности, для перехода с многопарного кабеля на обычный горизонтальный четырехпарный кабель. Кроссовое оборудование сохраняет целостность кабельной системы, а при монтаже обеспечивает возможность ручного перекоммутирования пар.

Кроме этого, кроссовое оборудование позволяет**:**

- оберегать порты СКС от скачков напряжений;
- проводить раздельно диагностику портов СКС и линии абонентской нагрузки;
- быстро производить перекроссировку (переключение) одной пары (порта, линии).

Самым распространенным, простым и дешевым представителем кроссового оборудования является **кросс 66-го типа** (гребенка). Название "гребенка" он получил за расположение контактов в виде гребешка. Гребенка позволяет коммутировать между собой 50 пар. Такой кросс не самый удобный в работе при подключении (зарядке) пар, но если надо кроссировать расположенные друг против друга пары, то гребенка наиболее подходящее решение. Соединение кроссируемых пар производится путем установки двух перемычек. Более прогрессивным и распространенным является к**росс 110-го типа**. В таком кроссе изоляция проводника пары прорезается изолированным и спрятанным в пластмассу контактом (рисунок 3.6).

Врезной контакт (из-за ограниченного доступа кислорода к месту контакта), не окисляется, не подвержен воздействиям, вызванным перепадом температур. Более того, часто в месте врезки происходит процесс диффузии — медь проводника и материал коннектора проникают друг в друга, увеличивая площадь контакта. Поэтому с годами электрические параметры таких соединений даже улучшаются. Эта технология нашла большое применение и получила несколько различных направлений. На сегодня, врезной контакт через изоляцию практически полностью вытеснил другие способы создания неразъемных соединений.

Группа контактов кросса изготавливается в виде отдельного блока, в котором врезные контакты являются составной частью разъемов — коннекторов 110. Эти коннекторы служат для оконцовки кабеля и дают возможность соединять его посредством коммутационных шнуров с другими кабелями или

с портами коммутационных устройств, снабженных соответствующими разъемами.

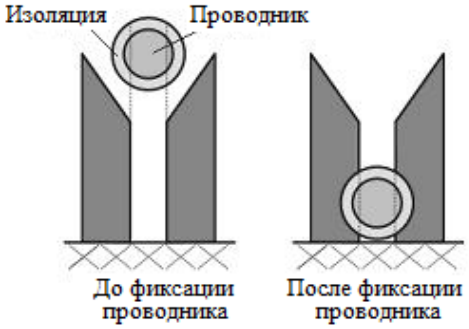


Рисунок 3.6 — Врезной контакт 110-го кросса

Коннекторы 110 располагаются совместно на одной несущей раме (плинте), на которой может быть находиться до 50 пар контактов. Очень часто с помощью таких плинтов разделывают стандартные 25-парные кабели, которые соединяют межэтажные сегменты сети. Кроссирование кабельных пар осуществляется с помощью коммутационных шнуров (пач-кордов), состоящих из одной, двух или четырех пар проводов, оконцованных с двух сторон коммутационными вилками 110. С помощью вилки 110 происходит соединение коммутационных шнуров с соответствующими розетками коннекторов 110.

Основное достоинство кросса 110 — высокая плотность соединений, но, а основной недостаток — ограниченное использование из-за отсутствия в нем защиты от перенапряжений. Но это не относится ко всем кроссам, использующих 110-й тип контактов. При необходимости кроссирования большого количества пар кабелей применяются несколько соединительных блоков, которые образуют кроссовую башню, помещаемую в кроссовый шкаф.

Для упорядочивания укладки избытка длины коммутационных шнуров в кроссовых шкафах применяются организаторы кабеля. Применение данных устройств позволяет избежать путаницы и образования петель, а также обеспечивает хорошую видимость маркировочных полос. Организаторы дополнительно предохраняют коммутационные шнуры от провисания под собственной тяжестью, что грозит ухудшением качества контактов в разъеме. Для построения кабельных линий категории 5е применение организаторов кабеля является обязательным условием.

3.3.2. Коммутационные панели

Коммутационная панель (***Patch panel***) предназначена для подключения и закрепления системных окончаний (розеток) электропроводных кабелей, обеспечивающая их коммутацию и подключение сетевого оборудования.

Патч-панель является эффективным средством администрирования для облегчения внесения изменений в конфигурацию сети.

Коммутационные панели обычно применяются в горизонтальной подсистеме СКС для подключения коммуникационного оборудования к симметричным медным кабелям связи. На лицевой стороне коммутационной панели устанавливаются розетки 8-контактных модульных разъемов для подключения коммутационных шнуров (**патч-кордов**). Для подсоединения магистральных или горизонтальных кабелей используются соединители на основе врезных контактов, расположенных на задней стороне панелей.

Коммутационная панель (рисунок 3.7) состоит из коммутационного блока, маркировочных полос и элементов крепления [8].

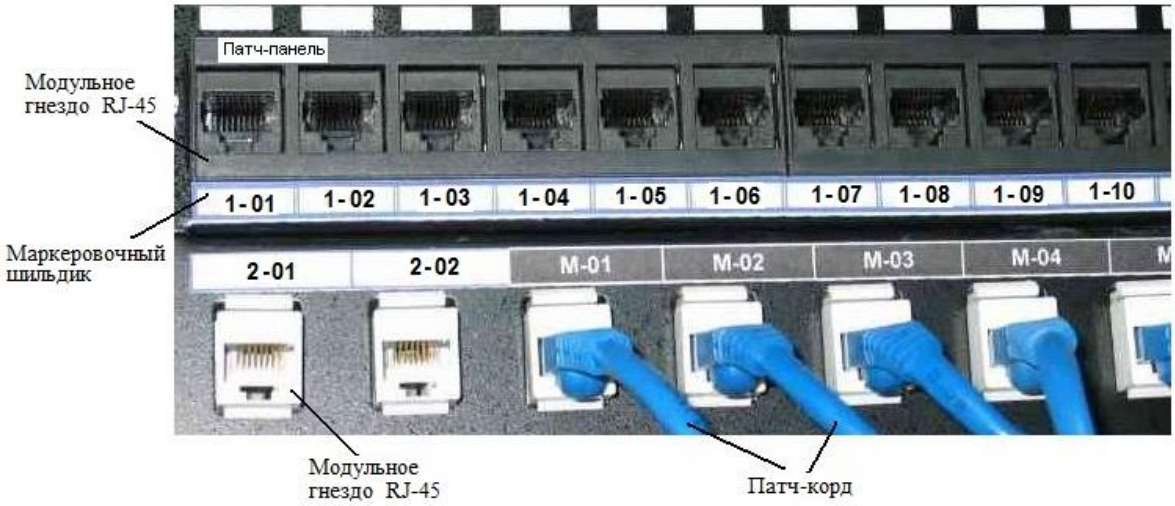


Рисунок 3.7 — Вид коммутационного блока

Базовым конструктивным элементом коммутационной панели является коммутационный блок. Он состоит из металлического основания и установленных на нем в один или несколько рядов розеток модульных разъемов типа **8P8C** (RJ-45) категории 5e. Коммутационные блоки делятся на неразборные и разборные. Неразборные блоки имеют модульные розетки, установленные в заводских условиях. Передача сигналов от ножевых контактов к информационным розеткам осуществляется по проводникам печатной платы. Разборные или розеточные блоки позволяют монтировать на них розеточные модули непосредственно на объекте монтажа. Панели разборного типа дают возможность устанавливать в них столько розеток, сколько необходимо в данный конкретный момент. Однако они уступают панелям с неразборными блоками по эстетическим показателям. С точки зрения обеспечиваемой плотности портов оба решения являются эквивалентными. Элементы крепления панели предназначены для ее монтажа на стене или в 19-дюймовых (шириной 600 мм) монтажных конструктивах — телекоммуникационных шкафах. Для коммутации оптических линий применяются оптиче-

ские кроссы, служащие для концевой заделки оптических кабелей и обеспечения коммутации магистрального кабеля с оконечным оборудованием. Оптический кросс представляет собой соединительную коробку для коммутации оптических волокон. Применяется несколько основных конструктивных исполнений оптического кроссового оборудования: блочное, шкафное и стоечное. Кроссы блочного и стоечного типа используются в основном для концевой заделки оптического кабеля большой емкости на объектах связи.

Стоечное исполнение оптического кроссового оборудования представляет собой комплект блоков, устанавливаемых в 19-дюймовый стандартный каркас стойки. Каждый блок обеспечивает концевую заделку кабеля, состоящего из 12...96 волокон.

Для создания соединений между панелями применяются специальные коммутационные кабели — **патч-корды**. Эти кабели имеют два важнейших признака — многожильные проводники и штекерные разъемы на концах. В соответствии с требованием стандартов, медные проводники каждой пары не являются цельным проводом, как в линейных сетевых кабелях, а имеют семь жил, скрученных в виде троса. Такая конструкция кабеля повышает его гибкость, что предотвращает нарушение целостности жил при многократном изгибании кабеля, которое сопровождается при переключениях на коммутационных панелях. Оптические соединительные шнуры (патч-корды) представляют собой отрезок оптического кабеля, с обеих сторон оконцованный оптическими коннекторами.

3.3.3. Телекоммуникационные шкафы

Телекоммуникационный шкаф по определению стандарта ANSI/TIA/EIA-569-A — многоэтажное устройство, предназначенное для размещения телекоммуникационного оборудования, кроссов, коммутационных панелей и точек терминирования, т.е. подключения разъемов кабельных линий [41]. Шкаф является точкой перехода между магистральной и горизонтальной подсистемами. Конструктивно телекоммуникационные шкафы изготовливаются в напольном или настенном вариантах, либо в виде стоек.

Напольные шкафы позволяют размещать окончания сотен линий, различное серверное и коммуникационное оборудование, блоки учрежденческой автоматической телефонной станции (УАТС). Телекоммуникационные стойки обладают вместимостью шкафов, но конструктивно проще (отсутствуют дверки), в связи с чем имеют меньшую стоимость. Их используют в ситуациях, не требующих особых условий эксплуатации или дополнительной защиты оборудования локальной сети от проникновения посторонних лиц.

Настенные шкафы применяются при небольшом числе линий связи, либо при отсутствии телекоммуникационного помещения. Телекоммуника-

ционные шкафы имеют стандартную 19-дюймовую (19′) ширину рабочего пространства (рисунок 3.8).

Величина 19 дюймов (482,5 мм) выбрана по той причине, что такую ширину имеют стандартные корпуса электронных приборов, которые должны входить в проем передней стенки шкафа. Коммутаторы, маршрутизаторы и пассивные элементы коммутационного оборудования, предназначенные для установки в телекоммуникационные шкафы, имеют ширину 19 дюймов, а их высота кратна условной дюймовой единице 1U. Единица 1Unit = 1¾ дюйма = 44,45 мм. Поэтому высоту телекоммуникационных шкафов обозначают в условных дюймовых единицах **U** или **RU** (*Rack Unit*).

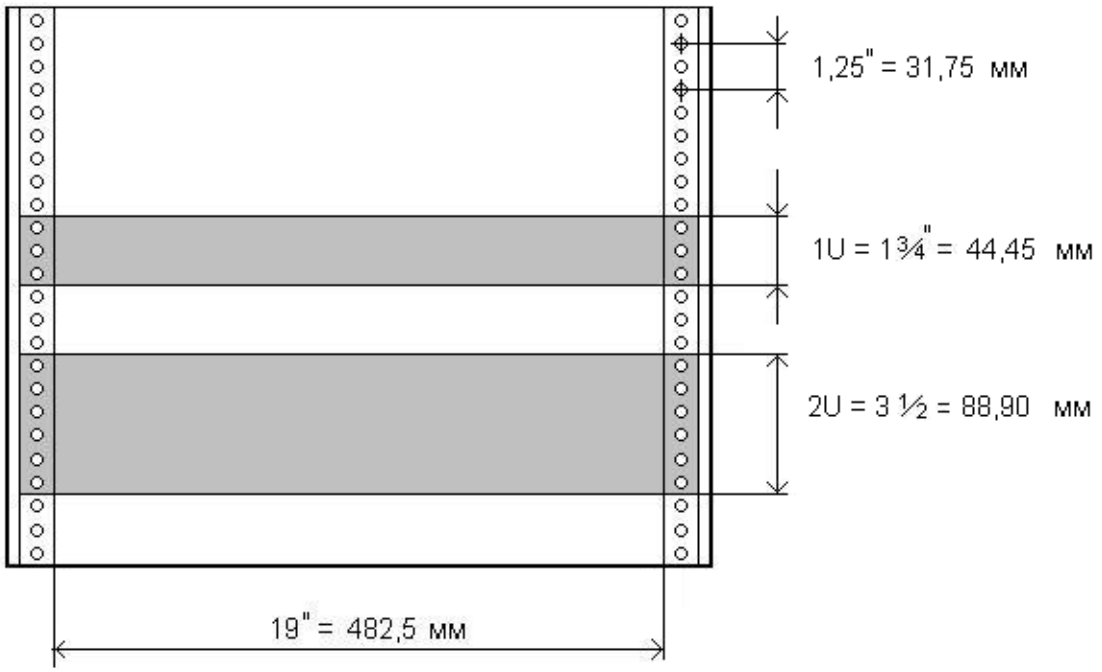


Рисунок 3.8 – Установочные размеры телекоммуникационного шкафа (вид спереди)

Промышленность выпускает широкий спектр телекоммуникационных шкафов различных типоразмеров, удовлетворяющие любые потребности. Наиболее часто используются 19" шкафы высотой 21U (1140 мм), 41U (2030 мм). Типовая глубина (Г) таких шкафов 600, 800 или 900 мм, ширина 600 или 800 мм.

3.4. Разработка физической структуры сети

3.4.1. Общие требования к схеме физической структуры сети

Физическая структура компьютерной сети предприятия отображает реальное расположение элементов сети и связи между ними. Она представляет собой полную электрическую схему с указанием всех пассивных и ак-

тивных компонентов сети, мест расположения их в пространстве с точным указанием координат размещения, всех линий связи, их типов и мест подключения, включая линии электропитания.

По причине громоздкости схемы сети ее рекомендуется выполнять в виде нескольких документов. В минимальный перечень таких документов курсового проекта входит схема структурированной кабельной системы (СКС), схема размещения коммуникационного оборудования и таблица кабельных соединений.

В процессе выполнения этого раздела проекта следует разработать поэтажные чертежи размещения СКС, составить спецификации кабелей и другого пассивного коммуникационного оборудования, схему размещения коммуникационного оборудования, а также таблицы соединений телекоммуникационных розеток с коммутационным оборудованием распределительных пунктов этажей (РПЭ) и РПЭ с распределительным пунктом здания (РПЗ). Количество схем и других документов определяется техническим заданием на проектирования и руководителем проекта. На этих чережах должны быть указаны места размещения распределительных пунктов этажей и здания, кроссовых и серверных помещений, телекоммуникационных шкафов, внутренних и городских кабельных вводов, телекоммуникационных розеток, трасс кабелей, места прохождения их через стены и потолочные перекрытия.

В спецификации кабелей и другого пассивного коммутационного оборудования должны содержаться сведения о типе, количестве и длине кабелей для горизонтальной и вертикальной систем, типе, количестве и длине кабелей для соединения РПЭ и РПЗ. При этом следует предусмотреть наличие запасных пар или кабелей для увеличения пропускной способности между монтажными шкафами. Кроме того, в спецификацию вносятся сведения о типах электрических и оптических соединителей, размерах кабельных коробов, держателей кабеля, крепежных деталях и других вспомогательных элементах.

Таблицы соединений должны содержать наименование (идентификаторы) кабелей, исходную и конечную точку кабеля, номер кросс-соединения (номер пары / номер порта), тип кабеля и его состояние (используется / не используется). С целью упрощения процедуры администрирования кабельной системы целесообразно также указывать промежуточные устройства, через которые проходит кабель (идентификатор кондуита, кабельной муфты и др.). При разработке чертежа соединений рекомендуется руководствоваться указаниями стандартов ГОСТ 2.702-69 и ГОСТ 21.614-88.

Расположение условных графических обозначений элементов на чертеже должно, как правило, давать примерное представление об их действительном расположении. Провода и кабели должны быть показаны на схеме отдельными линиями. Толщина линий, изображающих провода, жгуты и кабели на схемах, должна быть от 0,4 до 1 мм. Для упрощения начертания схе-

мы допускается сливать отдельные провода, идущие на схеме в одном направлении, в общую линию.

Номера и обозначения кабелей проставляют на полках линий-выносок, вблизи от мест разветвления проводов. На схеме следует указывать типы, сечения и, при необходимости, расцветку проводов, а также типы кабелей, количество, сечение и занятость жил.

При большом количестве электрических соединений данные о проводах и кабелях, а также адреса их присоединения целесообразно свести в таблицу, именуемую «Таблицей соединений». Таблицу соединений помещают на первом листе схемы, как правило, над основной надписью или выполняют в виде последующих листов.

3.4.2. Маркировка кабелей и компонентов СКС

Для облегчения задачи администрирования структурированной кабельной системы сети необходимо каждому из ее элементов присвоить идентификатор и осуществить их маркировку. Идентификаторы должны быть присвоены помещениям, кабелям, коммутационному оборудованию, коннекторам коммутационного оборудования, коммутационным панелям и элементам заземления. Идентификаторы следует присваиваться каждому элементу, подлежащему администрированию. Идентификаторы, используемые для доступа к набору записей одного типа, должны быть уникальными.

Идентификаторы администрирования могут быть кодированными (несущими в себе какую-либо дополнительную смысловую нагрузку), либо некодированными и всегда должны служить первичным средством идентификации элемента. При использовании кодированных схем особое внимание следует уделять полному документированию схемы кодирования, так, чтобы она была понятна любому, желающему ознакомиться с системой администрирования.

В качестве идентификаторов помещения целесообразно использовать нумерацию помещений, принятую в данном здании, например, А407 — помещение номер 7 находится в отсеке А на четвертом этаже. Если по номеру комнаты нельзя определить этаж, на котором она располагается, то к номеру комнаты впереди следует добавлять цифру номера этажа и при необходимости обозначение отсека или корпуса здания.

Каждый кабель, входящий в СКС, должен иметь собственный идентификатор. Международными стандартами ANSI/TIA/EIA-606 в качестве идентификаторов рекомендуется применять следующие обозначения:

Cxxx — горизонтальный кабель (*Cable*);
CBxxx — магистральный кабель (*Cable Backbone*;)
Jxxx — разъем (*Jack*);

CDxxx — кондуит (*Conduit*);

CTxxx — кабельный лоток (*Cable tray*);

где "xxx" – некоторые буквенно-цифровые обозначения.

В соответствии с рекомендациями каждый идентификатор состоит из префикса, обозначающего элемент кабельной системы, поля, определяющего местоположение элемента и букв, идентифицирующих систему, к которой относится данный элемент кабельной системы. Эти идентификаторы должны указываться как на схеме СКС, так и наноситься на элементы кабельной системы маркировкой водонерастворимыми чернилами оболочки непосредственно самого элемента или отмечаться бирками, прикрепляемыми к элементу.

Каждый кабель должен иметь нанесенный с двух сторон уникальный идентификатор, который содержит обозначение типа кабеля (**C** — четырехпарный кабель UTP; **CB** — Магистральный 25-парный или 100-парный UTP кабель вертикальной проводки) и сквозную нумерацию.

Идентификатор телекоммуникационной розетки должен содержть следующие поля:

- буква J (*Jack*);
- трехзначный номер, включающий № этажа (первая цифра), номер комнаты;
- № рабочего места в комнате;
- № розетки на рабочем месте в комнате.

Дополнительно в идентификатор может входить буква, определяющая систему, которую обслуживает кабель: D (*Data*) — сеть передачи данных; V (*Voice*) — телефон (эта буква вносится в карту учета кабелей горизонтальной подсистемы только после того, как будет определена принадлежность порта к определенной системе). Так обозначение розетки J301-PM06-01 означает: этаж 3, ком. 01, рабочее место 6, розетка № 1.

Идентификатор гнезда кросс-панели коммутационного шкафа для окончаний кабеля типа "витая пара" должен состоять из:

- буквы **MC** (*Main Cross-Connect*) для главного распределительного пункта (кросса), **IC** (*Intermediate Cross-connect*) для этажных промежуточных распределительных пунктов (кроссов);
- № комнаты, где расположен главный коммутационный узел;
- двузначного числа — номера модуля в коммутационном блоке (может задаваться произвольно или номером RU (*Rack Unit*) коммуникационного шкафа, см. например, рисунок 3.10);
- буквы, определяющей номер столбца многопарного модуля в главном кроссе (если есть деление на столбцы);
- однозначной цифры, указывающей номер ряда в линейке многопарного модуля (если есть деление на ряды);

- тире и двузначной цифры — номера порта панели, либо двузначную цифру после тире — номер пары подключенного 25-и или 100 парного кабеля.

Примеры обозначения гнезд коммутационных панелей для главного кросса (МС) и промежуточных этажных (IC) приведены в таблице 3.4.

Таблица 3.4

Обозначение гнезд коммутационных панелей

Идентификатор гнезда	Пояснения
МС.513.28-01	Гнездо патч-панели для подключения активного оборудования расположено в главном кроссе комната 513; место панели в шкафу – 28; № порта панели 01.
МС.513.31В1-01	Гнездо кросс-панели для подключения 25-парног телефонного кабеля, расположено в главном кроссе комната 513, место панели в шкафу − 31, столбец В, № ряда в столбце − 1, № пары в панели 01.
IC.102.08A1-05	Гнездо этажной кросс-панели для кроссировки 25-парного магистрального кабеля с 4-х парным кабелем горизонтальной проводки расположено в этажном кроссе помещения 02 на первом этаже, место панели в шкафу − 08, столбец А, № ряда в столбце − 1 , № порта 5.
IC.306.22-21	Гнездо патч-панели для подключения активного оборудования расположено в этажном кроссе комната 306; место панели в шкафу – 14; № порта патч-панели 21.

Для отображения минимально необходимой информации по каждому элементу кабельной системы стандартом требуется вносить такие данные в специальные таблицы (записи), содержащие минимум следующие поля: идентификатор элемента, тип элемента, общее описание элемента (например, кабель, 4-парный, кат. 5).

3.4.3. Пример разработки схемы СКС

В процессе оформления курсового проекта студент должен выбирать масштаб чертежа размещения СКС таким образом, чтобы на нем можно было изобразить телекоммуникационные, телефонные и силовые розетки и остальные компоненты. Пример фрагмента чертежа СКС одной комнаты здания показан на рисунке 3.9. На этом же чертеже для справки приведены стандартные условные графические обозначения элементов структурированной кабельной системы (ГОСТ 21.614-88.).

Физическая структура сети кроме схемы размещения СКС должна содержать схему размещения оборудования в телекоммуникационном шкафу, таблицу подключения кабелей и текстовую часть, поясняющую содержание этих документов. В текстовой части к данному подразделу необходимо при-

вести пояснения, которые дополнительно раскрывают детали представленных чертежей. Пример такого пояснения приведен ниже.

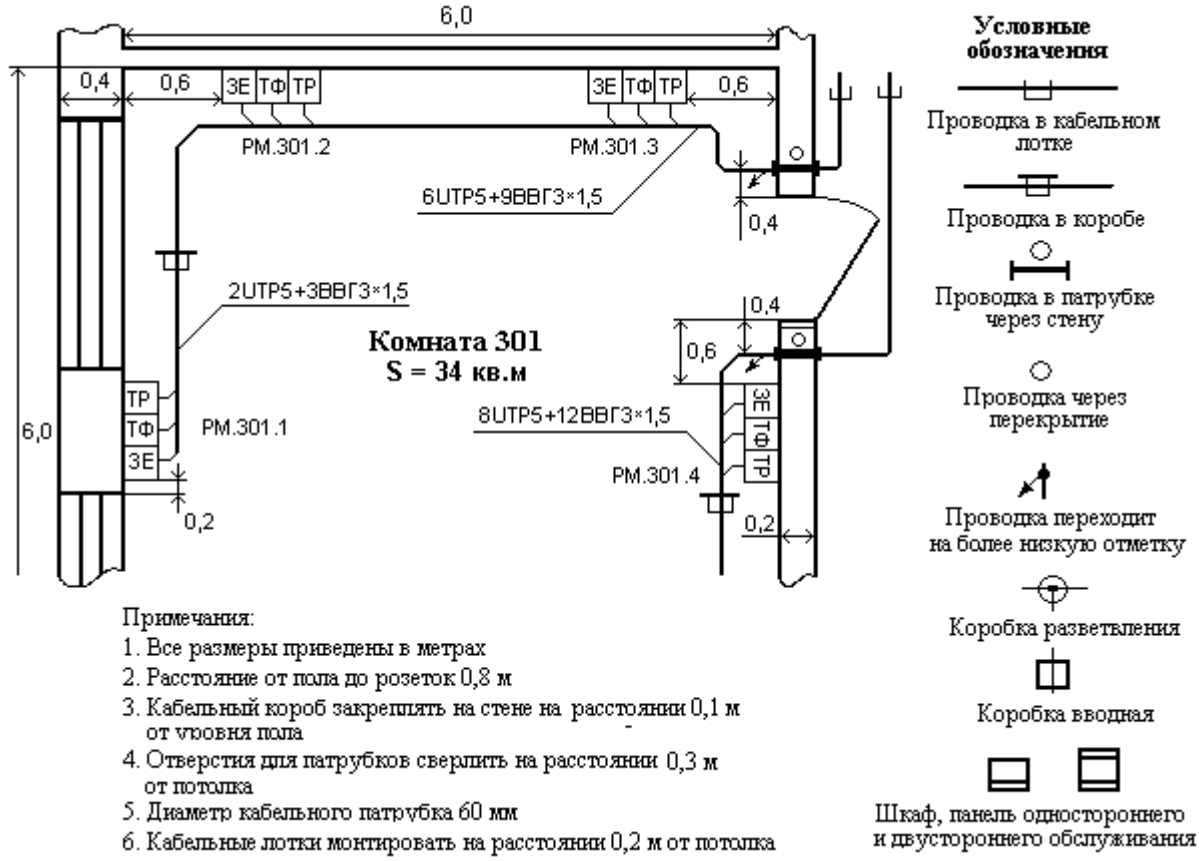


Рисунок 3.9 – Фрагмент чертежа размещения СКС в помещении и условные графические обозначения

На каждом индивидуальном рабочем месте установлены три силовых (Э) розетки напряжением 220 В две телекоммуникационные розетки (коннекторов). Одна из них предназначена для подключения телефона (ТФ), а вторая — для передачи данных (ТР). Первая розетка должна быть терминирована 4-парным кабелем (категория 3 или выше), а вторая — 4-парным кабелем категории 5. Телекоммуникационные, телефонные и силовые розетки устанавливаются на одинаковой высоте. Высота установки розеток определяется как расстояние от основного пола до центра лицевой пластины и должна составлять 800 мм. Расстояние между силовыми и информационными розетками не должно превышать одного метра.

На чертеже размещения СКС введены следующие обозначения: РМ.301.1 — обозначение рабочего места, содержащего номер комнаты и номер рабочего места; 2UTP 5 + 3ВВГЗ ×1,5 — 2 кабеля типа UTP 5-й категории и 3 силовых кабелей типа ВВГЗ сечением 1,5 мм^2.

Ввод кабелей в помещение осуществляется из кабельного лотка в двух точках через металлические патрубки (кондуиты). Затем производится спуск

кабелей в вертикально закрепленном кабельном коробе до уровня горизонтального короба. Кабели связи и силовые кабели должны быть размещены в раздельных секциях короба.

Схема установки пассивного и активного сетевого оборудования в телекоммуникационном шкафу показана на рисунке 3.10.

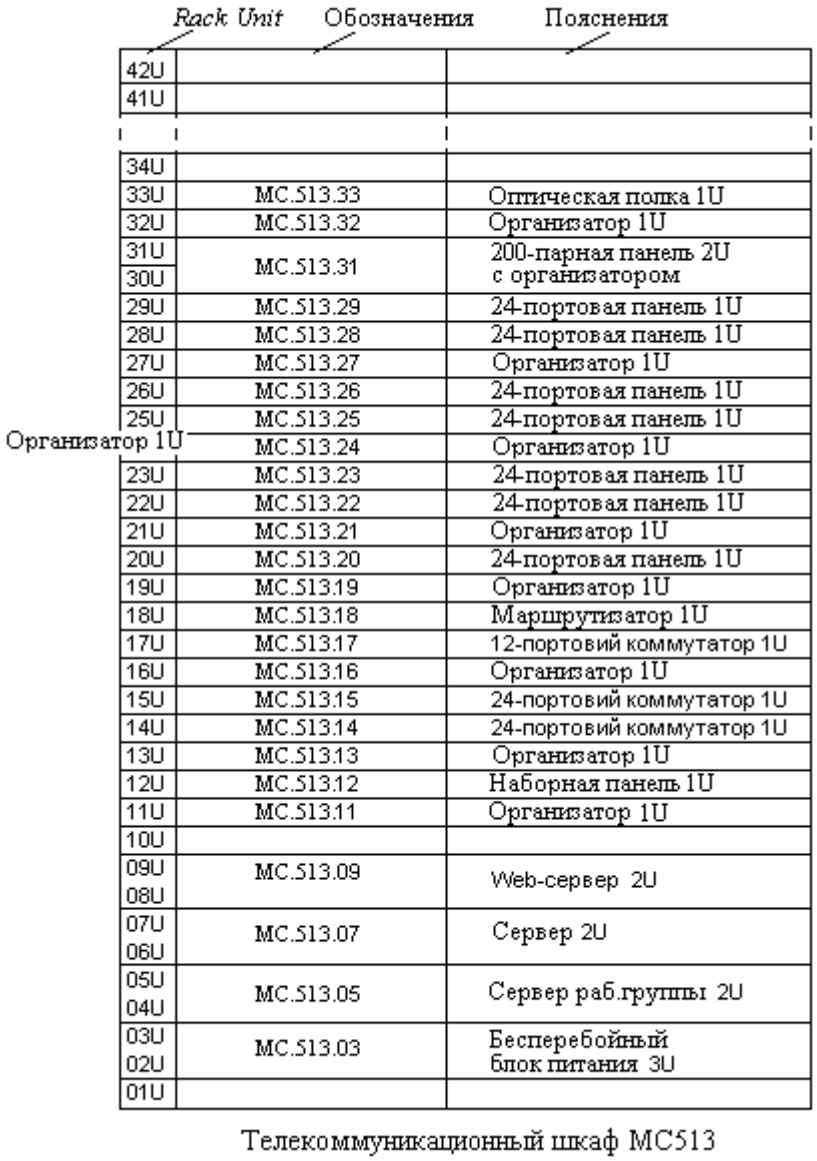


Рисунок 3.10 - Схема расположения оборудования в телекоммуникационном шкафу

Шкаф имеет стандартную высоту 42U (2055 мм), ширину 600 мм и глубину 600 мм. Серверы и 200-парная панель с организатором имеют высоту 2U, а остальное оборудование — высоту 1U. Для подключения оптических кабелей используется оптическая полка высотой 1U, на которой располагаются дуплексные розетки многомодового разъема типа SC, предназна-

ченные для подключения оптических кабелей подсистемы внутренних магистралей.

Для подключения горизонтальных кабелей установлено ряд 19-дюймовых коммутационных панелей высотой 1U с 24 розеточными частями модульных разъемов RJ-45. Выбор этой разновидности панелей обосновывается несколько меньшей трудоемкостью монтажа по сравнению с панелями удвоенной высоты.

В таблице 3.5 приведены сведения по соединениям некоторой кабельной системе компьютерной сети. В этой таблице, в качестве примера, приведены только две строки из таблицы соединений по кабельным элементам, которая может содержать десятки, сотни и тысячи подобных строк. Первая строка дает информацию о кабеле с идентификатором C0001, проходящем в кондуите CD31 и связывающем две точки — коннектор телекоммуникационной розетки J0001 на рабочем месте, расположенном в помещении A306, и коннектор 01 патч-панели 23, установленной в телекоммуникационном шкафу MC.A309 в помещении A309.

Из дополнительной информации видно, что описываемый кабель относится к категории 5, имеет длину 50 м, обслуживает персональный компьютер PC01 на рабочем месте, обеспечивая конечному пользователю сервис TR3. Вторая строка информирует о магистральном 25-парном пожаробезопасном кабеле (25 PR) типа CMR (*Communications Riser*), предназначенного для передачи сигналов речевых сообщений и данных и имеющим идентификатор CB02.

Таблица 3.5

Пример таблицы соединений

ID кабеля	**Трасса**	**Позиция начального терминирования / позиция конечного терминирования**	**Рабочая комната / кроссовая**	**Тип кабеля / длина кабеля в метрах**	**Приложение / оборудование**
C0001	CD31	J0001 / MC. A309.23-01	A306 / A309	Категория 5/ 50	TR3 / PC 01
CB02	CD37	C4R6-002 / MC.B305.31-08	B101 / B305	25 PR CMR / 23	Voice-Data

Кабель длиной 23 метра проходит через патрубок (кондуит) CD37 и терминируется портом 08 коммутационной панели с номером 31, установленной в телекоммуникационном шкафу MC.B305, находящемся в помещении B305.

4. Разработка политики информационной безопасности в сети предприятия и списков ограничение доступа

4.1. Основные требования к политике безопасности

Политика безопасности в компьютерной сети организации представляет собой совокупность руководящих принципов, правил, процедур и практических приёмов в области безопасности, которые регулируют управление, защиту и распределение информации в сети. В настоящее время выделяют следующие уровни политики безопасности [14,19, 26]:

- правила работы пользователей в корпоративной сети;
- политика обеспечения безопасности удаленного доступа к ресурсам компьютерной сети;
- политика обеспечения безопасности при взаимодействии с сетью Интернет;
- политика допустимого использования ресурсов;
- политика безопасности периметра;
- антивирусная политика, инструкция по защите от компьютерных вирусов;
- политика выбора и использования паролей;
- правила предоставления доступа к ресурсам компьютерной сети;
- политика установки обновлений программного обеспечения;
- политика резервного копирования, хранения и восстановления данных;
- соглашение о соблюдении режима информационной безопасности, заключаемое со сторонними организациями;
- прочие.

При разработке политик безопасности очень важным является корректное распределение ролей и обязанностей исполнителей. Весьма важно соблюдать принцип наименьших привилегий: "знать только то, что необходимо для выполнения служебных обязанностей". Кроме этого необходимо предусмотреть разделение обязанностей при работе на критичных системах и ситуациях.

Основные требования к политике безопасности сводятся к следующему [14,19,26]. Разработанная политика безопасности должна быть реалистичной и выполнимой, краткой и понятной, а также не приводить к существенному снижению общей производительности подразделений предприятия. Политика безопасности должна включать основные цели и задачи организации режима информационной безопасности, четко задавать области действия, а также указывать обязанности должностных лиц, касающиеся вопросов защиты информации. Рационально составленная политика безопас-

ности обычно занимает не более 3-5 страниц текста. На практике политика безопасности ежегодно пересматривается с целью учета текущих изменений в работе предприятия.

Следует заметить, что в реальной ситуации для создания эффективной политики безопасности необходимо вначале провести анализ рисков в области информационной безопасности. Затем определить оптимальный уровень риска для предприятия на основе заданного критерия. Политику безопасности и соответствующую корпоративную систему защиты информации нужно построить таким образом, чтобы не превышать заданного уровня риска при минимальных затратах.

При этом необходимо помнить, что главная задача любой системы информационной безопасности заключается в обеспечении устойчивого функционирования объекта: предотвращении угроз его безопасности, защите законных интересов владельца информации от противоправных посягательств, в том числе уголовно наказуемых деяний в рассматриваемой сфере отношений, предусмотренных Уголовным кодексом, обеспечении нормальной производственной деятельности всех подразделений объекта.

Другая задача сводится к повышению качества предоставляемых услуг и гарантий безопасности имущественных прав и интересов клиентов [19]. Для этого необходимо присвоить корпоративной информации гриф «Для служебного пользования», создать условия для своевременного обнаружения угроз нарушения информационной безопасности и принять все меры для минимизации нанесения финансовых, материальных и моральных потерь.

4.2. Дифференциация политики безопасности для отдельных уровней сервисов

Политика удаленного доступа определяет допустимые способы удаленного соединения с корпоративной информационной системой. Она представляет собой основной документ безопасности организаций и предприятий с разветвленной сетью филиалов и подразделений. Такая политика должна регламентировать все доступные способы удаленного доступа к внутренним информационным ресурсам компании: доступ по коммутируемым сетям (*SLIP, PPP*), доступ с использованием сетей *ISDN/Frame Relay, служб Telnet/SSH* через Интернет, выделенную линию (*DSL*) и пр. При этом должны быть четко определены все ограничения по организации удаленного доступа к информационным ресурсам сети.

Политика безопасности при взаимодействии с сетью Интернет. Соединение сети организации (предприятия) с Интернетом делает доступными для внутренних пользователей внешние сервисы, а для внешних пользователей – доступ к информационным ресурсам организации (предприятия). Поэтому на основе анализа и учета вида деятельности предприятия и

задач, стоящих перед ним, проектировщиком должна быть создана политика безопасности, которая четко и ясно определяет, какие сервисы разрешено использовать пользователям корпоративной сети, а какие – запрещено, как для внутренних, так и для внешних пользователей.

Существует достаточно большое количество Интернет-сервисов, имеющие различные степени защищенности. К наиболее распространенным можно отнести:

- Протоколы *FTP, telnet, http*. *FTP* - протокол передачи файлов в компьютерных сетях. Позволяет подключаться к серверам FTP, просматривать содержимое каталогов и загружать файлы с сервера или на сервер, кроме того, возможен режим передачи файлов между серверами. FTP не разрабатывался как защищённый протокол и имеет многочисленные уязвимости в защите. В протоколе *telnet* не предусмотрено шифрования, ни проверки подлинности данных. Поэтому он уязвим практически для любого вида атак. Для обеспечения удалённого доступа к сетевым ресурсам следует применять сетевой протокол SSH, при создании которого упор делался именно на вопросы безопасности. **HTTP** - протокол прикладного уровня, предназначавшийся вначале для передачи данных в виде гипертекстовых документов в формате HTML, в настоящий момент используется для передачи произвольных данных.
- Почтовый офисный протокол POP – служит для получения электронной почты с сервера. POP3 поддерживает различные методы аутентификации для предоставления разных уровней защиты от незаконного доступа к пользовательской почте. Более широкие возможности работы с почтовыми сообщениями, находящимися на центральном сервере предоставляет пользователю протокол IMAP.
- Протокол *Whois* **—** разработан для получения регистрационных данных о владельцах IP адресов и доменных имен в текстовом виде. Протокол часто применяется для проверки возможности использования доменного имени, свободно оно или уже зарегистрировано. Протокол Whois не содержит средств контроля безопасности, поэтому его можно применять только для открытой информации.
- Протоколы удаленной печати в Unix lp и lpr **—** предназначены для удаленного доступа к принтерам, присоединенные к другим хостам. Поэтому доступ к принтерам нужно обеспечивать посредством прокси-сервера, в противном случае доступ следует ограничить с помощью сетевого экрана.

Какие сервисы надо разрешать, а какие – запрещать, зависит от потребностей организации. Организация может захотеть поддерживать некоторые сервисы без усиленной аутентификации. Например, для загрузки внешними пользователями открытой информации может использоваться анонимный сервер FTP. В этом случае эти сервисы должны находиться на другой

машине, чем брандмауэр, или в сети, которая не соединена с корпоративной сетью организации, содержащей критические данные.

Примеры политики безопасности для некоторых сервисов, которые могут потребоваться в типовой организации, приведены в таблице 4.1

Таблица 4.1

Примеры политики безопасности для Интернета

Сервис	**Политика**				**Образец политики**
	Изнутри наружу		**Извне внутрь**		
	Использовние	Аутентификация	Использование	Аутентификация	
	Разрешено?	Выполняется?	Разрешено?	Выполняется?	
FTP	Да	Нет	Да	Да	
Telnet	Да	Нет	Да	Да	
Rlogin	Да	Нет	Да	Да	
HTTP	Да	Нет	Нет	Нет	
POP3	Нет	Нет	Да	Нет	
NNTP	Да	Нет	Нет	Нет	Внешний доступ к NNTP-серверу запрещен.
SQL	Да	Нет	Нет	Нет	
Rsh	Да	Нет	Нет	Нет	Входящие запросы на rsh-сервис должны блокироваться на брандмауэре.
Другие, такие как NFS	Нет	Нет	Нет	Нет	Доступ к любым другим сервисам, не указанным выше, должен быть запрещен в обоих направлениях, чтобы использовались только те Интернет-сервисы, которые нам нужны, и о безопасности которых имеется информация, а остальные были запрещены.

При разработке политики, связанной с обеспечением безопасности при взаимодействии с сетью Интернет нужно также учитывать административные проблемы, связанные с доступом к незащищенной сети. В таблице 4.2 приведена часть из этих проблем.

Таблица 4.2

Административные проблемы политики безопасности

Сервис	Протоколы	Что нужно сделать?	Почему это надо сделать?
E-mail		Пользователи должны иметь только по одному адресу электронной почты	Чтобы не раскрывать коммерческой информации.
	SMTP	Сервис электронной почты для организации должен осуществляться с помощью одного сервера	Централизованный сервис легче администрировать. В SMTP-серверах трудно конфигурировать безопасную работу.
	POP3	POP-пользователи должны применять APOP-аутентификацию.	Чтобы предотвратить перехват паролей.
	IMAP	Рекомендовать переход на IMAP.	Он лучше подходит для удаленных пользователей, имеет средства шифрования данных.
WWW	HTTP	Направлять на www.my.org	Централизованный WWW легче администрировать. WWW-серверы тяжело конфигурировать
*	Все другие	Маршрутизировать	

4.3. Процедуры безопасности

Процедурами в системах безопасности компьютерных сетей называют детальные пошаговые инструкции, которые сотрудники обязаны неукоснительно выполнять. Процедуры безопасности также важны, как и политики безопасности. Если политики безопасности определяют "что" должно быть защищено, то процедуры безопасности определяют "как" защитить информационные ресурсы компании. Рассмотрим примеры некоторых процедур безопасности (http://citforum.ru/security/internet/security_pol/).

Процедура управления конфигурацией обычно определяется на уровне всей организации или на уровне ее подразделений. Служба безопасности компании разрабатывает правила управления изменениями для всей организации (предприятия), которые обязательны для соблюдения всеми отделами и службами. Однако подразделения организации (предприятия) или рабочие группы могут иметь собственные процедуры управления конфигурацией. Правила контроля за изменениями должны регламентировать процесс документирования и запроса на изменения конфигурации всех масштабов (от простой инсталляции маршрутизатора до изменения списков контроля доступа на межсетевом экране). Одной из важнейших задач службы

безопасности является анализ изменений и контроль запросов на изменения. Процедура контроля изменений играет важную роль по следующим причинам [19]:

- документированные изменения обеспечивают возможность проведения аудита безопасности;
- в случае возможного простоя из-за изменения, проблема будет быстро определена;
- обеспечивается способ координирования изменений таким образом, чтобы одно изменение не влияло на другое изменение

Процедуры резервного копирования и хранения информации. Резервное копирование данных позволяет сохранить информацию при технических сбоях информационной системы или действий злоумышленников и обеспечить работоспособность предприятия (организации) в таких условиях. Для реализации процедуры резервного копирования в информационной системе следует инсталировать специальное программное обеспечение, предназначенное для этих целей. Резервные копии файлов следует хранить на съемных носителях (магнитных или оптических дисках, флэшкартах). Целесообразно резервные копии зашифровать. Для защиты от несанкционированного доступа резвные копии нужно хранить в несгораемых сейфах, находящихся в отдельных помещениях. В ряде случаев, по требованию клиентов или бизнес-партнеров, может потребоваться хранение информации за пределами организации. При этом должно быть сведено к минимуму количество сотрудников организации, которым предоставляется право доступа к резервным копиям, размещаемым за пределами организации (предприятия).

Периодически должна тестироваться возможность восстановления информации из резервных носителей на регулярной основе для проверки целостности резервных копий.

Процедура обработки инцидентов (случаев нарушения информационной безопасности). Инциденты информационной безопасности подразделяются на внутренние и внешние. При внутреннем инциденте источником нарушения является лицо, работающее в данной организации, а при внешнем — источник нарушения никак не связан с пострадавшей стороной. Постоянный рост количества внутренних и внешних инцидентов нарушения информационной безопасности приводит к необходимости внедрения процедур обработки инцидентов в каждой организации и предприятии. В политике безопасности должны быть определены действия на все известные случаи нарушения информационной безопасности. К наиболее типовым инцидентам относятся неправомерный доступ к данным; удаление информации; повышенная сетевая активность; сканирование портов, атаки типа "отказ в обслуживании", перехват и подмена трафиа, аномальное поведение приложений и др.

После обнаружения ицедента и нейтрализации его последствий должно быть проведено его расследование и переконфигурация информационной

системы с учетом повышенных требований к информационной безопасности.

4.4. Реализация политики безопасности в сети на основе списков доступа

В процессе реализации политики сетевой безопасности одной из важнейших задачей является возможность закрытия доступа для некоторых пакетов. Для отсечения нежелательных пакетов широко применяются списки доступа ***ACL*** (*Access Control Lists*)**,** которые являются своеобразными фильтрами пакетов [9,12,30,31].

Список доступа — это упорядоченный набор директив (команд), каждая из которых разрешает или запрещает прохождение пакета через интерфейс. Списки доступа могут применяться на входе в маршрутизатор (in) и на его выходе (out). В первом случае сначала выполняется проверка пакета, а затем, если прохождение его разрешено, выполняется его маршрутизация. Если пакет не пропускается, то по адресу его отправителя посылается управляющее ICMP-сообщение "хост недоступен" (*Host unreachable*). Во втором случае пакет сначала маршрутизируется и только потом его параметры сравниваются с условиями списка.

Для идентификации списков доступа им назначаются номера или присваиваются имена. Использование нумерованных или именованных списков доступа определяется их применением. Так одни протоколы требуют использования только нумерованных списков, а другие допускают как нумерованные, так и именованные списки. Если применяются нумерованные списки, то номера их должны находиться в определенном диапазоне, в зависимости от области применения списка доступа. Некоторые, наиболее часто используемые диапазоны номеров приведены в таблице 4.3.

Правила построения и назначения списков доступа для различных протоколов имеют свою специфику, однако, можно выделить два этапа работы с любыми списками доступа. Сначала, создается список доступа, а затем выполняется привязка его к соответствующему интерфейсу, линии связи или логической операции, выполняемой маршрутизатором (роутером).

Каждое предписание в списке доступа записывается отдельной строкой. Список доступа в целом представляет собой набор строк с директивами, имеющих один и тот же номер (или имя). Порядок задания директив в списке играет важную роль. Проверка пакета на соответствие списку производится последовательным применением предписаний из данного списка (в том порядке, в котором они были внесены). В конце каждого списка системой IOS добавляется неявное правило, состоящее в том, что если пакет удовлетворяет какому-либо предписанию, то дальнейшие проверки его на соответствие следующим директивам в списке НЕ ПРОИЗВОДЯТСЯ. Таким об-

разом, пакет, который не соответствует ни одному из введенных предписаний, отвергается.

Таблица 4.3

Стандартные номера списков доступа

Обозначение списков	**Доступ**	**Диапазон номеров**
Стандартный список IP	По IP-адресу источника	1 - 99
Расширенный список IP	По IP-адресам источника и получателя, протоколам, портам	100 - 199
MAC Ethernet address	По MAC-адресу	700 - 799
Стандартный IPX	По адресу IPX	800 - 899
Extended IPX	По полному адресу IPX	900 - 999
Фильтры IPX SAP	По адресу источника и типу службы	1000 -1099

Для одного списка можно определить несколько директив. Каждая из них должна ссылаться на имя или на номер списка, для того, чтобы все они были связаны с одним и тем же списком. Количество директив может быть произвольным, и ограничено лишь объемом имеющейся памяти. Однако, чем больше в списке директив, тем труднее понять логику работы списка и контролировать ее. Поэтому рекомендуется тщательно заносить всю информацию о списках в специальный журнал.

Как уже упоминалось выше, порядок строк в списке доступа очень важен, поскольку невозможно изменить этот порядок или исключить какие-либо строки из существующего списка доступа. По этой причине целесообразно предварительно создавать списки доступа (например, на tftp-сервере) и загружать их целиком в маршрутизатор, а не пытаться редактировать их на маршрутизаторе.

Если список доступа с данным номером (именем) существует, то строки списка с тем же номером (именем) будут добавляться к существующему списку в конец его. Поэтому, первой строкой в файле, содержащем описание списка доступа для загрузки с tftp-сервера, должна стоять команда отмены существующего списка "no access-list".

Для протокола IP поддерживаются следующие виды списков доступа:

- стандартные списки управления доступом (проверяют только адрес отправителя пакета);
- расширенные списки управления доступом (проверяют адрес отправителя, адрес получателя и дополнительно ряд параметров пакета);
- динамические расширенные списки управления доступом.

Расширенные списки управления доступом *extended ACL* (*extended Access Control List*) используются чаще, чем стандартные, поскольку они обеспечивают большие возможности контроля. Расширенные списки предписывают проверку как адреса источника, так и адреса получателя. Они могут также проверять конкретные протоколы, номера портов и другие параметры. Это придает им большую гибкость в задании проверяемых условий. Пакету может быть разрешена отправка или отказано в передаче в зависимости от того, откуда он был выслан и куда направлен.

Списки управления доступом представляют собой перечень особых директив (предписаний): «**разрешить**» (*permit*) и «**запретить**» (*deny*). Эти директивы применяются к адресам или протоколам верхних уровней (3-7). Предписание «разрешить» означает, что все пакеты, отвечающие определенным условиям, будут пропущены, т.е. им будет разрешено дальнейшее перемещение по сети. Предписание «запретить» указывает, что пакет, имеющий определенные характеристики, необходимо удалить. Списки доступа могут применяться для запрещения продвижения пакетов через определенный интерфейс маршрутизатора в ту или другую сторону, для ограничения доступа некоторых пользователей и устройств к сетевым ресурсам, для указания способа шифрования, а также для указания приоритетности обработки пакетов.

Каждая из директив в списке доступа читается процессором маршрутизатора по порядку, т.е. очередной пакет, проходящий через соответствующий порт, будет последовательно сравниваться со всеми критериями (адресом источника, адресом получателя или номером порта) в списке доступа с начала списка до конца. Если пакет не соответствует условию первой директивы, то он проверяется на соответствие второй директиве из списка управления доступом. А если параметры пакета соответствуют следующему условию, которое представляет собой директиву разрешения доступа, то ему разрешается отправка на интерфейс получателя. Таким образом, при первом обнаружении соответствия остальные директивы не рассматриваются. Поэтому, если была записана директива, разрешающая передачу всех данных, то все последующие директивы не проверяются. Следует особо подчеркнуть, что **в конце каждого списка выполняется неявное правило "deny all"** (запретить все), поэтому при назначении списков на интерфейс нужно следить, чтобы явно разрешить все виды необходимого трафика через интерфейс (не только пользовательского, но и служебного, например, обмен информацией по протоколам динамической маршрутизации).

Список доступа разрешается задавать для любого интерфейса маршрутизатора. Однако следует иметь в виду, что каждый сетевой протокол, поддерживаемый интерфейсом, ассоциируется только с одним списком доступа. Так для порта Ethernet0 маршрутизатора, который сконфигурирован под IP- и IPX-маршрутизацию, могут существовать отдельные списки доступа для фильтрации как трафика IP, так и IPX.

Один и тот же список доступа может быть предписан разным интерфейсам одного и того же маршрутизатора. При этом разрешается также задавать списки доступа отдельно для входящих и исходящих пакетов.

В случае необходимости внесения дополнительных директив следует удалить весь список и заново создать его с новыми предписаниями. Каждая дополнительная директива может добавляться только в конец списка. Таким образом, невозможно удалить в нумерованном списке отдельные директивы после того, как они были созданы, а можно удалить только весь список полностью.

Одной из разновидностей списков управления доступом, являются списки, учитывающие время (*Time-based access list*). Воздействие таких списков доступа на трафик определяется двумя переменными — днем недели (или точной датой) и временем суток. Использование временных списков доступа позволяет удовлетворить многие требования, предъявляемые к современной компьютерной сети. Например, политика ограничения доступа в организации может быть разной для рабочего времени, вечерних часов или выходных. В частности, сетевой администратор может ограничить пользование Internet только рабочим временем, т. е. разрешить доступ с 8:00 до 17:00, исключая при этом время на обеденный перерыв. Интервалы времени бывают двух типов — абсолютный (*absolute*) или периодический (*periodic*). В последнем случае диапазон времени может состоять более чем из одного временного интервала.

Более детально о составлении списков доступа, работе с ними и примеры задания списков доступа изложено в п.п.6.5 и в [2, 13, 31].

5. Проектирование сетей на основе коммутаторов

5.1. Архитектура программно-управляемых сетевых коммутаторов

В настоящее время промышленностью выпускается широкий спектр сетевых коммутаторов, позволяющих удовлетворить самые разнообразные запросы разработчиков и администраторов компьютерных сетей. Коммутаторы различных производителей обладают примерно одинаковыми техническими параметрами и эксплуатационными возможностями и отличаются преимущественно способом конфигурации, надежностью, возможностью работать в неблагоприятных условиях окружающей среды и стоимостью. Выбор того или иного производителя коммутаторов зачастую определяется экономическими возможностями заказчика и опытом и субъективными предпочтениями проектировщика.

По данным аналитических агентств наиболее крупными производителями коммутаторов для малых, средних и крупных предприятий на начало 2018 года является корпорация *Cisco Systems* (свыше 53 % мирового рынка), *Huawei* – 10,3%, *Hewlett-Packard Enterprise* (HPE) – приблизительно 5,9% мирового рынка. Далее следуют корпорации Arista Networks (5,9%), Juniper Networks, *D-Link* и прочие производители.

В данном разделе приводятся примеры проектирования локальных сетей преимущественно на основе коммутаторов *Cisco* (торговая марка *Catalyst*), особенностью которых является использование большого количества проприетарных телекоммуникационных протоколов. Поэтому в пособии также рассмотрены примеры создания компьютерных сетей на базе популярных в нашей стране коммутаторов D-Link и Huawei, в которых, как и в устройствах остальных производителей коммутационного оборудования, используются преимущественно стандартные телекоммуникационные протоколы.

5.1.1. Состав и устройство программно-управляемых коммутаторов

Програмно-управляемый коммутатор (*Switch*) представляет собой специализированный компьютер, предназначенный для выполнения ряда телекоммуникационных задач [6,10,11,16,32,36,39]. Такой коммутатор имеет собственный центральный процессор, тип которого может различаться в зависимости от класса коммутатора, фирмы-изготовителя, типа коммутатора внутри класса. Кроме центрального процессора в состав коммутатора входят запоминающее устройство и порты ввода/вывода. Процессоры коммутаторов могут работать с различными видами памяти (рисунок 5.1): ПЗУ (ROM),

ОЗУ (*RAM*), флэш-памятью и энергонезависимой оперативной памятью типа NVRAM (*Non Volatile RAM*). Из всех этих видов памяти только RAM является энергозависимой, в которой содержимое разрушается после выключения питания коммутатора.

Управление коммутатором выполняет собственная операционная система, например Cisco IOS (*Internetwork Operating System*). Она хранится обычно в ПЗУ или флэш-памяти. Энергозависимое ОЗУ используется преимущественно для хранения текущей конфигурации коммутатора, которая считывается при его начальной загрузке.

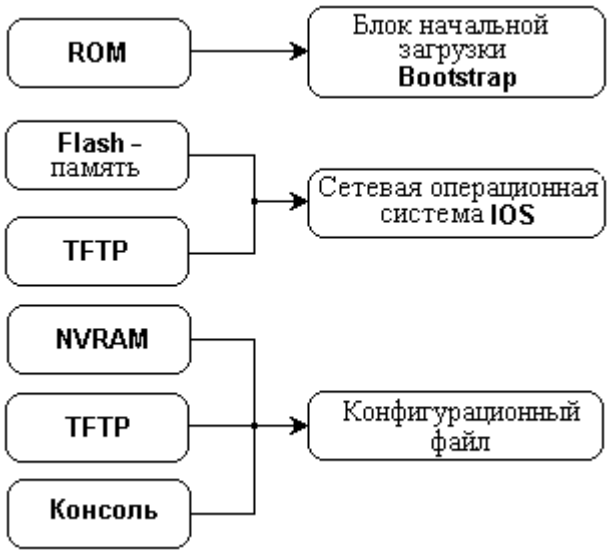


Рисунок 5.1 – Схема состава памяти и процесса начальной загрузки сетевого коммутатора

Для работы коммутатора необходимо наличие сетевой операционной системы IOS и файла с данными конфигурации. После подачи питания на коммутатор из ПЗУ в оперативную память заносится блок начальной загрузки Bootstrap. Программа начальной загрузки содержит ряд командных строк. Вначале исполняются команды тестирования устройства, так называемая POST-процедура (*Power On Self Test*). Если аппаратная часть коммутатора функционирует нормально, то инициализируется операционная система IOS, которая находится в Flash-памяти. В конце процесса загрузки из NVRAM в оперативную память загружается конфигурационный файл. После этого хранение команд и текущих изменений конфигурации будет осуществляться только в ОЗУ, и лишь при получении из командной строки инструкции «Запись» или «Копирование программы стартовой конфигурации» текущая конфигурация коммутатора будет сохранена в качестве стартовой в энергонезависимом запоминающем устройстве NVRAM.

Кроме этого коммутатор может сохранять данные на TFTP-сервере либо получать их с него. Так, например, если комутатор при старте не обнаруживает в NVRAM конфигурационного файла, то он пытается найти его на TFTP-сервере. И только, если коммутатор и на сервере не находит конфигурационного файла, происходит загрузка модуля Setup и коммутатор переключается в режим конфигурации с консоли. Такое состояние характерно для несконфигурированного коммутатора.

Конструктивно многие модели коммутаторов (например, коммутаторы фирмы *Cisco Catalyst* 4500 или *Catalyst* 6500, либо DES-7200 или DGS-3700 фирмы D-Link) представляет собой шасси (корпус) с одним или несколькими блоками питания и ряд слотов (соединителей). В настоящее время выпускается несколько вариантов шасси (с 3, 6, 9 и 13 слотами расширения) [10,32]. В такие слоты могут устанавливаться и различные виды модулей, в частности:

- системные модули, называемые супервизорами (*Supervisor Engine*), которые являются обязательным компонентом любого коммутатора *Catalyst*;
- интерфейсные модули (*Line Card*), реализующие широкий спектр сетевых интерфейсов (**портов**), посредством которых осуществляется подключение; физически порты представляет собой разъёмы, к которым с помощью кабелей подключаются рабочие станции, другие коммутаторы, маршрутизаторы и т.п.;
- сервисные модули, аппаратно реализующие дополнительную функциональность, в частности, межсетевой экран, средства мониторинга и анализа трафика, систему обнаружения вторжений и т. д.

В коммутаторах можно комбинировать модули с различными типами портов. Модульная конструкция коммутаторов обеспечивает хорошую масштабируемость и возможность постепенной замены основных компонент системы по мере их физического и морального износа.

Управление интерфейсными портами осуществляется программными модулями Supervisor, входящих в ОС коммутатора. Обычно один модуль управляет несколькими портами. Так в коммутаторах семейства Catalyst 5000, для получения максимальной гибкости и эффективности решения поставленных задач, используются пять вариантов модулей супервизора, что позволяет решать задачи коммутации на уровнях от коммутационного шкафа до малых и средних магистралей.

В большинстве устройств модули Supervisor Engine обеспечивают многоуровневую коммутацию: уровень 2 (MAC), уровень 3 (IP) и уровень 4 (TCP/UDP). В качестве интерфейсных применяются разнообразные модули с портами со скоростью обмена 10/100 Мбит/с или 1 Гбит/с для медного кабеля, 100Base-FX и 10Gigabit для оптоволокна. Существуют модули 10/100Base-T и 10/100/1000Base-T с подачей питания по медному кабелю для IP-телефонов и точек доступа беспроводных сетей. На практике в 10-

слотовом шасси, в зависимости от модели, можно обеспечить подключение от 96 до 336 портов разного типа.

На рисунке 5.2 показан общий вид модульного коммутатора семейства Catalyst 5500 с двумя управляющими модулями, 13 слотами расширения и с двумя блоками питания.

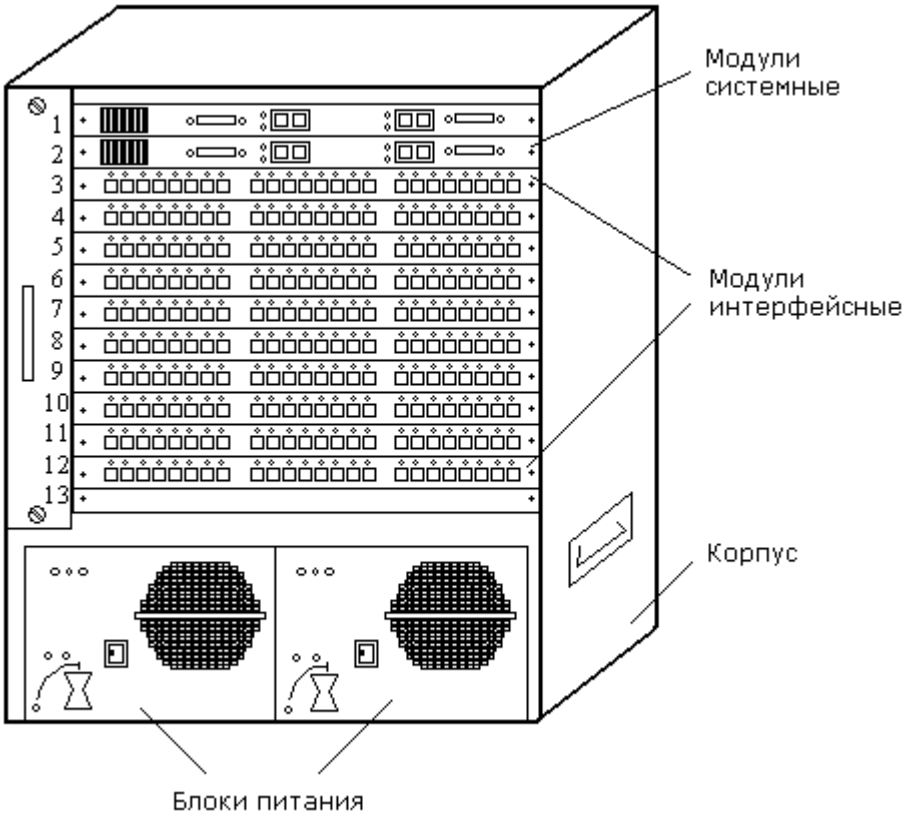


Рисунок 5.2 – Общий вид модульного коммутатора

В устройствах Cisco каждый канальный интерфейс называется *портом* и обозначается несколькими способами. В коммутаторах с фиксированной конфигурацией интерфейсы нумеруются последовательно без привязки к слоту, в котором они установлены. В устройствах модульной конструкции с заменяемыми платами интерфейсов порты нумеруются с использованием синтаксиса типа модуль(слот)/порт. Системный модуль имеет нулевой номер. Например, второй порт платы интерфейса Ethernet, установленной в первый слот, будет иметь обозначение ethernet 1/2. Для конфигурирования интерфейсов используется основная команда **interface**. Эта команда с указанием после нее номера порта интерфейса или слот/порт используется в режиме конфигурирования. В модульных коммутаторах Catalyst при обозначении модулей сначала указывается тип интерфейса, затем слот, а после него порт. Например, 3-й Ethernet модуль и 2-й порт на плате обозначается как "e 3/2".

По конструктивному исполнению коммутаторы подразделяются на три вида: настольные коммутаторы (*Desktop switch*); коммутаторы для установки в телекоммуникационный шкаф или стойку (*Rack mounted switch*) и коммутаторы на основе общего корпуса — шасси (*Chassis switch*). По сравнению с настольными устройствами коммутаторы, устанавливаемые в телекоммуникационный шкаф, обладают более высокой производительностью и надежностью. Они имеют больше портов и реализуют более широкий набор сетевых функций. Коммутаторы на основе шасси содержат слоты, которые могут быть использованы для установки интерфейсных модулей расширения, резервных источников питания и процессорных модулей. Модульное решение обеспечивает гибкость применения, высокую плотность портов и возможность резервирования критичных для функционирования коммутатора компонентов.

Все программируемые коммутаторы имеют ***консольный порт***, функции которого выполняет асинхронный интерфейс RS-232. Такой порт позволяет управлять коммутатором с персонального компьютера, который с помощью консольного кабеля соединяется с COM-портом ПЭВМ. В новых типах коммутаторов консольный порт имеет разъем RJ-45. Этот разъем можно соединить посредством специального консольного кабеля и переходника с COM-портом компьютера.

С целью задания режимов и параметров работы коммутатора необходимо осуществить процедуру его настройки (***конфигурации***). Для выполнения конфигурации следует соединить консольным кабелем свободный COM-порт компьютера с консольным портом коммутатора. Затем на ПЭВМ нужно запустить программу эмуляции терминала (например, *Hyper Terminal*) и настроить ее параметры. Кроме конфигурации через консольный порт настройка коммутатора может осуществляться и по сети с использованием протоколов *Telnet* или *TFTP*. Порт консоли устанавливается на следующие характеристики: скорость передачи 9600 бод; 8 бит данных; один стоповый бит; контроль четности отсутствует.

Настройка коммутатора выполняется с помощью **интерфейса командной строки CLI** (*Command-Line Interface*), который предоставляется операционной системой IOS [4].

Большинство современных коммутаторов, независимо от производителя, поддерживают несколько дополнительных возможностей, отвечающих общепринятым стандартам. Среди них к самым распространенным и наиболее используемым относятся следующие:

- реализация технологии виртуальных сетей – *VLAN;*
- поддержка протокола *Spanning Tree* IEEE 802.1d и *Rapid Spanning Tree* IEEE 802.1w;
- объединение каналов *Ethernet* в единый магистральный поток;
- поддержка SNMP-управления потоком данных;

- обеспечение функции безопасности *Port Security*, или привязка MAC-адреса к определенному порту и др.

5.1.2. Объединение коммутаторов в стек

Для увеличения количества портов, при сохранении единства управления и мониторинга ими, разработаны специальные коммутаторы, позволяющие объединять их в одно логическое устройство — стек коммутаторов. Такие коммутаторы представляют собой устройства, которые могут работать автономно, так как выполнены в отдельном корпусе, но имеют специальные интерфейсы, которые позволяют их объединять в общую систему, работающую как единый виртуальный коммутатор. Объединение коммутаторов в стек осуществляется с помощью специальных интерфейсных модулей и кабелей. Объединенные в стек коммутаторы имеют общие таблицы коммутации, а коммутаторы уровня L3 и общие таблицы маршрутизации.

Существуют две топологии стекирования: *кольцевая* и *звездная* [10]. При кольцевой топологии каждый коммутатор, входящий в стек, соединяется специальными кабелями с выше и ниже установленными коммутаторами. Выход коммутатора, расположенного на вершине стека, соединяется со входом самого нижнего устройства. При передаче данных кадры последовательно передаются от одного коммутатора стека к другому до тех пор, пока не достигнут портов назначения. Модуль управления стеком автоматически определяет оптимальный путь передачи кадров, стремясь к максимальному использованию пропускной способности. Преимуществом топологии "кольцо" является то, что при выходе одного устройства из строя или обрыве связи остальные устройства стека будут продолжать функционировать в обычном режиме.

При звездной топологии коммутаторы соединяются не друг с другом, а со специальным узловым коммутаторомтак называемым мастером стека, выполняющим управление стеком и обменом данными между любыми парами, входящими в стек коммутаторов. По сравнению с кольцевой звездная топология обеспечивает большую живучесть сети, т.к. нарушение связи между любым коммутатором и мастером не повлияет на остальные каналы связи стека. Мастер стека является единственной точкой управления в масштабах всего стека. Все члены стека могут исполнять роль мастера стека. Если мастер стека становится недоступным, оставшиеся члены стека выбирают из самих себя нового мастера.

Современные коммутаторы позволяют объединять в стек до 8 устройств, а некоторые типы 12 коммутаторов и более.

5.2. Алгоритмы покрывающего дерева

5.2.1. Алгоритм STP

В сетях *Ethernet* коммутаторы поддерживают только древовидные связи, т.е. которые не содержат петель. При построении или модернизации сегментированной сети с большим количеством мостов и/или коммутаторов в результате ошибок монтажа или попыток резервирования соединений возможно образование дополнительных связей между сегментами, когда от одного сегмента к другому пакет может попасть более чем одним путем (рисунок 5.3).

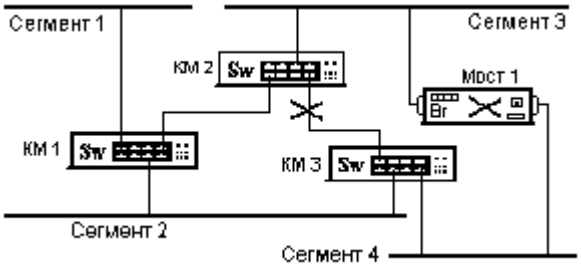


Рисунок 5.3 — Пример иллюстрации наличия петель в сети

Это приведет к циркуляции пакетов в замкнутых петлях и перегрузке сети. Кроме того, каждый посланный пакет, поступающий через разные порты, мосты/коммутаторы принимают за два различных пакета и постоянно обновляют свои таблицы. В приведенном примере проблема может быть решена удалением моста 1 и разрывом связи, помеченной знаком “X”. Для автоматического решения проблемы зацикливания пакетов был предложен так называемый "алгоритм покрывающего дерева". Алгоритм покрывающего дерева **STA** (*Spanning Tree Algotithm*) обеспечивает построение древовидной топологии связей сети с единственным путем минимальной стоимости от каждого коммутатора и от каждого сегмента до некоторого выделенного корневого коммутатора — корня дерева. Реализация алгоритма осуществляется на основе протокола **STP** (*Spanning Tree Protocol*), в результате действия которого мост или коммутатор самостоятельно обнаруживает лишние связи и автоматически блокирует ряд соединений, приведших к образованию петель. В случае возникновения аварийных ситуаций и недоступности основного пути, заблокированные соединения могут быть вновь открыты. Этим обеспечивается высокая надежность сети. STP входит в состав протокола мостов и коммутаторов IEEE 802.1d.

При использовании протокола STP при начальной конфигурации каждой линии связи присваивается определенный вес (чем выше приоритет, тем меньше вес). Мосты и коммутаторы периодически рассылают специальные сообщения – протокольные блоки данных моста **BPDU** (*Bridge Protocol*

Data Unit), которые содержат коды уникальных идентификаторов, присвоенных им при изготовлении. Мост или коммутатор с наименьшим значением такого кода становится корневым ("корень дерева"). Затем выявляется наикратчайшее расстояние от корневого моста/коммутатора до любого другого моста в сети. В основу алгоритма STA положена теорема из теории графов, которая утверждает, что структура любого связного графа, содержащего петли, может быть изменена путем удаления ребер таким образом, что он сохранит прежнюю связность, и при этом не будет иметь петель. Граф, описывающий дерево наикратчайших связей, и является "покрывающим деревом". Такое дерево включает все узлы сети, но необязательно все мосты или коммутаторы. Алгоритм STA функционирует постоянно, отслеживая все топологические изменения. Реализация алгоритма в компьютерной сети возможна только при условии поддержки его всеми коммутаторами/мостами. Мосты и коммутаторы, поддерживающие алгоритм STA, автоматически создают активную древовидную конфигурацию связей, то есть связную конфигурацию без петель. Древовидная структура сети строится на основании информации, полученной в результате обмена служебными пакетами, и адаптивно перестраивается при возникновении изменений в сети. В последующем при описании протокола мы будем для упрощения связывать его с сетевыми коммутаторами, подразумевая, что это относится и к мостам.

В начале работы администратор указывает корневой коммутатор путем задания ему нулевого (самого высокого) уровня приоритета, т.е. значение двух старших байт его идентификатора равно нулю. Приоритет других коммутаторов должен быть отличным от нуля. В этом случае, не зависимо от значения MAC-адресов коммутаторов сети, корневой будет всегда иметь минимальное значение идентификатора. Кроме этого администратор должен задать стоимость портов каждого из коммутаторов. Стоимость порта (*Port Cost*) определяется как условное время передачи бита через данный порт. На практике стоимость порта часто вычисляют по формуле:

Стоимость порта = 1000 / (*скорость передачи порта*, Мбит/с).

Например, стоимость порта 10Base-T=100; 100Base-TX =10; *Token Ring* –250 или 63, канала T1 = 651 и т.д. Значения другого варианта задания стоимостей, регламентированные стандартом IEEE 802.1d, приведены в таблице 5.1.

Построение сети без петель по протоколу STP осуществляется следующим образом. Каждый из сетевых коммутаторов путем выдачи на все свои порты BPDU-блоков анонсируют себя в качестве корневого, помещая свой идентификатор в полях "Идентификатор корневого коммутатора" и "Идентификатор коммутатора". Затем для каждого сетевого коммутатора из всех портов данного коммутатора определяется *корневой порт (root port),*

т.е. такой порт, путь от которого до любого из портов корневого моста имеет минимальную стоимость.

Таблица 5.1

Стоимость порта в зависимости от скорости передачи

Скорость передачи, Мбит/с	4	10	16	45	100	155	622	1000	10000
Стоимость порта	250	100	62	39	19	14	6	4	2

Для этого корневой коммутатор рассылает BPDU-блоки на все свои выходные порты. В поле "Стоимость пути до корня" вначале устанавливается нулевое значение. Следующие коммутаторы прибавляют к этому полю стоимость своих портов и отправляют блоки далее смежным узлам. Это дает возможность каждому коммутатору определить свой корневой порт, через который можно попасть в корневой коммутатор с минимальной стоимостью. Как только коммутатор получает BPDU-блок, содержащий идентификатор корневого коммутатора со значением меньше его собственного, он перестает генерировать свои собственные кадры BPDU, а начинает ретранслировать только кадры нового претендента на статус корневого коммутатора.

В процессе ретрансляции кадров каждый коммутатор увеличивает указанную в пришедшем блоке BPDU стоимость пути до корня дерева на величину стоимости сегмента (*Segment cost*), через который поступил данный блок. Тем самим в кадре BPDU, по мере прохождения через коммутаторы, аккумулируется стоимость пути до корневого узла. В течение этой процедуры каждый коммутатор для каждого из своих портов запоминает параметры путей минимальной стоимости до корня, содержащиеся во всех принятых этим портом кадрах BPDU. Затем эти коммутаторы выделяют из всех своих портов тот, который имеет минимальную стоимость до корневого коммутатора и назначает его своим **корневым портом**. Для коммутатора Sw 06 корневым портом назначается Port 6.3. Аналогичным образом находятся корневые порты остальных коммутаторов сети. На рисунке 5.3 они выделены утолщенной линией.

На следующем этапе функционирования алгоритма для каждого логического сегмента сети из всех портов всех коммутаторов, подсоединенных к данному сегменту, выбирается порт, через который будут передаваться пакеты от этого сегмента в направлении **корня** через **корневой порт** одного из коммутаторов. Для этого сначала из рассмотрения исключаются корневые порты коммутаторов, подключенных к данному сегменту. Затем из всех оставшихся портов выбирается порт с минимальной стоимостью пути до корня. Этот порт называется "**назначенный порт"** (*designated port*), а коммутатор, которому он принадлежит, получил название ***назначенный коммутатор*** *(designated switch).* Если в данном коммутаторе имеется несколько

портов с одинаковой стоимостью, то назначенным определяется порт, имеющий минимальный идентификатор. Все остальные порты, кроме корневых и назначенных, отключаются и переводятся в резервное состояние, то есть такое, при котором они не передают обычные кадры данных.

При таком выборе активных портов в сети исключаются петли и оставшиеся связи образуют покрывающее дерево. Обратите внимание, что у сегмента может быть только один назначенный порт. У корневого коммутатора все порты являются назначенными, а их стоимости до корня полагаются равными нулю. Корневой порт у корневого коммутатора отсутствует. В процессе нормальной работы корневой коммутатор продолжает генерировать служебные пакеты BPDU, а остальные коммутаторы принимают их своими корневыми портами и ретранслируют через назначенные порты. Если по истечении максимального времени жизни сообщения (по умолчанию — 20 с) корневой порт любого коммутатора сети не получит служебный пакет BPDU, то он инициализирует новую процедуру построения покрывающего дерева. Алгоритм STA включает кроме процедуры инициализации активной конфигурации и процедуру изменения конфигурации при отказах элементов сети.

5.2.2. Быстрые RSTP и MSTP протоколы

Для преодоления отдельных ограничений STP, мешающих внедрению ряда новых функций коммутаторов, в частности, функций 3-го уровня, был предложен быстрый алгоритм покрывающего дерева. Этот алгоритм стал основой международного стандарта IEEE 802.1w, получившим название **RSTP** (*Rapid Spanning Tree Protocol*). Он является дальнейшим развитием стандарта IEEE 802.1d и поддерживая обратную совместимость с ним. Процедура вычисления параметров связующего дерева у обоих протоколов одинаков. Однако, в отличие от стандартного STP, использующего временные интервалы для сбора топологии сети, RSTP использует двухстороннюю передачу данных между активными портами. Коммутаторы сохраняют таблицы MAC-адресов активных портов, участвующих в формировании покрывающего дерева. Поэтому при работе RSTP порт может перейти в состояние передачи значительно быстрее, так как он не зависит от настройки таймеров и порты больше не должны ждать стабилизации топологии, чтобы перейти в режим продвижения.

В новом алгоритме используются такие же механизмы определения топологии корневого коммутатора, однако у него применяются собственные методы, позволяющие создавать несколько вариантов связующего дерева при наличии VLAN сетей. В процессе реализации алгоритма процедуры,

основанные на RSTP, позволяют создавать единственное дерево для всех VLAN, работающих в одном STP домене.

Первоначальное построение архитектуры сети у RSTP занимает столько же времени, как и у STP. Однако, когда топология сети построена, и все коммутаторы подключены, любые операции с сегментами сети (например добавление порта, восстановление соединения), происходят мгновенно, и не требуют такого количества времени, как при использовании стандартного протокола Spanning Tree. В зависимости от размеров сети, время, которое требуется на обновление топологии, варьируется от десяти миллисекунд, до нескольких секунд.

В случае возникновения изменения в топологии сети коммутаторы они очищают свои таблицы MAC-адресов и отправляют пакет уведомления изменения топологии TCN (*Topology Change Notification*) на другие коммутаторы, пропуская таймауты STP. Повышение скорости изменения топологии сети при наличии сбоев элементов сети, достигается за счет отсутствия таймаутов. Для обеспечения быстрого восстановления топологии, RSTP выполняет следующие действия:

1) отслеживаются статусы MAC-адресов и отключения нефункционирующих портов;
2) используются пакеты BPDU для определения изменений в топологии сети;
3) отслеживаются статусы портов, которые предоставляются альтернативные пути к корневому коммутатору;
4) определяется, в случае исчезновения пути к порту корневого коммутатора, альтернативный порт и мгновенно отправляются пакеты через резервный путь;
5) применяется соединение типа «точка-точка», которое требует меньшее время на синхронизацию.

Rapid Spanning-Tree использует метод быстрого переключения между статусами STP. Для этого, в место пяти статусов оригинального протокола *Spanning Tree*, он использует четыре: *Discarding, Learning, Forwarding* и *Disabled*. Также как и в оригинальном протоколе Spanning Tree, данный статус устанавливается вручную.

В соответствии с протоколом *Rapid Spanning Tree* функции портов корневого и ближайшего к корневому порту остаются, а функция заблокированного порта в этом протоколе разделяется на резервный и альтернативный порты. Функция порта указывается протокольным блоком данных моста BPDU. В протоколе *Rapid Spanning Tree* определены следующие виды портов:

- корневой порт (Root Port) — расположенный ближе всего к корневому коммутатору, с точки зрения веса пути;

- определенный порт (Designated Port) — порт, принимающий кадр BPDU от корневого порта;
- альтернативный порт (Alternate Port) — порт коммутатора, получающий кадр BPDU от корневого коммутатора по второму пути;
- резервный порт (Backup Port) — данный порт подобен альтернативному порту, но получает BPDU от самого себя (это может быть порт коммутатора, который переправляет BPDU от корневого коммутатора и получает BPDU через другой порт);
- граничный порт (Edge Port) — настраиваемый порт, который подсоединяется к конечному устройству и не может создавать межкоммутаторную петлю. Этот порт пропускает все этапы инициализации и сразу переходит в статус Forwarding.

Для использования STP в каждой отдельной VLAN компьютерной сети разработан протокол множественного покрывающего дерева MSTP (*Multiple Spanning Tree Protocol*), оформленный в виде стандарта **IEEE 802.1s.** Этот протокол яляется расширением протокола RSTP и предназначен для расширения возможностей использования VLAN сетей. Он позволяет настраивать несколько независимых STP-деревьев в разных VLAN. Сетевой администратор может группировать и назначать VLAN на отдельные связующие деревья. Каждое такое дерево может иметь свою независимую от других деревьев топологию. Благодаря этому повышается отказоустойчивость сети к возможным сбоям, т.к. сбой соединений в отдельном дереве не повлияет на других деревья.

Применение MSTP облегчает задачу администрирования и управления крупными сетями. Так путем настройки нескольких VLAN и настройкой независимых деревьев на различных сегментах сети можно использовать резервные маршруты передачи данных.

Большинство моделей коммутаторов Catalyst поддерживают все версии протоколов связующего дерева. Однако корпорацией Cisco Systems для повышения быстродействия протокола 802.1D было сделанно несколько усовершенствований, в том числе введена функция *UplinkFast*. После включения функции UplinkFast на коммутаторе его приоритет увеличивается до 49152, а стоимость портов устанавливается равной 3000. При этом отслеживаются альтернативные корневые порты, на которых были получены сообщения Hello от корневого коммутатора. Если основной корневой порт выходит из строя, то коммутатор сразу переключается на запасной и переводит его в состояние forward. Кроме того, UplinkFast позволяет коммутаторам обновить записи в таблицах коммутации, без использования уведомление об изменении топологии сети TCN (*Topology Change Notification*) BPDU. Вместо TCN коммутатор находит MAC-адреса всех локальных устройств и отправляет один групповой (multicast) фрейм с каждым MAC-адресом в поле адреса отправителя. Удаляются также остальные записи в таблицы коммута-

ции самого коммутатора. В RSTP эта функция не используются, так как улучшения уже встроены в данный протокол.

5.3. Технология агрегирования каналов по протоколам LACP, EtherChannel и PAgP

Для получения большей скорости соединения и снижения вероятности аварийного разрыва связи между смежными коммутаторами или маршрутизаторами и коммутаторами разработана специальная технология агрегирования (объединения) каналов (портов). В соответствии с технологией агрегирования каналов создается новое соединение, которое может работать как обычное соединение или как магистраль.

В отличие от протокола покрывающего дерева STP, при агрегировании физических каналов все избыточные связи остаются в рабочем состоянии, а находящиеся в очереде кадры распределяется между ними для достижения баланса (выравнивания) нагрузки. При отказе одного из соединения, входящих в такой логический канал, трафик распределяется между оставшимися соединениями.

Технология агрегирования каналов регламентирована специальными протоколами. Первый из них разработан IEEE и издан в виде международного стандарта IEEE 802.3 ad, получившим название *Link-Aggregation Control Protokoll* (LACP). Важнейшим достоинством протокола LACP является то, что данный протокол не зависит от производителя коммутационного оборудования и поддерживается почти всеми коммутаторами.

Все реализации агрегирования каналов, выполняют одну задачу по объединению двух и более портов, в единый логический порт, обладающий повышенной пропускной способностью, резервированием соединений и балансировкой нагрузки между физическими соединениями. Технически, можно соединить коммутаторы несколькими физическими соединениями, для создания канала с повышенной пропускной способностью, но протокол *Spanning Tree*, воспримет эти соединения, как петли и отключит дублирующиеся соединения, оставив активным только одно. Агрегирование портов, помогает избежать такой ситуации и создает одно логическое соединение, которое может служить как магистралью (для нескольких VLAN сетей) или в качестве единого соединения (для подключения серверов).

В соответствии с протоколом LACP множество агрегируемых соединений объединяется в одну или несколько групп LAG (*Link Aggregated Groups*). Один из портов в группе выступает в качестве «связующего». Поскольку все члены группы в агрегированном канале должны быть настроены для работы в одинаковом режиме, все изменения настроек, произведенные по отношению к «связующему» порту, относятся ко всем членам группы.

Таким образом, для настройки портов в группе необходимо только настроить «связующий» порт. Балансировка исходящего потока между активными портами осуществляется на основании хешированной информации пакетных заголовков и последующий прием входящего потока на каждом активном порту. В хешированной части содержатся Ethernet-адреса источника и получателя сообщений, а также их IP4/IP6-адреса.

Важным моментом при реализации объединения портов в агрегированный канал является распределение трафика по ним. Если кадры одного сеанса будут передаваться через различные портам агрегированного канала, то может возникнуть ситуация, при которой два или более смежных кадров одного сеанса станут передаваться через разные порты агрегированного канала. В этом случае из-за неодинаковой длины очередей в их буферах кадры могут поступать получателю не в том порядке, в каком они генерировались на передающей стороне. По этой причине в большинстве реализаций механизмов агрегирования используются методы статического, а не динамического распределения кадров по портам, т. е. осуществляется закрепление за определенным портом агрегированного канала потока кадров определенного сеанса между двумя узлами. В этом случае все кадры будут проходить через одну и ту же очередь и их очередность не нарушится. Обычно при статическом распределении выбор порта для конкретного сеанса выполняется на основе выбранного алгоритма агрегирования портов, т.е. на основании некоторых признаков поступающих пакетов. В современных коммутаторах большинства производителей используются балансировка на основании MAC-адресов источника или получателя, MAC-адресов источника и получателя, IP-адресов источника либо получателя, IP-адресов источника и получателя.

Стандарт IEEE 802.3ad применим для всех типов Ethernet-каналов. Поэтому с его помощью можно создавать даже многогигабитные линии связи, состоящие из нескольких каналов *Gigabit Ethernet* (до 8 интерфейсов в одной группе).

Коммутаторы Cisco поддерживают агрегирование каналов по стандарту LACP, однако специалистами корпорации Cisco Systems разработаны также собственные (проприетарные) протоколы объединения каналов, в частности, объединения 10 Мбит/с Ethernet-каналов — протокол *EtherChanne*l, 100 Мбит/с FastEthernet-каналов — протокол FEC (*Fast EtherChanel*) и гигабитовых каналов — протокол GEC (*Gigabit EtherChanel*) и протокол PAgP (*Port Aggregation Protocol*).

Технология позволяет объединять несколько портов как сетей *Fast Ethernet* так и *Gigabit Ethernet*, при этом средняя пропускная способность нового соединения больше, чем в любом отдельно взятом соединении. При объединении порты *Fast Ethernet* образуют порт *Fast EtherChanel*, а агрегирование гигабитовых портов формирует порт *Gigabit EtherChanel*.

Объединение нескольких портов по терминологии технологии *EtherChannel* получило название сегмента. Повышение скорости передачи по соединению *EtherChannel* происходит за счет распределения нагрузки (кадров) между несколькими портами. Объединение портов в устройстве выполняет специальный контроллер группы портов, который распределяет кадры по сегменту *EtherChannel*, основываясь только на MAC-адресе отправителя или только получателя, либо на паре адресов — отправителя и получателя кадра. Некоторые модели коммутаторов третьего уровня и все маршрутизаторы производят распределение нагрузки на основании IP-адресов либо номеров портов TCP/UDP. В коммутаторах соединение *EtherChannel* формируется обычно с помощью аппаратных средств.

Технология *EtherChannel* может быть использована для объединения портов в группы по два, четыре и восемь штук. Два соединения позволяют получить удвоенную общую пропускную способность одного соединения, объединение из четырех — четырехкратную. Например, группа из двух *Fast Ethernet* интерфейсов позволяет получить соединение со скоростью 400 Мбит/с (в дуплексном режиме). Таким образом, с помощью данной технологии можно регулировать скорость обмена данными между источником и получателем в диапазоне стандартов от *Fast* до *Gigabit Ethernet*.

С точки зрения алгоритма распределенного связующего дерева канал *EtherChanne*l рассматривается как один порт, а не как несколько портов. Если в соответствии с алгоритмом связующего дерева линия *EtherChannel* переводится в состояние передачи или в блокирования, все сегменты этой линии переключаются в одно и то же состояние.

Различные модели коммутаторов имеют определенные ограничения на правила объединения портов. Так некоторые устройства позволяют объединять лишь два или четыре порта. При этом для объединения можно использовать только соседние порты, причем все порты должны принадлежать одной и той же сети VLAN. Если порты используются для магистралей, то все они должны быть магистрального типа.

Поэтому, прежде чем устанавливать *EtherChannel*-соединение на коммутаторе или маршрутизаторе, следует выяснить технические возможности конфигурируемого устройства и существующие в нем ограничения. В любом случае, если порты сконфигурированы для соединения в магистраль, нужно убедиться, что все они находятся в одной и той же сети VLAN, а на всех портах с обоих концов линии установлена одинаковая скорость и дуплексный режим передачи. Обычно для коммуникационных устройств, поддерживающих технологию *EtherChannel*, имеются четкие правила объединения портов. Эти ограничения обусловлены особенностями аппаратной реализации устройств, используемым набором микросхем и другими факторами.

Для объединения портов в сегмент *EtherChannel* и задания его параметров используются специальные инструкции, вводимые в командной строке либо активируемые пунктом соответствующего меню.

Чтобы облегчить процесс конфигурирования агрегированного Ethernet-соединения, корпорацией Cisco был разработан протокол агрегирования портов PAgP (*Port Aggregation Protocol*). Он помогает автоматически формировать соединение по технологии EtherChannel между двумя коммутаторами Catalyst. Протокол PAgP коммутатора может быть сконфигурирован в одном из четырех состояний: `on`, `off`, `auto` или `desirable`. Поэтому при конфигурации соединения *EtherChannel* необходимо указать, какое из состояний PAgP коммутатор Catalyst должен включить. Параметры `on` и `off` указывают на то, что коммутатор Catalyst всегда (или никогда) объединяет порты в соединение *EtherChannel*. При использовании параметра `desirable` коммутатор Catalyst разрешает создавать соединение по технологии EtherChannel до тех пор, пока противоположная сторона будет его поддерживать и пока конфигурация устройства соответствует правилам группировки портов в соединение *EtherChannel*.

Программный модуль, реализующий алгоритм распределенного связующего дерева STP, функционирует на *EtherChannel* как на обычном порту коммутатора. После того как в *EtherChannel* были добавлены порты, модуль STP проводит необходимую реконфигурацию, чтобы обеспечить беспетельную топологию сети. При внесении конфигурационных изменений для добавления или удаления портов из *EtherChannel*-сегмента необходимо учитывать их влияние на распределенное связующее дерево, что особенно важно в реально функционирующей сети, где такие изменения могут привести к нарушению работы сети.

5.4. Межсетевая операционная система коммутаторов Catalyst

5.4.1. Виды и особенности операционных систем коммуникационного оборудования

В различных коммутаторах Catalyst фирмы Cisco применялись в основном две операционные системы: система *Catalyst Operating System* (сокращенно **CatOS** или **COS**) и сетевая система ввода/вывода фирмы **Cisco IOS** (*Internet Operation System*) либо расширенная ее версия **Supervisor IOS**. Операционная система CatOS функционировала на процессорах сетевого управления устаревших коммутаторов Catalyst серии 4000, 5000 и 6000 и в новых моделях коммутаторов не используется.

Операционная система IOS применяется в сетевом оборудовании, выпускаемом корпорацией Cisco — в коммутаторах, беспроводных точках до-

ступа, мощных маршрутизаторах с десятками интерфейсов, обслуживающих магистрали сети Интернет. В Cisco IOS реализованы следующие сетевые сервисы [4]:

• базовые функции коммутации и маршрутизации;
• надёжный и безопасный доступ к сетевым ресурсам;
• функции, позволяющие легко масштабировать сеть.

Наличие нескольких операционных систем явилось результатом слияния фирмы Cisco с другими компаниями, имеющими к этому времени свои разработки коммутаторов с соответствующими ОС.

Характерным признаком работы с коммутатором с операционной системой **COS** является общее обозначение коммутатора в командной строке (приглашение) **Console**>, а с коммутатором, управляемым системой IOS, строка приглашения имеет вид **Switch**>. В процессе конфигурирования администратор может установить произвольное имя коммутатора. Обычно для упрощения администрирования сети задается либо тип коммутатора с порядковым номером или без него, либо название, указывающее на расположении коммутатора в определенном помещении или принадлежность его к какой-то сети, например, Cat2513, SwitchB501 или SwDecanat.

Сетевая операционная система Cisco IOS обеспечивает работу коммутаторов, маршрутизаторов, а также ряда телекоммуникационного оборудования различных уровней. В ней реализована широкая функциональность, применяемая во многих областях сетевых технологий, в частности [4]:

1) обеспечивается работа с основными сетевыми протоколами (IP4, IP6, IPX, AppleTalk, OSI, SNA, DECnet и др.);
2) имеются средства поддержки большого количества протоколов маршрутизации (OSPF, IS-IS, EIGRP, BGP);
3) возможна передача мультимедийных данных (данных, голосовых и видеосообщений) в пределах единой IP сети;
4) внедрены механизмы обеспечения качества обслуживания (QoS), которые позволяют приоритетное обслуживание более важных приложений;
5) включены средства комбинированного обеспечения безопасности (межсетевого защитного экрана, системы обнаружения вторжений и VPN-концентратора), что позволяет во многих случаях использовать вместо нескольких отдельных устройств безопасности одно устройство под управлением Cisco IOS;
6) поддерживается стандарт мобильного интернета (Mobile IP), позволяющий пользователю сохранить один и тот же IP адрес при перемещении его из одной сети в другую;
7) введена многоадресная рассылка (IP multicast) для одновременной передачи группе маршрутизаторов или хостов служебной информации или мультимедийных типов данных многочисленным пользователям;

8) включены разнообразные средства управления, позволяющие осуществлять удаленную настройку параметров сети, а также контроль производительности сети, измерение пропускной способности на ее отдельных участках, количество потерянных пакетов, времени задержки передачи пакетов и пр.

5.4.2. Интерфейс командной строки

В качестве интерфейса для конфигурирования оборудования и администрирования сети в системе Cisco IOS используется базовый интерпретатор командной строки CLI (*Command-Line Interface*). Существует несколько способов получения доступа к командной строке устройства:

- посредством консольного порта;
- посредством службы Telnet или SSH;
- через AUX-порт.

Доступ через низкоскоростной консольный порт служит для начальной настройки коммутатора или маршрутизатора, когда сетевые параметры устройства ещё не настроены. Для этого применяется специальный кабель и программа-эмулятор виртуального терминала. Консольный порт доступен всегда, даже если сетевые службы не функционируют. Помимо стартовой настройки системы, его используют в случае отказа сети или поиска неисправности, когда невозможно удалённо получить доступ к устройству, а также для процедуры восстановления забытого пароля. Вход через консольный порт следует защитить паролем, чтобы избежать несанкционированного доступа к устройству. Для восстановления утерянного пароля существует специальный набор процедур, позволяющий его восстановить.

Доступ к интерфейсу командной строки CLI через AUX-порт, также как и доступ через консольный порт, не требует предварительного конфигурирования сетевых служб коммуникационного устройства. Обычно он использовался при возможности установлении модемной связи по коммутируемым каналам телефонной сети общего пользования. Вход через AUX-порт может быть осуществлён и локально посредством прямого подключения компьютера с применением программы эмулятора терминала. Однако, по причине ряда ограничений, этот способ применяется только в случае отсутствия возможности использовать консольный порт, например, если неизвестны параметры консольного соединения.

Чтобы получить удалённый доступ к CLI используют протоколы Telnet или SSH (*Secure Shell*). Для успешного подключения необходимо, чтобы хотя бы один интерфейс был в рабочем состоянии, и ему был назначен IP-адрес. Сетевая операционная система содержит Telnet сервер, стартующий при загрузке устройства, и Telnet клиент. Однако, протокол Telnet не дает возможности защитить доступ к CLI с помощью пароля, а сам пароль

передаётся через сеть в открытом виде и может быть легко перехвачен. Поэтому рекомендуется вместо Telnet применять SSH. Служба SSH обеспечивает более строгий процесс аутентификации, трафик, передаваемый с помощью этого протокола, шифруется. С клиентских станций SSH соединение устанавливается с использованием SSH клиентов, присутствующих по умолчанию или специально установленных. Большинство новейших версий IOS включает в себя SSH сервер, включенный по умолчанию. IOS содержит также клиент SSH, позволяющий установить SSH соединение с другими устройствами. Особенности конфигурирования коммутаторов Catalyst для различных операционных систем подробно освещены в [29,32].

При попытке войти в систему конфигурирования (log in) коммутатора Catalyst пользователю предлагается ввести пароль. При вводе правильного пароля пользователь попадает в режим конфигурации коммутатора Catalyst в ***пользовательском*** режиме. В данном режиме пользователь имеет право просматривать большинство параметров конфигурации коммутатора Catalyst, однако у него отсутствует право для внесения изменений в конфигурацию.

Если пользователю нужно внести изменения в конфигурацию, он должен войти в ***привилегированный*** режим работы с коммутатором Catalyst. В привилегированном режиме пользователь имеет право просматривать конфигурацию и вносить в нее изменения. В этом режиме пользователю предоставляется право вводить и испольнять любые команды.Для входа в данный режим необходимо выполнить команду **`enable`**. Возврат в пользовательский режим осуществляется путем ввода команды **`disable`** или **`exit`**.

Схема переключения режимов коммутатора показана на рисунке 5.4.

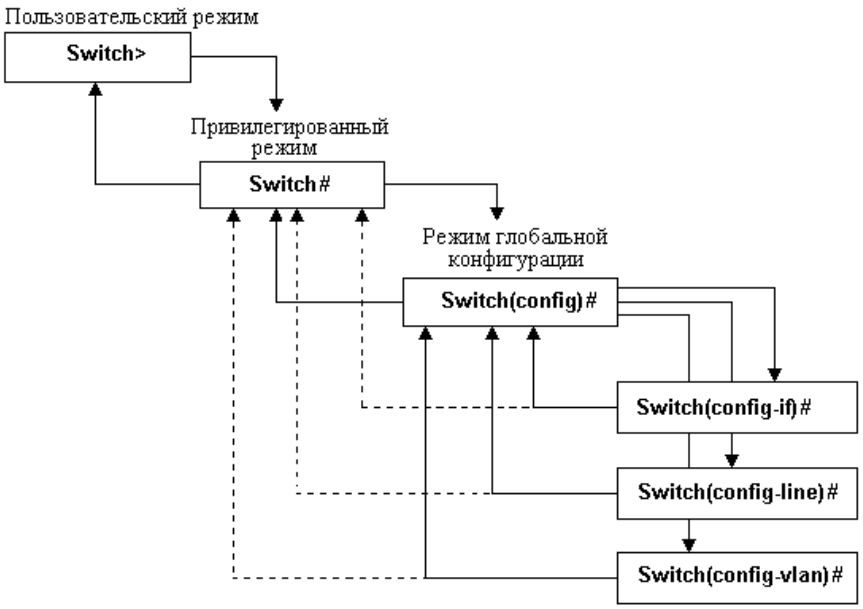


Рисунок 5.4 – Схема переключения режимов коммутатора

Для начала работы и в пользовательском и в привилегированном режиме операционная система может потребовать ввести пароли соответствующих уровней. Настройка параметров интерфейсов коммутатора и других функций выполняется в режиме глобальной конфигурации. В этом режиме администратору предоставляются команды, оказывающие влияние на коммутатор в целом. Из этого режима возможен переход в более конкретный уровень конфигурации отдельных ресурсов устройства. Способы перехода на эти специфические уровни будут рассмотрены ниже. Возврат из специфического уровня на более общий осуществляется путем исполнения команды **exit**. Для выхода из любого режима и возврата в привилегированный режим применяется команда **end** или комбинация клавиш <Ctrl>+<z>. Команды управления коммутатором могут вводиться из любого режима: привилегированного, глобальной конфигурации, конфигурации интерфейса и подинтерфейса, конфигурирования базы данных виртуальных сетей и т.д. Для запуска какой-либо функции коммутатора нужно ввести с клавиатуры команду и ее параметры. Для отключения команды следует ввести ключевое слово **no** и за ним идентификатор команды.

Текущие настройки коммутатора можно посмотреть в привилегированном режиме с помощью команды `show running-config`. Команды и параметры можно вводит в сокращенном виде, состоящих из одной или нескольких начальных букв.

5.4.3. Краткая характеристика команд коммутаторов Catalyst с операционной системой Cisco IOS

Все доступные команды управления коммутаторами могут показаны в любом режиме работы путем ввода в командную строку вопросительного знака ? После ввода знака ? нажатие клавиши ВВОД не требуется. Например, для коммутатора **Cisco3560** результат будет следующим:

```
Cisco3560#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Cisco3560(config)#?
Configure commands:
aaa       Authentication, Authorization and Accounting.
access-list     Add an access list entry
alias           Create command alias
```

Если при вводе команды не ясно, какие могут быть другие команды, необходимо ввести соответствующую команду с пробелом и ?. В результате будут показаны все возможные варианты:

```
Cisco3560#configure ?
memory              Configure from NV memory
network             Configure from a TFTP network host
overwrite-network   Overwrite NV memory from TFTP network host
terminal            Configure from the terminal
Cisco3560#configure
```

Имеется также возможность завершить команду после ввода одного или нескольких начальных символов путем нажатия клавиши табуляции, если сокращение не является двусмысленным.

```
Cisco3560#configure n <TAB>
Cisco3560#configure network
```

Как упоминалось выше, пользователь может вводить команды только в привилегированном (**enable**) режиме настройки коммутатора. Привилегированный режим легко распознается по наличию значка # в командной строке. Просмотр текущей конфигурации коммутатора может быть произведен путем ввода следующей команды:

```
Cisco3560#show running-config
```

Для сохранения текущей конфигурации в энергонезависимой памяти NVRAM нужно ввести команду:

```
Cisco3560#copy running-config startup-config
```

В результате выполнения этой команды все настройки параметров коммутатора переносятся из оперативной памяти (RAM) в ПЗУ (NVRAM). Если по каким-то причинам стартовая конфигурация должна быть заменена установками текущей конфигурации, то следует развернуть команду наоборот:

```
Cisco3560#copy startup-config running-config
```

Для конфигурации интерфейса необходимо сначала переключиться в режим ***глобальной конфигурации***. Для этого применяется команда **configure terminal.** В результате в командной строке появится индикатор глобального режима **(config)#,** как это показано ниже.

```
Switch#configure terminal
Switch(config)#
```

В этом режиме можно, например, задать имя коммутатора, например Cisco3560

```
Switch(config)# hostname <Cisco3560>
```

указать ключевое слово (пароль) для привилегированного режима,

```
Cisco3560(config)#
enable secret <Ключевое слово>
```

или активировать IP–маршрутизацию:

```
Cisco3560(config)# ip routing .
```

Коммутаторы Catalyst располагают различными типами интерфейсов. При этом существует различие между интерфейсами для локальных (LAN) и глобальных (WAN) сетей. Каждому интерфейсу соответствует один или несколько физических портов коммутатора. Все интерфейсы различаются по:

- типу (Fast-Ethernet для сетей 10/100-Ethernet, Serial или bri для глобальных сетей);
- принадлежности к модулю (слоту); для некоторых коммутаторов имеется только модуль 0;
- номеру порта (начиная с номера 1 и т.д.);

например, `fastethernet 0/1, gigabitethernet 0/1, serial0/4, bri0/2.`

Чтобы конфигурировать интерфейс необходимо сначала переключиться режим глобальной конфигурации. После этого становится возможным задания команд соответствующим интерфейсам, например

```
Switch#configure terminal
Switch(config)# interface bri0
Switch(config-if)#encapsulation ppp
Switch(config-if)#exit
Switch(config)#   .
```

Коммутаторам 2-го уровня могут быть присвоены IP-адреса, которые используются *только с целью администрирования*. Благодаря этому коммутатором можно управлять с удаленного терминала. IP-адреса могут быть установлены или получены с помощью протокола динамического конфигурирования узла DHCP (*Dynamic Host Configuration Protocol*), протокола начальной загрузки BOOTP (BOOT*strap Protocol*) или протокола обратного преобразования адресов RARP (*Reverse Address Resolution Protocol*). Коммутаторы Catalyst также могут иметь активный административный адрес (*management address*) в одной виртуальной сети VLAN. Стандартной административной сетью IOS-коммутаторов, может быть только одна виртуальная сеть. Ею является сеть VLAN 1. Данная процедура не является обязательной для функционирования коммутатора. В случае, если IP-адрес не был задан, единственным способом управления коммутатором является консольное соединение.

Конфигурирование IP-адреса (необязательный этап, но рекомендуется его выполнять). Конфигурирование IP-адреса вручную производится путем задания команд:

```
Switch(config)# interface Vlan Vlan_number
!-- режим глобальной конфигурации
Switch(config-if)# ip address address mask
!-- режим конфигурирования интерфейса или подынтерфейса
Switch(config-if)#
```

5.5. Общая характеристика коммутаторов Cisco Catalyst

Корпорацией Cisco Systems™ разработаны сетевые коммутаторы для различных коммуникационных потребностей и условий эксплуатации [15, 29]. Некоторые модели предназначены для работы в сложных производственных условиях машиностроительных и металлургических предприятий при наличии сильной вибрации, резких колебаний температуры, повышенной загазованности и воздействия других неблагоприятных факторов. Другие модели обеспечивают предоставление сетевых услуг в отраслях, в которых выдвигаются специальные требования к кабельным соединениям. К ним относится, в частности, розничная торговля (точки продаж, киоски, контрольно-кассовые пункты, склады), сфера образования (классные комнаты, общежития, лаборатории), медицина (кабинет врача, приемное отделение больницы, кабинет для обследования пациентов, лаборатория), гостиничный бизнес и индустрия развлечений (гостиничный номер, каюта круизного лайнера, конференц-зал, игровые заведения), а также офисная среда.

Особенностью коммутаторов новых серий (например, Cisco C-Series) является повышенная защищенность пользовательских услуг, включая унифицированные коммуникации, беспроводной доступ, IP-видео и другие приложения, в среде с ограниченными возможностями кабельных соединений, небольшим рабочим пространством и недостаточными энергетическими мощностями. Компанией Cisco одной из первых в отрасли реализованы функции PoE (*Power over Ethernet*) — подачи электропитания по каналам Ethernet, позволяющие коммутаторам Cisco C-Series работать в среде, где отсутствуют розетки электрических сетей. Эти функции радикальным образом упрощают кабельную разводку и снижают уровень инфраструктурных требований.

Для сопряжения коммутаторов с различными видами среды передачи сигналов в них предусмотрена установка преобразователей (конвертеров) сигналов. В настоящее время в коммутаторах применяются несколько типов конвертеров. **Конвертер гигабитных интерфейсов GBIC** (*Gigabit Interface Convertек*) является промышленным стандартом трансиверов, поддерживающих режим горячей замены. С помощью разных модулей GBIC осуществляется подключение сетевых устройств к разным видам среды передачи (медная пара или оптоволокно). Для мониторинга параметров GBIC-модулей

используется функция системы диагностики DDM (*Digital Diagnostic Monitoring*). Эта функция также известна как цифровой оптический контроль DOM (*Digital Optical Monitoring*). Данная функция позволяет контролировать такие параметры GBIC-модулей, как мощность входящего сигнала (Rx) и исходящего сигнала (Tx), температуру контрольных точек модуля. Стандартные модули GBIC работают со скоростью от 1 до 1,25 Гбит/с в дуплексном режиме, в диапазоне оптических волн длиной 850, 1310 и 1550 нм и обеспечивают связь на расстоянии до 100 км.

Взамен более громоздких модулей GBIC разработаны более современные интерфейсные модули типа SFP (*Small Form factor Pluggable module*). **Модули SFP** используются для присоединения платы сетевого устройства (коммутатора или маршрутизатора) к оптическому волокну или неэкранированной витой паре, выступающих в роли среды передачи. Модуль имеет разъём, сопоставимый по размеру с разъёмом типа 8P8C (RJ-45), что позволяет на одном 1U-модуле 19-дюймового телекоммуникационного шкафа разместить до 48 оптических портов. Для подключения модуля к среде используется в основном оптический кабель, терминированный (оконцованный) разъемом типа LC (см. рисунок 1.13). В процессе эксплуатации допускается «горячая» замена модуля, без выключения электропитания оборудования (функция *hot-swap*).

Различные типы модулей SFP могут преобразовывать сигналы информационных потоков сетей: 100 Мбит Ethernet; 1Гбит Ethernet; 2Гбит Fiber Channel; 4Гбит Fiber Channel; STM4 или STM16. SFP модули выпускаются в вариантах с различными комбинациями приёмника (Rx) и передатчика (Tx), что позволяет выбрать необходимую комбинацию для заданного соединения, исходя из используемого типа оптоволоконного кабеля: многомодового (MM) или одномодового (SM). Некоторые производители выпускают универсальные SFP-модули, которые способны транспортировать как 100 Мбит Ethernet, 1 Гбит Ethernet, так и потоки синхронной цифровой иерархии STM4 и STM16.

Для использования в 10Gbit сетях появился новый формат интерфейсных модулей типа XFP, который отличается большими габаритами, но при этом использует тот же тип оптического разъема LC.

В коммутаторах Cisco новых моделей упрощена их настройка и унифицировано сетевое управление. Так, начальная настройка коммутаторов Cisco C-Series осуществляется с помощью функции Cisco Catalyst Smart Operations, не требующей вмешательства оператора. Кроме того, эта функция значительно ускоряет процессы диагностики сети. Благодаря функции Cisco Auto Smartports осуществляется автоматическая настройка конфигурации коммутатора в зависимости от типов подключенных к нему устройств. Автоматическая поддержка качества услуг (QoS) позволяет реализовать самые современные функции IP-телефонии и видео с помощью всего лишь одной

команды. Уникальное качество услуг Cisco гарантирует непрерывность качественной передачи голоса и видео даже при высоких объемах сетевого трафика. Коммутаторами Cisco C-Series можно управлять в удаленном режиме вместе с устройствами, установленными в распределительном шкафу, что существенно сокращает стоимость установки и управления.

В коммутаторах Cisco обеспечивается очень высокий уровень безопасности. В них реализована защита удаленных устройств от несанкционированного доступа, подслушивания и кражи. Все пакеты в канале между коммутатором и оконечными устройствами шифруются. Поддерживаются жесткие правила информационной безопасности с применением пользовательских идентификаторов, учетом должностных обязанностей и типов устройств. В результате пользователи получают возможность безопасной и гибкой совместной работы в любой точке сети.

Коммутаторы Cisco C-Series поддерживают спецификации стандарта безопасности для карточных платежей PCI SSC (*Payment Card Industry Security Standards Council*), что позволяет выполнять все нормативные требования платежных систем. Все современные коммутаторы включают средства подачи питания на удаленные устройства через порты Ethernet PoE (15,4 Вт на порт) и PoE+ (20 Вт на порт).

В соответствии с трехуровневой иерархической моделью локальной сети (рисунок 1.4) коммутаторы по функциональному назначению подразделяются коммутаторы уровня доступа, уровня распределения и уровня ядра. На различных этапах развития микропроцессорной техники, технологии производства коммутаторов и программного обеспечения, производители коммуникационной техники выпускают множество моделей коммутаторов для использования их на всех трех уровнях. С течением времени на смену устаревшим моделям приходят новые, обладающие более высокой производительностью, новыми функциональными возможностями, потребляющие меньше энергии. Поэтому при проектировании компьютерной сети необходимо использовать современные перспективные устройства, которые оправдают инвестиции в ее создание за счет увеличения срока службы инфраструктуры. Ниже рассмотрены функциональные возможности и основные технические параметры современных на момент написания книги коммутаторов корпорации Cisco.

5.5.1. Коммутаторы уровня доступа

Для подключения небольших рабочих групп Ethernet, Fast Ethernet и серверов, простого и недорогого построения сети на основе витых пар со скоростью передачи 100 Мбит/с предназначены 8-портовые коммутаторы Fast Ethernet CatalystR 2908 XL 10/100, которые характеризуются высокой

производительностью, простотой управления и относительно невысокой ценой.

Улучшенная архитектура коммутаторов содержит в себе оборудование с производительностью 3,2 Гбит/с и скоростью коммутации до 1,19 миллионов пакетов в секунду, обеспечивая независимую работу всех портов на максимальной скорости. Коммутатор Catalyst 2908 XL имеет возможность простого управления на базе Web-интерфейса и дополнительные возможности обеспечения безопасности. Web-интерфейс позволяет управлять коммутатором из любого места сети, используя стандартный клиент Web, такие как Microsoft Explorer, Netscape Navigator и др. Многоуровневая система безопасности доступа к консоли исключает доступ неавторизованных пользователей к конфигурации коммутатора. Автоматический конфигуратор позволяет настроить несколько коммутаторов с одного загрузочного сервера.

Для подключения на уровне доступа большего количества пользователей целесообразно использовать коммутаторы серии Cisco ME 2400, которые кроме 24-х 10/100 Ethernet портов имеют два восходящих порта для подключения малогабаритных медиаконверторов SFP (*Small Form factor Pluggable module*). Ethernet-коммутаторы доступа Cisco ME серии 2400 (Cisco ME 2400 Series Ethernet Access Switch) хорошо подходят для организации популярных услуг Triple Play (доступ в Интернет, IP-телефония и IP-телевидение). Эти коммутаторы относятся к устройствам уровня L2 модели OSI. Кроме широких функциональных возможностей коммутаторов они отличаются компактность исполнения, все разъемы располагаются на передней панели, что упрощает доступ при поиске неисправностей на месте. Коммутаторы могут быть запитаны как от сети переменного тока (ME 2400-24TS-24 AC), так и постоянного (ME 2400-24TS-24 DC). Представителем стекируемых коммутаторов уровня доступа являются устройства L2-уровня типа Cisco Catalyst 2960-S. Они имеют 24/48 портов 10/100/1000 Мбит/с с фиксированными портами каскадирования: 4x1G или 2x10G SFP+. Для возможности объединения в стек в них установлены 20Gbit каналы стекирования.

Перспективными устройствами для сетей малых офисов являются компактные коммутаторы второго поколения Catalyst серий 2960-C и 3560-C. Они имеют от 8 до 12 портов 10/100 Ethernet или 8 портов 10/100/1000 Ethernet с двумя портами 1GE uplinks. Это первые промышленные коммутаторы со сквозной технологией электропитания по каналам Ethernet.

Для использования на уровне доступа крупных локальных сетей предприятий и организаций, удаленных офисов и небольших компаний разработаны многоуровневые коммутаторы серии Cisco 3750. Они могут применяться как в составе стека, так и в качестве отдельных устройств. Многие модели этой серии устройств, позволяют использовать коммутаторы Cisco 3750 не только на уровне доступа, но и для агрегирования трафика на уровне распределения, а также для магистральных соединений сетей компаний среднего

масштаба. Существует возможность объединить в стек до 9 устройств Catalyst 3750, которые будут функционировать как один логический коммутатор. При этом можно получить до 468 портов 10/100TX или до 252 портов 10/100/1000T, добавляя новые коммутаторы в стек по мере необходимости. Пропускная способность шины стека составляет 32 Гбит/с.

5.5.2. Коммутаторы уровня распределения

В качестве коммутаторов уровня распределения целесообразно применять коммутаторы серий Catalyst 3750-X и 3560-X, функционирующих на уровнях L2 и L3 модели OSI [29,36-39]. Они обеспечивает не только все функции LAN, но и высокопроизводительную маршрутизацию трафика IP и имеет аппаратную поддержку маршрутизации IPv6. Поддерживается большинство протоколов маршрутизации – RIPv1, RIPv2, OSPF, IGRP, EIGRP, BGPv4. Коммутаторы содержат 24 или 48 портов Gigabit Ethernet и могут объединяться в стек. Некоторые модели коммутаторов этого семейства позволяют осуществлять агрегацию оптических каналов. Коммутаторы данного семейства могут быть использованы и на уровне доступа.

К семейству доступных по цене управляемых коммутаторов, предназначенных для малых предприятий и в качестве этажных коммутаторов на предприятиях среднего размера, относятся коммутаторы серии Cisco 300 — часть линейки сетевых решений *Cisco Small Business*. Эти коммутаторы обладают большим набором функций, обеспечивающим повышение производительности, сетевой безопасности и удобство работы в сети. В коммутаторах Cisco 300 установлено больше портов Gigabit Ethernet на коммутатор, чем в традиционных устройствах. Так модели Gigabit Ethernet представлены коммутаторами с 28 и 52 портами. В серия 300 также имеются слоты расширения типа мини-GBIC, позволяющие подключать к коммутатору дополнительные оптоволоконные восходящие каналы или каналы Gigabit Ethernet. Промышленность также предлагает модели с 8…48 портами Fast Ethernet и 10…52 портами Gigabit Ethernet.

В коммутаторах включена схема подачи электропитания по сети Ethernet (PoE) на 48 портах Fast Ethernet и портах Gigabit Ethernet. Кроме этого использована технология сокращение энергопотребления EEE (*Energy Efficient Ethernet*), в соответствии с которой производится отслеживание трафика и перевод каналов в спящий режим, когда передача данных отсутствует или порты не используются. Коммутаторы позволяют задавать списки управления доступом и создавать виртуальные локальные сети VLAN. В устройствах Cisco 300 реализована поддержка протокола IPv6, что позволяет использовать сетевые приложения и операционные системы нового поколения, не проводя массовой модернизации оборудования.

В коммутаторах используется система управления качеством обслуживания QoS, реализованная во всех моделях, задает приоритеты передаваемых по сети данных для обеспечения максимальной производительности наиболее важных сетевых приложений. Средства статической маршрутизации/IP-маршрутизации третьего уровня обеспечивают передачу данных между сетями VLAN без снижения производительности приложений.

Коммутаторы семейства **Cisco Catalyst Express 500** являются программно управляемыми устройствами 2-го уровня и предназначены для создания сетей организаций с количеством сотрудников до 250. В состав серии входит несколько типов коммутаторов с количеством портов от 8 (модель WS-CE500G-12TC) до 48 портов 10/100/1000Base-T (модель ESW-520-48-K9). Практически все модели снабжены несколькими слотами для медиаконвертеров типа SFP. Для централизованного управления коммутаторами Catalyst Express 500 разработано специальное программное приложение Cisco Network Assistant, существенно упрощающее администрирование коммутаторов. В его состав входит мастер настройки, который значительно облегчает реализацию сетей и интеллектуальных сетевых сервисов.

5.5.3. Коммутаторы уровня ядра

Для работы на уровне ядра (магистрали) корпорация Cisco производит в настоящее время несколько семейств коммутаторов второго, третьего и четвертого уровней модели OSI. К ним относятся семейства коммутаторов Cisco Catalyst 4500-X/4500-E, 6500/6807-XL, 6880-X и др. В этих коммутаторах реализована поддержка протокола безопасности 802.1x, списков доступа для трафика, коммутируемого на втором уровне (VLAN ACL), на третьем и четвертом уровнях (Router ACL), а также списки доступа на основе портов PACL (*Port-based ACLs*). Для обеспечения безопасности при администрировании поддерживаются протоколы SSH и SNMPv3, а также централизованная аутентификация на TACACS+ и RADIUS серверах. В коммутаторах осуществляется поддержка качества обслуживания (QoS), в частности, по классу дифференциального обслуживания (поле DSCP заголовка IP-пакета) или класса обслуживания (поле CoS заголовка кадра канального уровня), а также по исходным и конечным MAC-, IP-адресам или портам TCP/UDP. Также реализована приоритетная очередность, ограничение полосы пропускания, гарантированная полоса пропускания CIR (*Committed Information Rate*) и функция AutoQoS. Поддерживается большинство протоколов маршрутизации – RIPv1, RIPv2, OSPF, IGRP, EIGRP, BGPv4 и др.

Коммутаторы типа **Cisco Catalyst 4500-E** поддерживают базовый набор функций для уровней ядра и распределения. Они также могут совмещать функции уровня доступа и распределения. Из всех коммутаторов уров-

ня ядра они являются наиболее дешевыми. В различной комплектации коммутаторы содержат от 16 до 40 гигабитовых портов (10G/1G). Общая пропускная способность коммутаторов достигает 800 Гбит/с. Коммутаторы также могут осуществлять маршрутизацию сетевых пакетов по протоколам IPv4 и IPv6.

Коммутаторы семейства Cisco Catalyst 4500 поддерживают подключение к рабочим станциям линейных карт следующих типов:

- *Fast Ethernet over Fiber* – линейные карты, обеспечивающие соединение на скорости 100 Мбит/с по волоконно-оптическому кабелю;
- *Fast Ethernet over Copper* – линейные карты, позволяющие осуществлять передачу данных по медному кабелю со скоростью 100 Мбит/с;
- *Fast Ethernet Pover over Ethernet* – линейные карты, обеспечивающие соединение на скорости 100 Мбит/с с поддержкой технологии передачи электрической энергии по сетям Ethernet (PoE);
- *Gigabit Ethernet* (GBIC or SFP) – линейные карты, обеспечивающие соединение на скорости 1Гбит/с при помощи стандартных GBIC-трансиверов или портов SFP;
- *Gigabit Ethernet over Copper* – линейные карты, позволяющие передавать данные по медному кабелю со скоростью 1Гбит/с;
- *Gigabit Ethernet over Copper with Power over Ethernet* – линейные карты с возможностью передачи данных со скоростью до 1Гбит/с и поддержкой технологии PoE.

Каждая из линейных карт содержит от 24 до 48 портов со скоростями передачи 10/100/1000 Мбит/с или 18 портов типа 1000BASE-X GBIC.

Семейство коммутаторов Cisco Catalyst 6500 представляет собой серию высокопроизводительных модульных коммутаторов, работающих от 2-го до 7 уровня эталонной модели OSI. Коммутаторы Catalyst 6500 целесообразно применять в сетях крупных предприятий, операторов связи, городских сетях, а также в сетях распределенных вычислений. В зависимости от комплектации Catalyst 6500 могут быть установлены на различных уровнях сетевой иерархии: доступа, распределения и ядра (магистрали).

Устройства Catalyst 6500 обеспечивают масштабируемую производительность (до 720 Гбит/с) и высокую плотность портов (до 576 портов Gigabit Ethernet или 32 портов 10 Gigabit Ethernet). Коммутаторы Catalyst 6500 выполняют маршрутизацию трафика на скоростях до 400 млн. пакетов в секунду. При этом поддерживается аппаратная маршрутизация трафика протоколов IPv4 и IPv6 (протоколы маршрутизации RIP, OSPF, IS-IS, EIRGP, BGP4, MBGP и т. д.), аппаратная реализация функциональности MPLS, а также NAT и GRE. Поддерживается маршрутизация трафика протоколов IPX, AppleTalk и др. Широкий ассортимент сменных модулей позволяет подключать Catalyst 6500 практически к любым каналам локальных и глобальных сетей, в частности: 10 Gigabit Ethernet (LR, ER), Gigabit Ethernet

(SX, LX/LH), Fast Ethernet (TX, FX), Ethernet (FL), CWDM, ATM, T1/E1, T3/E3 и др.

Коммутаторы **Cisco Catalyst 6800** специально разработаны для соединения кампусных сетей с передачей по магистральным линиям со скоростями 10, 40 и 100 Гбит/с. Они обеспечивает совместимость с широко используемыми коммутаторами семейства Catalyst 6500.

Корпорацией Cisco также разработан модульный коммутатор Catalyst 6807-XL, предназначенный для кампусных магистралей нового поколения, который оптимизирован для скоростей 10/40/100 Гбит/с. Catalyst 6807-XL размещается в модульном шасси с 7 слотами, со скоростью передачи до 880 Гбит/с на слот.

Для предприятий среднего размера выпускается коммутатор **Cisco Catalyst 6880-X**. Он имеет корпус с 3 слотами, супервайзером с 16 фиксированными портами на скорость 10 Гбит/с каждый и 4 полуслотами для установки опционных линейных карт 10 Гбит/с или 40 Гбит/с, поддерживающими до 80 портов 10 Гбит/с или 20 портов 40 Гбит/с. Коммутаторы Cisco Catalyst 6880-X являются частью семейства 6800. Устройства наследовали полный функционал от семейства коммутаторов 6500 и могут работать на скоростях 40G/100G. Они снабжаются 4 слотами для интерфейсных модулей. В коммутаторе может быть установлено до 80 1/10G-портов или двадцати 40G-портов. Общая производительность коммутатора равна 2Тбит/с.

5.5.4. Мультисервисные коммутаторы

Серия мультисервисных маршрутизирующих коммутаторов Catalyst 8500 обеспечивает интеграцию коммутации ATM с мультипротокольной маршрутизацией и коммутацией на втором уровне в рамках одной платформы. При этом обеспечивается поддержка многочисленных функциональных свойств программного обеспечения операционной системы Cisco IOS для управления качеством обслуживания и безопасности. Серию Catalyst 8500 целесообразно применять в компьютерных сетях масштаба города или кампуса для обеспечения масштабируемой производительности, высокой управляемости и экономической эффективности. Эти устройства обладают всеми функциональными возможностями, необходимыми для современных сетей, базирующихся на технологиях Интранет и Интернет. Одновременная поддержка технологий Fast Ethernet/Gigabit Ethernet, ATM и высокоскоростной мультипротокольной маршрутизации дает возможность применять перечисленные технологии в рамках единой сети, используя преимущества каждой из них. Это также упрощает процесс перехода от одной сетевой технологии к другой по мере изменений требований к функциональным свойствам и пропускной способности сети. Благодаря высокой производительно-

сти, наличию удобных средств управляения и механизмов контроля за трафиком, коммутаторы серии Catalyst 8500 позволяют интегрировать их с коммутаторами Catalyst 5500, маршрутизаторами серий Cisco 7500/7200, коммутаторами ATM, а также мультисервисными устройствами различных типов.

В коммутаторах данного семейства Catalyst 8510 и Catalyst 8540 применена высокопроизводительная коммутирующая архитектура со скоростями передачи соответственно 10 Гбит/с и 40 Гбит/с, в результате чего коммутация пакетов IP, IPX, IP-multicast трафика повысилась до 6 и 24 миллионов пакетов в секунду для Catalyst 8510 и Catalyst 8540 соответственно. В коммутаторах осуществляется поддержка протоколов маршрутизации ПО IOS, включая OSPF, IGRP, EIGRP, RIP, RIP2, в том числе RIP и EIGRP для IPX, планируется внедрения поддержки протоколов маршрутизации BGP и NLSP. Расширенные средства безопасности ПО IOS, включая поддержку протоколов TACACS+, RADIUS, Kerberos, технологии Lock and Key и шифрование MD5. В коммутаторах предусмотрена балансировка нагрузки на третьем уровне между несколькими сетевыми путями, технологии Fast и Gigabit EtherChannel для балансировки на втором уровне.

Дальнейшим развитием коммутаторов семейства Catalyst 8500 явились коммутирующие маршрутизаторы Catalyst 8500 CSR, представляющих собой новый класс специализированных коммутирующих маршрутизаторов, имеющих неблокирующую архитектуру, предотвращающую потерю пакетов даже в моменты максимальной загрузки.

Интегрированные возможности коммутации ATM делают Catalyst 8500 CSR единой промышленной платформой, способной воплотить в себе возможности интеграции данных, голосового и видео трафика. Масштабируемость Catalyst 8500 CSR сочетается с расширенными функциями управления качеством сервиса QoS, которые были разработаны для предотвращения потерь данных и использования новых мультимедиа приложений, чувствительных к временным задержкам.

5.6. Общая характеристика коммутаторов D-Link

5.6.1. Состав и обозначение коммутаторов D-Link

Коммуникационное оборудование корпорации D-Link, благодаря своей относительно невысокой стоимости и широкому спектру функциональных возможностей, широко применяется в бюджетных сетях. Выпускаемые промышленностью коммутаторы D-Link ориентированы на работу любого из трех уровней иерархической модели локальной сети (рисунок 1.4). Следует также отметить удачную систему обозначений коммуникационных

устройств D-Link, которая позволяет по названию определить тип, назначение и особенность исполнения коммутатора или другого изделия. Обозначение каждого коммутатора содержит три части [11].

Первая часть обозначения состоит их трех букв. Начальная буква обозначает производителя устройства — D-Link. Вторая отображает особенности сетевой технологии, а третья является сокращением от слова коммутатор (*Switch*) или модуль (*Module*). В настоящее время имеются следующие виды обозначений:

- DES (*D-Link Ethernet Switch*) — это коммутаторы или модули для коммутаторов D-Link для сети Ethernet со скоростью передачи 10/100 Мбит/с; в таких коммутаторах могут присутствовать порты со скоростью передачи 1000 Мбит/с;
- DGS (*D-Link Gigabit Switch*) — коммутаторы D-Link со скоростью передачи 1000 Мбит/с или модули к ним; в таких коммутаторах могут присутствовать порты со скоростью передачи 5 или 10 Гбит/с;
- DXS (*D-Link X-Stack Switch*) — коммутаторы D-Link со скоростью передачи 1 или 10 Гбит/с или модули к ним; в таких коммутаторах могут присутствовать порты со скоростью передачи 10, 40 или 120 Гбит/с;
- DWS (*D-Link Wireless Switch*) — коммутаторы D-Link, выступающие в качестве контроллеров беспроводных сетей;
- DEM (*D-Link Ethernet Module*) — дополнительные модули или трансиверы для коммутаторов;
- DEM-CB (*D-Link Ethernet Module — CaBle*) – дополнительные кабели для коммутаторов;
- DPS (*D-Link Power Switch*) — резервные источники питания для коммутаторов.

Вторая часть обозначения состоит из 4-х или 6-ти цифр. Последние две цифры отображают суммарное количество портов коммутатора. Если коммутатор является модульным, то последние две цифры указывают на количество слотов в шасси. Первые две или четыре цифры обозначают класс управляемости коммутатора.

Третья часть обозначения отображает особенность исполнения коммутатора, например:

- G, TG или SC свидетельствует о том, что большинство портов коммутатора являются оптическими;
- T, TX, TP или TC говорит о том, что большинство портов коммутатора предназначены для подключения медных линий связи. Также, о том, что большинство портов предназначены для медных линий, говорит отсутствие букв в конце названия коммутатора;
- P или PC обозначает, что некоторые или все порты коммутатора поддерживают функцию PoE;

- ME говорит о том, что коммутаторы ориентированы на использование в городских сетях (*Metro Ethernet*).

К сожалению, в последних моделях коммутаторов наблюдается отклонение от ранее принятой системы обозначений.

Разработчики коммутаторов D-Link подразделяют их по возможности управления на три класса.

1. **Неуправляемые коммутаторы** (*Unmanaged Switches*) функции управления и настройки не поддерживают. Примером этого класса устройств являются коммутаторы серий DES-10xx и DGS-10xxD/GE. Коммутаторы серий DGS-10xxD/RU и DGS-10xxD/GE поддерживают энергосберегающую технологию *Green Ethernet*. Эта энергосберегающая технология позволяет сократить расходы на электроэнергию, не оказывая при этом влияния на производительность и функциональность устройств.

2. **Настраиваемые коммутаторы** (*Smart Switches*) занимают промежуточную позицию между ними. Эти коммутаторы позволяют выполнять настройку определенных параметров (изменять режимы работы портов, создавать виртуальные сети, объединять порты в группы), но не поддерживают удаленное управление по протоколам SNMP и Telnet. Примером таких коммутаторов являются DES-12xx, DGS-12xx и DES-1210-xx. Коммутаторы серии *Smart* поддерживают функции обеспечения отказоустойчивости, безопасности, сегментации сети, качества обслуживания, мониторинга трафика и диагностики кабеля. Управление коммутаторами может осуществляться через Web-интерфейс, утилиту *SmartConsole*, упрощенный интерфейс командной строки и протокол SNMP. Помимо этого, коммутаторы серии DGS-1210-xx поддерживают технологию *Green Ethernet* и *Jumbo*-фреймы.

3. **Управляемые коммутаторы** (*Managed Switches*) по сравнению с неуправляемыми коммутаторами и коммутаторами серии *Smart* являются сложными устройствами, поддерживающими расширенный набор функций 2 и 3 уровня модели OSI. Такие устройства предоставляют большой выбор интерфейсов, обладают высокоскоростной внутренней магистралью, возможностью установки дополнительных модулей и физического стекирования. Управление коммутаторами может осуществляться посредством Web-интерфейса, с командной строки (CLI), протокола SNMP, Telnet и др. К этому классу относятся, в частности, коммутаторы D-Link 2-го уровня (L2) DES-1210-28ME, DES-1228ME, DES-2108, DES-30xx, DGS-30xx, DES-32xx, DGS-32xx, DGS-34xx, DGS-3420, DES-35xx, DGS-37xx и коммутаторы 3-го уровня (L3) DES-33xx, DGS-33xx, DXS-33xx, DGS-36xx, DXS-3600, DGS-3610, DGS-3620, DES-38xx, DES-3810, DES-63xx, DES-65xx, DGS-6600, DES-72xx.

В качестве коммутаторов **уровня доступа** для малых предприятий и отдельных офисов целесообразно использовать неуправляемые коммутаторы с количеством портов от 8 до 24 в настольном и стоечном исполнении. К

ним относятся модели **DES-1008D/1016D/1024D**. Для подключения серверов следует применять более высокоскоростные коммутаторы, например, **DGS-3120-xx**. На предприятиях среднего размера, при необходимости разделения сети предприятия на отдельные подсети, нужно применять настраиваемые или управляемые коммутаторы. Примерами таких устройств являются коммутаторы типа **DES-1210-xxG** и **DGS-1210-xx**. На крупных предприятиях экономически целесообразно использовать стекируемые коммутаторы, представителями которых являются модели **DES-3552** и **DES-3550.** Коммутаторы поддерживают физическое стекирование по протоколу Ethernet, статическую маршрутизацию, функции управления многоадресной рассылкой, расширенные функции безопасности и виртуальных локальных сетей VLAN. Устройства легко интегрируются с коммутаторами L3 уровня ядра для формирования многоуровневой сетевой структуры с высокоскоростной магистралью и централизованными серверами.

Новым поколением мультисервисных коммутаторов D-Link, предназначенных для использования на уровне доступа сетей крупных предприятий и городских сетей *Metro Ethernet* являются коммутаторы *Fast Ethernet* 3 уровня типа DES-3810-xx. В них реализованы сервисы *Triple Play*, при котором по одной линии связи передаются сигналы данных Интернет, кабельного телевидения и телефонной связи. В них реализованы функции управления качеством обслуживания (QoS), маршрутизации пакетов IPv4, многоадресной рассылки и множество функций безопасности и др. Также коммутаторы серии DES-3810-xx поддерживают функцию управления ресурсами коммутатора SRM (*Switch Resource Management*), позволяющую администратору оптимизировать ресурсы коммутатора при его использовании в различных типах сетей.

На **уровне распределения** интенсивность трафика существенно выше, чем на уровне доступа. Поэтому коммутаторы этого уровня должны обладать более высокой пропускной способностью и более широким диапазоном конфигурации. Такие возможности имеют коммутаторы D-Link класса управляемости 3xxx, например, **DGS-36xx**. Эти коммутаторы относятся к семейству маршрутизирующих управляемых коммутаторов *Gigabit Ethernet* 3 уровня с поддержкой портов 10 GE. Они характеризуются высокой производительностью и расширенной поддержкой функций многоадресной передачи данных. Коммутаторы позволяют значительно повысить эффективность предоставляемых операторами связи таких услуг, как видео по требованию (VoD), IP-телевидение (IPTV) и телевидение высокой четкости (HDTV). Коммутаторы также поддерживают протоколы маршрутизации BGP, OSPF, RIP1/2, возможность создания статических маршрутов IP v4/v6.

Важнейшим требованием, предъявляемым к коммутаторам **уровня ядра,** является их производительность и возможность поддержки третьего уровня коммутации. К коммутаторам, удовлетворяющим этим требованиям,

можно отнести семейство высокопроизводительных коммутаторов *Gigabit Ethernet* 3 уровня с поддержкой портов 10 GE серии **DGS-3620-xx**. Коммутаторы разработаны для применения на уровне ядра сетей крупных предприятий и городских сетей (Metro Ethernet). Коммутаторы поддерживают физическое стекирование через порты 10GE SFE+ и позволяют объединить в стек до 12 устройств. На уровне ядра сетей крупных предприятий, сетей небольших операторов связи, а также для организации широкополосного доступа в Интернет в крупных торговых комплексах и бизнес-центрах целесообразно использовать модульные коммутаторы 3 уровня серии **DGS-66xx**, характеризующихся высокой производительностью и высокой плотностью портов.

Перспективными моделями коммутаторов для уровня ядра являются модульные высокопроизводительные коммутаторы, выполненные на основе шасси. К ним относятся коммутаторы 66-го классов управляемости типа **DGS-6600** и интеллектуальный высокопроизводительный многоуровневый модульный коммутатор **DES-7200**. Устанавливая в шасси модули расширения, пользователи могут получить до 384 гигабитных портов, до 64 портов 10GE, до 192 портов SFP или их комбинаций. Коммутаторы поддерживают богатый набор функций 2 и 3 уровня, включая поддержку протоколов BGP, MPLS (*MultiProtocol Label Switching*) и др.

Модульные коммутаторы 3 уровня серии DGS-66xx представляют собой высокопроизводительные устройства с высокой плотностью портов, предназначенные для использования на уровне субядра сетей крупных предприятий, сетей небольших операторов связи, а также для организации широкополосного доступа в Интернет в крупных торговых комплексах и бизнес-центрах. Широкий выбор модулей позволяет обеспечить гибкость при подключении пользователей. В максимальной конфигурации шасси поддерживает до 144 гигабитных портов или до 24 портов 10GE. Шасси поддерживает расширенный набор функций 2 уровня. Функции 3 уровня включают поддержку маршрутизации OSPF v.2/3, RIP v.1/2/ng для IP v4/v6, BGP. Расширенные функции управления, мониторинга и сбора статистики, предоставляют администратору сети возможность следить за состоянием сети и анализировать причины возникновения в ней ошибок и узких мест.

Коммутаторы 3 уровня на основе шасси серии DES-72xx являются высокопроизводительными устройствами с высокой плотностью портов, предназначенными для уровня ядра сетей крупных предприятий и *Metro Ethernet*. Устанавливая в шасси модули расширения, пользователи могут получить до 384 гигабитных портов, до 32 портов 10GE, до 192 портов SFP или их комбинаций. Коммутаторы поддерживают богатый набор функций 2 и 3 уровня, включая поддержку протоколов BGP, MPLS, функции IPFIX, позволяющей получать статистику о сетевом трафике.

Корпорацией D-Link также разработаны коммутаторы для осуществления доступа пользователей к сети по протоколу Ethernet по волоконно-

оптическим линиям пассивной оптической сети GEPON. К ним относится коммутатор типа DPN-3012-E, являющийся устройством класса OLT (*Optical Line Terminal*) и коммутатор типа DPN-301/304, относящийся к оптическим абонентским устройством класса ONU (*Optical Network Unit*), рассмотренным в подразделе 1.5. Эти два типа коммутаторов, совместно с пассивными оптическими разветвителями (сплиттерами) позволяют создавать законченные решения по построению оптических сетей, обладающих топологией «точка-многоточка».

5.6.2. Краткая характеристика системы команд

Конфигурация многих моделей коммутаторов D-Link осуществляется путем ввода команд с использованием интерфейса командной строки CLI (*Command-Line Interface*). Процедура конфигурации коммутаторов D-Link аналогична конфигурации коммутаторов Cisco, однако вид и синтаксис команд заметно отличается.

Все управляемые коммутаторы D-Link, как правило, имеют защиту от доступа неавторизованных пользователей, поэтому после загрузки устройства появляется приглашение ввести имя пользователя и пароль. По умолчанию имя пользователя и пароль в коммутаторах D-Link не определены. Поэтому для пропуска этапов ввода логина и пароля и появления приглашения в командной строке следует дважды нажать клавишу Enter. В результате в командной строке появится приглашение, например `DES-3800:admin#`. После этого можно вводить команды.

В сетевой операционной системе (IOS) коммутаторов D-Link существует большое количество команд CLI. Для просмотра всего состава команд в командной строке следует после пробела ввести знак вопроса и нажать Enter. В результате на экран монитора выводится список всех команд данного уровня. Для выяснения параметра команды необходимо после ее ввода после пробела ввести знак вопроса «?» и нажать клавишу Enter. На экране появятся все возможные завершения команды. Также можно воспользоваться клавишей TAB, после очередного нажатия которой будут последовательно выводиться на экран все возможные завершения команды. Рассмотрим основные команды, наиболее широко используемые при конфигурации коммутаторов D-Link.

Для обеспечения защиты коммутатора от доступа неавторизованных пользователей требуется создание учетных записей для пользователей, обладающих соответствующими правами. Создавая учетную запись для пользователя, можно задать один из двух уровней привилегий: *Admin* или *User*. Учетная запись *Admin* имеет наивысший уровень привилегий.

Создание учетной записи. Создать учетную запись пользователя можно с помощью следующих команд CLI:

```
DES-3800:admin#create account admin/user <username>
```

Знак «/» означает ввод или одного параметра, или другого. Далее появится приглашение для ввода пароля и подтверждения ввода:

```
Enter a case-sensitive new password:
Enter the new password again for confirmation:
```

Длина имени пользователя и пароля может изменяться от 0 до 15 символов. После успешного создания учетной записи на экране монитора появится слово *Success* (благоприятный исход).

Просмотр текущей конфигурации коммутатора осуществляется путем ввода команды `show switch`.

Изменение пароля и удаление учетной записи. Изменить пароль для пользователя с существующей учетной записью, можно с помощью команды:

```
DES-3800:admin# config account <username>
```

В результате появится приглашение ввести сначала старый пароль, а затем новый. Проверить созданную учетную запись можно с помощью команды:

```
DES-3800:admin# show account
```

Результатом выполнения команды будет имя пользователя и уровень пользователя.

Удалить учетную запись можно, выполнив команду

`delete account <username>`.

Задание IP-адреса коммутатору. Для того чтобы коммутатором можно было удаленно управлять через Web-интерфейс или Telnet, ему необходимо назначить IP-адрес из адресного пространства сети, в которой планируется его использовать. IP-адрес может быть задан автоматически с помощью протоколов DHCP или BOOTP либо статически, с помощью следующих команд CLI:

```
DES-3800:admin# config ipif System dhcp
DES-3800:admin# config ipif System ipaddress AAA.BBB.CCC.DDD/MM
```

где AAA.BBB.CCC.DDD — IP-адрес, MM — длина префикса в CIDR-формате, например, /24 или /30);

System — имя управляющего интерфейса коммутатора.

Настройка параметров портов коммутатора. По умолчанию порты всех коммутаторов D-Link поддерживают автоматическое определение ско-

рости и режима работы (дуплекс и/или полудуплекс). Но может возникнуть ситуация, что автоопределение будет действовать некорректно и потребуется ручная установка скорости и режима. Для установки параметров портов на коммутаторе D-Link можно воспользоваться командой `config ports`.

Фрагмент сценария установки скорости равной 100 Мбит/с, дуплексного режима работы, разрешения процедуры обучения и анализа MAC-адресов и состояния для портов коммутатора с 1 по 3 и разрешения аппаратного контроля потока передаваемых данных имеет следующий вид:

```
DES-3800:admin# config ports 1-3 speed 100_full learning ena-
ble state enable

Comand: config ports 1-3 speed 100_full learning enable state
enable

Success.

DES-3800:admin#
```

Контроль состояния портов коммутатора. Для просмотра состояния портов применяется команда

```
show ports <список портов>
```

В результате на экран будет выведена таблица с информацией о настройках портов коммутатора.

Сохранение текущей конфигурации коммутатора осуществляется в энергонезависимую память NVRAM. Для этого необходимо выполнить команду **`save`**.

```
DES-3800: admin#save
Comand: save
Saving all configurations to NV-RAM… Done
DES-3800: admin#
```

Перезагрузка коммутатора выполняется с помощью команды `reboot`, а **сброс настроек** коммутатора к заводским установкам осуществляется с помощью команды `reset`.

5.6.3. Асимметричные VLAN и сегментация трафика

С целью более эффективного использования разделяемых ресурсов, таких как серверы или Интернет-шлюзы, в программном обеспечении ряда коммутаторов D-Link уровня L2 реализована поддержка функции Asymmetric VLAN. Асимметричные виртуальные локальные сети позволяют клиентам, принадлежащих разным VLAN и не поддерживающим тегирова-

ние 802.1Q, взаимодействовать с сервером (или нескольким серверам) с через один физический канал связи с коммутатором, не требуя использования внешнего маршрутизатора. Активизация функции «Асимметричные VLAN» на коммутаторе 2-го уровня позволяет сделать его немаркированные порты членами нескольких виртуальных локальных сетей. При этом рабочие станции останутся полностью изолированными друг от друга. Например, асимметричные VLAN могут быть настроены таким образом, чтобы обеспечить доступ к почтовому серверу всем почтовым клиентам.

Основное различие между базовым стандартом IEEE 802.1Q VLAN (или симметричными VLAN) и асимметричными VLAN заключается в том, как выполняется отображение адресов. Симметричные VLAN используют отдельные адресные таблицы, и таким образом не существует пересечения адресов между VLAN-ами. Асимметричные VLAN могут использовать одну, общую таблицу адресов. Однако, использование одних и тех же адресов (пересечение по адресам) происходит только в одном направлении. При использование асимметричных VLAN протокол IGMP Snooping не поддерживается. При активизации асимметричных VLAN, уникальный идентификатор PVID назначается всем портам, создавая отдельную VLAN для каждого порта. Каждый порт при этом, может получать кадры от VLAN по умолчанию. Асимметричные VLAN в коммутаторе по умолчанию отключены.

Для работы с асимметричными виртуальными сетями в операционную систему коммутаторов D-Link введен ряд команд. Так команда `enable asymmetric_vlan` позволяет глобально активизировать асимметричные VLAN. Задавая команду `disable asymmetric_vlan` можно глобально отключить асимметричные VLAN. Чтобы проконтролировать статус асимметричной VLAN следует ввести команду `show asymmetric_vlan`. Примеры конфигурации асимметричных VLAN можно посмотреть в [10].

С целью разграничения доменов на уровне L2 в коммутаторах D-Link введена функция сегментации трафика (*Traffic Segmentation*). Эта функция позволяет настраивать порты коммутатора таким образом, чтобы они были изолированы друг от друга, но в то же время имели доступ к разделяемым портам, используемым для подключения серверов и магистрали сети провайдера. Данная функция может быть использована при построении сетей провайдеров. Важной также является возможность одновременного использования сегментации трафика с VLAN, что позволяет производить дальнейшее разграничение прав доступа.

Метод сегментации трафика аналогичен используемой технологии для ограничения трафика в VLAN, но ограничения при сегментации трафика еще более строгие.

Настройка сегментации трафика на коммутаторе осуществляется по команде

```
config traffic_segmentation <portlist> forward_list <portlist>
```

Просмотр настроек сегментации трафика

```
show traffic_segmentation <portlist> .
```

Здесь `portlist` — список номеров портов, входящие кадры которых будут передаваться через порты, обозначенные параметром `forward_list`.

5.7. Общая характеристика коммутаторов Huawei

5.7.1. Обозначение и состав коммутаторов Huawei

Для построения компьютерных сетей уровня предприятий в настоящее время достаточно широко используются коммутаторы корпорации Huawei (производитель Китайская народная республика). К наиболее широко используемым коммутаторам компании Huawei относятся коммутатолры типа Quidway серии Sx700. Они предназначены для применения на уровне доступа, так и на уровнях агрегирования и ядра кампусных сетей.

Общее сокращенное обозначение коммутаторов имеет вид: SxAyy-pp. Здесь S – коммутатор (Switch), цифра x – 1 – неуправляемые коммутаторы; 2 или 3 уровень коммутатора (L2 или L3 соответственно) или наличие гигагитовых Ethernet-портов (цифра 5) или портов 10GE (цифра 6). Цифра A – назначение коммутатора (7 – для предприятий); yy-подсерия устройства. Цифры pp показывают максимальное количество портов всех типов. Буквы после количества портов уточняют спецификацию портов. Так символы PC показывают, что в коммутаторе имеется возможность подключать платы расширения; буквосочетание TP означает, что в число портов устройства входят комбинированные порты (электрические или оптические); буква P – имеются фиксированные оптические порты, передающие в восходящем направлении. Кроме этого, в обозначение могут входить символы, показывающие вид питания (от сети или по Ethernet-кабелю), версию устройства (упрощенная – L1, SI – стандартная, EI - улучшенная и др.

В линейку коммутаторов Quidway Sx700 входят устройства серии S1700, S2700, S3700, S5700, S6700, S7700 и S9700. В этом оборудовании реализовамны расширенные функции безопасности, включающие защиту от DoS-атак; DHCP Snooping на основе анализа MAC- и IP-адресов, времени аренды IP-адресов, идентификаторов виртуальных сетей VLAN ID и интерфейсов доступа пользователей. Кроме этого в коммутаторах применяется защита от ARP-атак, введена централизованная аутентификация MAC-адресов и аутентификация по протоколу 802.1x.

Коммутаторы позволяют поддерживать качество сетевого сервиса (QoS). При этом используется информация, содержащаяся в полях заголов-

ков (TOS, тип IP-протокола, тип протокола Ethernet, порт источника TCP, VLAN ID, класс обслуживания CoS и др.).

Неуправляемые и управляемые через Web-интерфейс коммутаторы второго (L2) уровня серии S1700 предназначены для малых и средних предприятий. Имеют от 8 до 48 портов со скоростью передачи 10/100/1000 Мбит/с. Отличаются низким энергопотреблением. Техническое обслуживание коммутаторов сведено к минимуму.

Коммутаторы второго (L2) уровня серии S2700 располагают от 8 до 48 портов, в зависимости от подсерии устройства. Они позволяют разделять локальную сеть на VLAN на основе группирования портов или портов и MAC-адресов. Для обеспечения качества сервисов QoS коммутаторы S2700 могут выполнятьт классификацию трафика на основе VLAN ID, IP, MAC/IP-адресов источника, MAC/IP-адресов получателя, приоритета или номера порта кадров. Используются коммутаторы преимущественно на уровне доступа. Для малых предприятий, интернет-кафе, школ компанией Huawei разработаны бюджетные коммутаторы второго уровня серии S1700. Разновидности этой серии располагают от 8 до 48 портов и могут поддерживать оптические модули SFP.

Устройства S3700 выполняют функции коммутации второго (L2) и третьего (L3) уровня эталонной модели OSI, обеспечивая эффективный доступ и агрегирование трафика в сетях предприятий на уровне распределения. В Huawei серии S3700 поддерживаются все стандартные протоколы маршрутизации (RIPv1, RIPv2, OSPF, IS-IS и BGP). Устройства могут маршрутизировать пакеты протоколов IPv4 так и IPv6.

Коммутаторы серии Quidway S53xx относятся к коммутаторам третьего уровня и отличаются наличием гигагбитовых портов**.** Устройства серий S7700 и S6700 представляют собой высокопроизводительные интеллектуальные маршрутизирующие коммутаторы, позволяющие осуществлять агрегацию гигабитных каналов и передачу трафика 10GbE в устройства следующих сетевых уровней. Они могут применяться в крупных кампусных сетях для агрегации трафика серверов, а также в центрах обработки данных ЦОД.

5.7.2. Основные команды управления коммутаторами Huawei

Система команд управления телекоммуникационным оборудованием корпорации Huawei принципиально мало чем отличается от системы команд Cisco. Оборудование Huawei может конфигурироваться как с командной строки CLI, так и посредством Web-интерфейса. Интерфейс командной строки по принципу работы практически полностью соответствует интерфейсу телекоммуникационных устройст Cisco, только несколько изменился синтаксис команд. Так же как и у Cisco, в оборудовании Huawei имеется два

режима работы с командной строкой – привилегированный и непривилегированный.

Для непривилегированного режима характерным является приглашение в угловых скобках вида <Switch> для коммутатора или <Router> для маршрутизатора, а для привилегированного режима имя коммутатора или маршрутизатора в приглашении заключается в прямоугольные скобки: [Switch] или [Router]. Команды, как и у Cisco, можно набирать в сокращенном виде, т.е. вводить лишь первые начальные символы.

Основные команды конфигурации коммутатора, их значение и примеры записи приведены в таблице 5.2.

Таблица 5.2

Основные команды управления коммутаторами Huawei

Команда	Значение	Пример
clock timezone	Настройка часового пояса на коммутаторе	<switch_1>clock timezone EKT add 03:00:00
clock datetime	Настройка даты (выполняются в непривилегированном режиме)	<switch_1>clock datetime 10:30:00 2018-09-06
system-view	Переход в привилегированный режим	< switch_1>system-view [switch_1]
quit	Выход из привилегированного режима	[switch_1]quit < switch_1>
display current-configuration	Просмотр текущей конфигурации (или порта коммутатора)	<SW1-Q2326> display current-configuration interface Ethernet 0/0/6
display interface	Просмотр состояния порта	<SW1-Q2326> display interface ethernet0/0/2
display mac-address	Просмотр mac-адреса	<SW1-Q2326> display mac-address
display interface description	Просмотр описания портов коммутатора	<SW1-Q2326> display interface description
display vlan	Просмотр информации о созданных VLAN	<SW1-Q2326> display vlan
display interface-statictics	Просмотр статистики интерфейса	<SW1-Q2326> display interface-statistic Ethernet 0/0/4
shutdown и undo shutdown	Включение/отключение административной блокировки интерфейса	[SW1-Q2326] interface Ethernet 0/0/4 [SW1-Q2326 interface Ethernet 0/0/4] shutdown
vlan {vlan-id}	Создание VLAN	[huawei] vlan 20

int vlanif	Создание VLAN интерфейса	[Quidway]int vlanif 1
ip address [address mask]	Присвоение интерфейсу адреса и маски	[Quidway-Vlanif1]ip address 172.20.0.47 21
vlan batch [vlan-id to vlan-id]	Создание нескольких VLAN	vlan batch [vlan-id1 to vlan-id4]
undo vlan {vlan-id}	Удаление VLAN	
description	Задание имени VLAN	[SW1-Q2326-vlan2] description Admin_vlan
pvid vlan {vlan-id}	Добавление идентификатора для нетегированной VLAN	

Пример 5.1. Настройка порта доступа коммутатора

```
<huawei>system-view
[huawei]interface Ethernet0/0/1
[huawei-Ethernet0/0/1]port link-type access
[huawei-Ethernet0/0/1]port default vlan 2
[huawei-Ethernet0/0/1]quit
[huawei]quit
<huawei>display current-configuration interface Ethernet 0/0/1
```

Пример 5.2. Настройка магистрального порта коммутатора

```
 huawei> system-view
[huawei] interface GigabitEthernet0/1
[huawei-GigabitEthernet0/1] description Uplink
[huawei-GigabitEthernet0/1] port link-type trunk
[huawei-GigabitEthernet0/1] port trunk allow-pass vlan 12 to 22
[huawei-GigabitEthernet0/1] port trunk pvid vlan 12
[huawei-GigabitEthernet0/1] quit
```

5.8. Протоколы автоматизации конфигурации VLAN в коммутаторах

В компьютерных сетях с несколькими коммутаторами, соединенными транковой магистралью, коммутатор должен иметь возможность пересылать кадры, относящиеся к какой-либо виртуальной сети, на другой коммутатор, содержащий порты данной VLAN. Для этого такой коммутатор должен имеет сведения об идентификаторе и имени этой виртуальной сети. Поэтому в процессе настройки сети предприятия администратор сети должен вручную занести эти сведения в каждый из коммутаторов сети. Причем, любые изменения в конфигурации сети должны быть произведены на всех коммута-

торах сети. Если таких коммутаторов в сети предприятия несколько десятков или сотен, то этот процесс занимает много непроизводительного времени и не исключает появления ошибок конфигурации. Для облегчения этого процесса разработан ряд протоколов, позволяющих автоматизировать процесс настройки виртуальных сетей. К ним относятся стандартные протоколы регистрации общих и множественных параметров виртуальных сетей **GVRP** и **MVRP**, а также аналогичный GVRP популярный проприетарный протокол магистральных каналов виртуальных локальных сетей **VTP** корпорации Cisco Systems. Стандартные протоколы поддерживаются практическими всеми мировыми производителями коммутаторного оборудования, а в коммутаторах Cisco, при наличии возможности поддержки стандартных протоколов, используется преимущественно протокол собственной разработки VTP.

Следует заметить, что применение протокола автоматизации конфигурации виртуальных сетей может нарушить безопасность сети по причине неудачной ее конфигурации (непреднамеренной или злонамеренной).

5.8.1. Протоколы GVRP и MVRP

Стандартный протокол GVRP — сокращенное обозначение протокола *GARP VLAN Registration Protocol* — разработан для автоматического информирования коммутаторов о наличии VLAN в сети. GARP расшифровывается как *Generic Attribute Registration Protocol*. GVRP является протоколом канального уровня эталонной модели ISO/OSI. Он позволяет коммутатору локальной сети сообщить соседним устройствам, что он может принять кадры для одной или нескольких VLAN. Главная цель GVRP — позволить коммутаторам автоматически обнаружить сведения о VLAN, которая иначе должна была бы быть вручную сконфигурирована в каждом коммутаторе.

Протокол GVRP использует сообщения GVRP BPDU (GVRP *Bridge Protocol Data Units*), рассылаемые на многоадресный MAC-адрес 01-80-C2-00-00-21 для оповещения устройств-подписчиков о различных событиях. Кадры оповещения (Advertisement) могут содержать информацию о включении или удалении порта в VLAN, о настройке или удалении VLAN на локальном подписчике, об удалении всех зарегистрированных на магистральном порте VLAN, о параметрах различных таймеров GVRP и др.

GVRP также может быть использован и сетевыми серверами. Эти серверы обычно конфигурируются для вхождения в несколько VLAN, и затем сообщают коммутаторам о VLAN, к которым из них они намерены присоединиться.

На настоящее время протокол GVRP используется довольно часто, однако на смену ему пришел более быстродействующий протокол множественных регистраций виртуальных сетей MVRP (*Multiple VLAN Registration*

Protocol). Он также является сетевым протоколом второго уровня и предназначен для тех же целей, что и его предшественник. Протокол MVRP был определён приложением 802.1ak к рекомендациям IEEE 802.1Q-2005. Протокол MVRP регламентирует динамический обмен между коммутаторами информацией о виртуальных сетях и конфигурацию необходимых VLAN. Реализация стандарта IEEE 802.1Q-2005 позволяет:

1) динамически конфигурировать и распределять информацию о принадлежности VLAN через механизмы MVRP;
2) поддерживать комбинированные статические и динамические конфигурации, при которых некоторые VLAN конфигурируются посредством механизмов управления, а для других VLAN сохраняется возможность динамической конфигурации средствами MVRP.

5.8.2. Протокол VTP

Протокол магистральных каналов виртуальных локальных сетей VTP (*VLAN Trunking Protocol*) предназначен для распространения информации о VLAN на начальном этапе функционирования виртуальной сети. VTP является фирменным протоколом корпорации Cisco, разработанным для облегчения создания и конфигурации виртуальных VLAN администраторами сетей [9,16]. При использовании такого протокола администратору достаточно создать виртуальную сеть (т.е., описать ее) только на одном коммутаторе, а после этого информация о VLAN автоматически распространяется на все коммутаторы локальной сети. Протокол VTP задает правила обмена информацией о конфигурации VLAN между коммутаторами Cisco через **магистральный канал** (*Trunk*). Он регламентирует передачу кадров с информацией, позволяющей узнать о существовании каждой виртуальной сети по ее идентификатору и имени VLAN-сети. Но протокол не сообщает (не анонсирует) сведения о том, какие порты коммутатора относятся к той или иной виртуальной сети. Магистральные соединения позволяют за счет уплотнения линии связи передавать между коммутаторами кадры, относящиеся к различным VLAN. Коммутатор Cisco, получивший VTP-кадр, может определить, в какую VLAN его направить.

При удалении или добавлении в компьютерную сеть VLAN или любом изменении конфигурации VLAN модуль VTP заставляет все коммутаторы некоторого домена сети синхронизировать конфигурации VLAN так, чтобы в них были заданы одинаковые идентификаторы и имена всех VLAN.

Для функционирования протокола VTP локальная сеть должна быть разделена на **домены**. Домены VLAN являются некоторой аналогией автономных систем глобальных сетей, в которых группа коммуникационных устройств совместно использует ряд атрибутов. Для возможности примене-

ния протокола VTP, необходимо, чтобы коммутатор Catalyst принадлежал какому-либо домену. Только коммутаторы, относящиеся к одному и тому же сетевому домену, могут совместно использовать конфигурационную информацию о данной виртуальной сети.

Любой коммутатор VLAN может функционировать в *серверном, клиентском* или *прозрачном режимах*. Отличие между указанными режимами состоит в разных способах генерации конфигурационных VTP-сообщений и реакции на полученные уведомления. В режиме VTP-сервера коммутатор Catalyst автоматически рассылает через все свои магистральные порты соседним коммутаторам VTP-уведомления на групповой адрес (*multicast address*), в которых содержатся сведения о параметрах созданной на сервере виртуальной сети. Передаваемая информация включает имя домена, номер версии протокола, активные VLAN и другую информацию. Посредством таких сообщений остальные коммутаторы, входящие в одноименный домен, информируются о появлении новой виртуальной сети. Информацию, содержащуюся в VTP-сообщениях, учитывают только те коммутаторы, которые сконфигурированы в режиме сервера или клиента.

Коммутаторы Cisco, настроенные на прозрачный режим, не могут генерировать VTP-сообщения. В случае создания виртуальной сети на таком коммутаторе информация о новой VLAN остается локальной и не передается остальным коммутаторам, даже если между ними существует магистральное соединение.

В момент старта любой коммутатор виртуальной сети автоматически конфигурируется в качестве сервера. При создании, удалении или переводе сети в неактивное состояние при помощи коммутатора Cisco, находящимся в прозрачном или серверном режиме, коммутатор сохраняет конфигурационную информацию в энергонезависимой памяти и при включении питания может восстановить последнюю известную информацию. В коммутаторах-клиентах информация о всех виртуальных сетях при отключении питания теряется. Таким образом, для создания сетей VLAN коммутатор Cisco должен быть сконфигурирован администратором в режиме сервера или прозрачном режиме.

Для создания магистрали необходимо предварительно установить соединение и разрешить в нем магистральные процессы. С целью передачи данных по магистрали специалистами Cisco разработан протокол мультиплексирования трафика в VLAN. Согласно этому протоколу к данным пользователя присоединяются дополнительные заголовки и для каждого кадра определяется адрес VLAN отправителя. Соединение, образованное в соответствии с таким протоколом, называется межкоммутаторным каналом ISL (*Inter Switch Link*). Коммутатор Catalyst, отправляя кадр через магистральный интерфейс (порт), функционирующий в соответствии с протоколом ISL, присоединяет к исходному блоку данных ISL-заголовок и указывает его

принадлежность к сети VLAN-отправителя. Формат инкапсулированного кадра показан на рисунке 2.7.

Коммутаторы Cisco позволяют передавать по магистрали трафик всех виртуальных сетей. Однако предусмотрена возможность передавать данные только определенных сетей. Для этого в IOS коммутатора введены команды удаления и добавления сетей в магистраль.

5.9. Примеры конфигурирования сетевых коммутаторов

Рассмотрим особенности применения команд сетевой операционной системы Cisco IOS и конфигурации оборудования на примерах создания виртуальных локальных сетей VLAN на базе различных типов коммутаторов. Список команд и особенности их применения детально освещены во многих источниках [6.10,29].

5.8.1. Создание VLAN и назначение портов

Коммутаторы Catalyst имеют несколько виртуальных локальных сетей VLAN, объявленных по умолчанию (default). Сеть VLAN 1 содержится всегда, и все активные порты отнесены к ней по умолчанию. Если требуется добавить больше виртуальных сетей, нужно их создать. Команды создания VLAN для операционных систем COS и IOS несколько отличаются. В приведенных примерах используются только команды IOS. При выполнении команды просмотра сеть VLAN 1 всегда будет отображаться с именем default. Разработчиками дополнительно для сетей типа FDDI и Token Ring предусмотрены виртуальные сети VLAN с номерами 1002 – 1005. Эти сети не могут быть удалены, так как они являются частью конфигурации коммутатора по умолчанию. В таблице 5.3 показан пример такой конфигурации коммутатора Catalyst. Вывод сокращенной конфигурации коммутатора на экран монитора осуществляется по команде `Sw-2960#show vlan brief`.

Коммутаторы Catalyst позволяют создавать изолированные виртуальные сети. Так коммутатор Catalyst 2950 на базе стандартной IOS может обеспечить поддержку 64 VLAN, а при использовании Enhanced Software Image (EI) — 250 VLAN. На основе Catalyst 3550 можно создать 1005 VLAN, причем номера (идентификаторы) сетей от 1002 до 1005 зарезервированы для локальных сетей Token Ring и FDDI.

При создании виртуальных сетей следует помнить, что в них имеется два типа портов.

1. **Access port** — порт доступа. К этому порту подключаются оконечные устройства, как правило, рабочие станции. Кадры, передаваемые между портом доступа и оконечным устройством, нетегированные. Каждый порт

доступа входит в определённую VLAN. Все кадры, поступающие в этот порт от оконечного устройства, получает метку данной виртуальной сети, а кадрах, выдаваемых портом рабочеей станции, эта метка изымается портом коммутатора.

Таблица 5.3

Пример просмотра конфигурации коммутатора Catalyst 2960

VLAN	Name	Status	Ports
1	default	active	Fa0/1,Fa0/2,Fa0/3,Fa0/4,Fa0/5,Fa0/6,
			Fa0/7,Fa0/8,Fa0/9,Fa0/10,Fa0/11,Fa0/12,
			Fa0/13,Fa0/14,Fa0/15,Fa0/16,Fa0/17,Fa0/18,
			Fa0/19,Fa0/20,Fa0/21,Fa0/22,Fa0/23,Fa0/24
			Gi0/1,Gi0/2
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

2. **Trunk port** — магистральный порт**.** Этот порт предназначен для множественного использования, т.е. по нему в разные моменты времени перемещаются кадры различных VLAN. В заголовке каждого кадра присутствует метка (тег), указывающая на номер виртуальной сети, к которой относится данный кадр.

Кроме того, в множестве виртуальных сетей, созданных на коммутаторе, обязательно присутствует «родная» сеть (*Native* VLAN). Трафик этой виртуальной сети не тегируется. По умолчанию такой сетью является первая виртуальная сеть — VLAN1. Операционная система коммутатора позволяет изменить номер родной сети. Такая сеть введена для обеспечения совместимости с устройствами, в которых не поддерживается протокол 802.1q, т.е. в них не применяется тегирование кадров и они не могут распознавать тегированные кадры. И если нетегированный кадр поступит в trunk-порт, то он не будет проигнорирован коммутатором, а будет помещён в Native VLAN.

Если проектируемая сеть содержит несколько коммутаторов (1…3), то виртуальные сети можно создавать вручную, т.е., не прибегая к применению специальных средств автоматизации настройки и управления VLAN.

VLAN создается в режиме глобальной конфигурации с помощью команды Vlan <vlan-id>.

Пример 5.3. Создать виртуальную сеть отдела кадров с номером 3 и присвоить ей имя «Cadry». Сконфигурировать порты с коммутатора с Fa0/5 по Fa0/12 в качестве портов доступа, а порт Fa0/1 в качестве транкового и включить все эти порты в VLAN 3. Транковый порт пропускает кадры только принадлежащие виртуальным сетям 3 и 6. Проверить конфигуцию сети и сохранить ее.

```
Switch#configure terminal
Switch(config)#vlan 3
!-- создание VLAN с номером 3
Switch(config-vlan)#name Cadry
!-- присвоение сети имени Cadry (отдел кадров)
Switch(config-vlan)#exit
!-- возврат в режим глобальной конфигурации
Switch(config)#interface range fa0/5—12
!-- выбор диапазона интерфейсов в качестве портов доступа
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 3
!-- включение порта доступа в vlan 3
Switch(config-if)#exit
Switch(config)# interface fa0/1
!-- выбор интерфейса для транкового порта
Switch(config-if)#switchport trunk allowed vlan 3,6
!-- разрешить прохождение через транковый порт кадров
!-- только сетей 3 и 6
Switch(config-if)#switchport mode trunk
!-- определить транк
Switch(config-if)#end
!—возврат в привилегированный режим
Switch#show vlan
!-- просмотр базы данных виртуальных сетей
Switch#show running-config
!-- проверка конфигурации vlan
Switch#copy running-config startup-config
!-- сохранение конфигурации
```

Для ликвидации VLAN применяется команда **no vlan <vlan-id>.**

5.9.2. Конфигурирование VLAN с использованием протокола VTP

Для больших сетей ручная конфигурация VLAN становится весьма трудоёмкой задачей. Поэтому при конфигурации большого количества коммутаторов целесообразно воспользоваться протоколом VTP (*VLAN Trunk Protocol*), который предназначен для автоматического обмена информацией о VLAN через магистральные порты. При использовании этого протокола любые установки и изменения на одном коммутаторе автоматически распространятся на все остальные устройства данной сети.

После включения большинство коммутаторов Catalyst устанавливаются в режиме "сервер". Для просмотра на коммутаторе, например на устройстве 3524XL, состояния VTP, воспользуемся командой `show vtp status`.

```
3524XL#show vtp status

VTP Version : 2
Configuration Revision : 0
Maximum VLANs supported locally : 254
Number of existing VLANs : 5
VTP Operating Mode : Server
!--- Это режим используется по умолчанию

VTP Domain Name :
VTP Pruning Mode : Disabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0xBF 0x86 0x94 0x45 0xFC 0xDF 0xB5 0x70
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

1. Создадим VLAN на коммутаторе 3524XL.

Следует отметить, что коммутатор может создавать VLAN только если он находиться в режиме VTP "сервер" или VTP "прозрачный". По умолчанию все порты коммутатора принадлежат первой сети, т.е. VLAN 1. Данную сеть нельзя ни удалить, ни переименовать. Для просмотра информации об этой сети выполним команду `show vlan`.

```
3524XL# show vlan

VLAN  Name      Status   Ports
----  -------   ------   ---------------------------
1     default   active   Fa0/1,  Fa0/2,  Fa0/3,   Fa0/4,
                         Fa0/5,  Fa0/6,  Fa0/7,   Fa0/8,
                         Fa0/9,  Fa0/10, Fa0/11,  Fa0/12,
                         Fa0/13, Fa0/14, Fa0/15, Fa0/16,
                         Fa0/17, Fa0/18, Fa0/19, Fa0/20,
                         Fa0/21, Fa0/22, Fa0/23, Fa0/24,
```

Как видно из ответа коммутатора, имеется только одна активная сеть VLAN 1 с именем `default, содержащая` 24 порта FastEthernet со скоростью передачи 100 Мбит/с и два гигабитовых порта.

Для того чтобы создать VLAN 2 с именем `cisco_vlan_2,` воспользуемся следующими командами:

```
3524XL#vlan database
!-- Вход в базу данных VLAN, чтобы сконфигурировать VLAN.
3524XL(vlan)#vtp server
Device mode already VTP SERVER.
!-- Последнюю команду можно опустить, если коммутатор уже
!--- находится в режиме "сервер" и мы хотим оставить его в этом режиме.
3524XL(vlan)#vlan 2 name cisco_vlan_2
VLAN 2 added:
Name: cisco_vlan_2
3524XL(vlan)#exit
!-- Следует выйти из базы данных VLAN для того,
!-- чтобы изменения были приняты.
!--
APPLY completed.
Exiting....
3524XL#
```

2. Осуществим проверку наличия новой VLAN, для чего снова воспользуемся командой `show vlan`

```
3524XL# show vlan

VLAN  Name            Status  Ports
----  --------------  ------  ---------------------------
1     default         active  Fa0/1,   Fa0/2,   Fa0/3,   Fa0/4,
                              Fa0/5,   Fa0/6,   Fa0/7,   Fa0/8,
                              Fa0/9,   Fa0/10,  Fa0/11,  Fa0/12,
                              Fa0/13,  Fa0/14,  Fa0/15,  Fa0/16,
                              Fa0/17,  Fa0/18,  Fa0/19,  Fa0/20,
                              Fa0/21,  Fa0/22,  Fa0/23,  Fa0/24,
                              Gi0/1,   Gi0/2
2     cisco_vlan_2    active
```

Как видно из сообщения, созданная сеть VLAN 2 активная, однако пока пустая, а все наличные порты принадлежат сети VLAN 1. Для включения портов во вторую сеть следует перейти в режим конфигурации интерфейса для каждого порта, который нужно добавить в VLAN.

```
3524XL#configure terminal
```

```
Enter configuration commands, one per line.
End with CNTL/Z.
!-- Следующие команды припишут второй порт
!-- Fast Ethernet 0/2 к VLAN 2.
3524XL(config)#interface fastethernet 0/2
3524XL(config-if)#switchport access vlan 2
!--
3524XL(config-if)#exit
!-- Следующие команды припишут третий интерфейс
!-- Fast Ethernet 0/3 к VLAN 2.
3524XL(config)#interface fastethernet 0/3
3524XL(config-if)#switchport access vlan 2
3524XL(config-if)#end
3524XL#
!-- Сохраняем конфигурацию
3524XL#write memory
Building configuration...
```

3. Проверим правильность назначения портов.

```
3524XL# show vlan

VLAN  Name            Status  Ports
----  --------------  ------  ---------------------------
1     default         active  Fa0/1, Fa0/4,  Fa0/5,  Fa0/6,
                              Fa0/7, Fa0/8,  Fa0/9,  Fa0/10,
                              Fa0/11,Fa0/12, Fa0/13, Fa0/14,
                              Fa0/15,Fa0/16, Fa0/17, Fa0/18,
                              Fa0/19,Fa0/20, Fa0/21, Fa0/22,
                              Fa0/23,Fa0/24, Gi0/1,  Gi0/2
2     cisco_vlan_2    active  Fa0/2, Fa0/3
```

Из сообщения видно, что второй и третий порты теперь относятся ко второй виртуальной сети, а остальные порты коммутатора остались в первой сети.

4. Выполним, если нужно, удаление порта из VLAN.

Для того чтобы удалить порт из VLAN необходимо задать команду

```
no switchport access vlan vlan_number
```

в конфигурации интерфейса. После того, как порт удаляется из VLANa, он автоматически помещается в default VLAN. Так для удаления интерфейса fastethernet 0/2 из VLAN 2, следует выполнить команды:

```
3524XL#configure terminal
Enter configuration commands, one per line. End with
!-- Следующие две команды удалят интерфейс Fast Ethernet 0/2
!-- из VLAN 2.
3524XL(config)#interface fastethernet 0/2
3524XL(config-if)#no switchport access vlan 2
3524XL(config-if)#end
3524XL# show vlan

VLAN  Name            Status  Ports
----  ------------    ------  --------------------------
1     default         active  Fa0/1,  Fa0/2,  Fa0/4,  Fa0/5,
                              Fa0/6,  Fa0/7,  Fa0/8,  Fa0/9,
                              Fa0/10, Fa0/11, Fa0/12, Fa0/13,
                              Fa0/14, Fa0/15, Fa0/16, Fa0/17,
                              Fa0/18, Fa0/19, Fa0/20, Fa0/21,
                              Fa0/22, Fa0/23, Fa0/24, Gi0/1,
                              Gi0/2
2     cisco_vlan_2    active  Fa0/3,
```

Из сообщения видно, что второй порт Fa0/2, снова возвращен в первую виртуальную сеть.

5. Произведем, в случае необходимости, удаление виртуальной сети.

Для удаления VLAN применяется команда `no vlan vlan_number` в режиме базы данных VLAN. Интерфейс в этой виртуальной сети остается ее частью, но деактивируется, поскольку он не принадлежит никакой VLAN.

```
3524XL# vlan database
!-- Вход в режим VLAN database.
3524XL(vlan)# no vlan 2
!-- Удаление VLAN из базы данных.
Deleting VLAN 3...
3524XL(vlan)# exit
APPLY completed.
Exiting....
3524XL# show vlan
VLAN  Name          Status   Ports
----  ----------    ------   --------------------------
1     default       active   Fa0/1,  Fa0/2,  Fa0/4,   Fa0/5,
                             Fa0/6,  Fa0/7,  Fa0/8,   Fa0/9,
                             Fa0/10, Fa0/11, Fa0/12,  Fa0/13,
```

```
                    Fa0/14, Fa0/15, Fa0/16,  Fa0/17,
                    Fa0/18, Fa0/19, Fa0/20,  Fa0/21,
                    Fa0/22, Fa0/23, Fa0/24,  Gi0/1,
                                             Gi0/2
```

Как видно из сообщения, порт Fa0/3 не отображается в выводе команды show vlan. Удаление VLAN 2 деактивировало данный порт и до тех порт пока он снова не будет добавлен к какую-нибудь VLAN, этот порт не будет отображаться и не будет функционировать. Если осуществить просмотр статуса этого интерфейса, то видно, что и порт и линейный протокол отключены (down).

```
3524XL# show interfaces fastethernet 0/3
FastEthernet 0/3 is down, line protocol is down
```

5.9.3. Конфигурирование VLAN на основе коммутаторов D-Link и Cisco

По мере расширения сети предприятия и приобретения нового коммуникационного оборудования в ряде случаев появляется необходимость объединение коммутаторов различных производителей, например Cisco и D-Link. Сценарий конфигурации такого оборудования приведен в примере 5.2.

Пример 5.6. Пусть сеть организации состоит из 8 рабочих станций и двух коммутаторов разных производителей Catalyst 2950 и DES-3526 и должна быть разделена на две изолированные подсети (VLAN). К каждому из коммутаторов должно быть подключено по 2 рабочих станции каждой из подсетей. Составить схему сети и выполнить конфигурацию коммутаторов, удовлетворяющим заданным условиям. Схема сети организации изображена на рисунке 5.5. Номера портов, к которым подключены рабочие станции, указаны на схеме.

В качестве магистральных портов на коммутаторе DES-3526 используется порт 26, а на коммутаторе Catalyst 2950 порт Fa4.

Настройка DES-3526:

```
!-- Создание VLAN с VID=2
DES-3526#create vlan vlan2 tag 2
!-- Добавление порта 26 в VLAN default как tagged для
организации
!-- тегированной магистрали
DES-3526#config vlan default add tagged 26
!-- Удаление порта 12 из VLAN default
DES-3526#config vlan default delete 12
```

```
!--  Добавление порта 12 в VLAN2
DES-3526#config vlan vlan2 add untagged 12
!-- Удаление порта 13 из VLAN default
DES-3526#config vlan default delete 13
!--  Добавление порта 13 в VLAN2
DES-3526#config vlan vlan2 add untagged 13
```

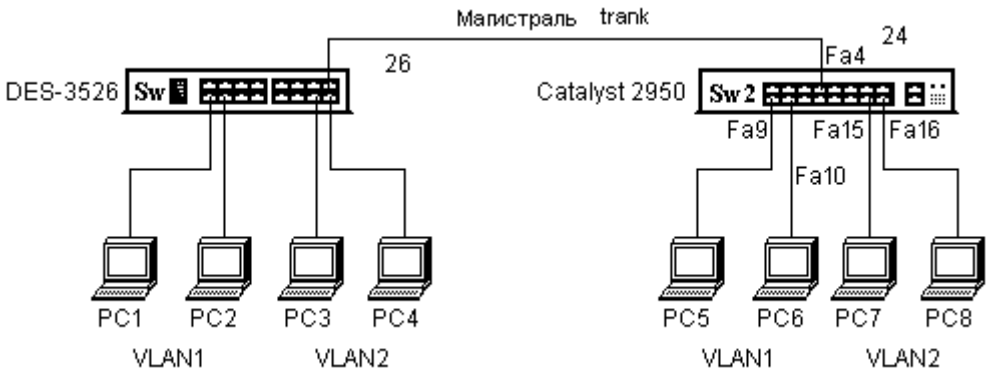


Рисунок 5.5 – Компьютерная сеть на основе разнотипных коммутаторов

```
!-- Добавление порта 26 в VLAN2 как tagged для органи-
зации тегированной
!-- магистрали
DES-3526#config vlan vlan2 add tagged 26
```

Настройка Cisco Catalyst 2950:

```
!-- Переключение в режим конфигурирования
Switch#configure terminal
!-- Вход в режим конфигурирования интерфейса 9
Switch(config)#interface fa 0/9
!-- Задание режима access (untagged) в первой VLAN
Switch(config-if)#switchport access vlan 1
!-- Выход из режима конфигурирования интерфейса
Switch(config-if)#exit
!-- Вход в режим конфигурирования интерфейса 10
Switch(config)#interface fa 0/10
!-- Задание режима access (untagged) в первой VLAN
Switch(config-if)#switchport access vlan 1
!-- Выход из режима конфигурирования интерфейса
Switch(config-if)#exit

!-- Переключение в режим конфигурирования интерфейса 15
Switch(config)#interface fa 0/15
```

```
!-- Задание режима access (untagged) во второй VLAN
Switch(config-if)#switchport access vlan 2
!-- Выход из режима конфигурирования интерфейса
Switch(config-if)#exit
!-- Переключение в режим конфигурирования интерфейса 16
Switch(config)#interface fa 0/16
!-- Задание режима access (untagged) во второй VLAN
Switch(config-if)#switchport access vlan 2
!-- Выход из режима конфигурирования интерфейса
Switch(config-if)#exit

!-- Переключение в режим конфигурирования интерфейса 4
Switch(config)#interface fa 0/4
```

Switch(config-if)# switchport mode trunk encapsulation dot1q

```
!-- Задание магистрального канала trunk с инкапсуляцией
802.1q
Switch(config-if)# end
```

5.9.4. Конфигурирование агрегированных каналов коммутаторов Cisco и D-Link

На коммутаторах Cisco Catalyst для повышения скорости и отказоустойчивости соединениия можно включить функции LACP, EtherChannel, Fast EtherChannel (FEC) или Gigabit EtherChannel (GEC). Эти функции позволяют использовать несколько физических линий связи между двумя одинаковыми устройствами как один более скоростной логический канал с балансировкой (выравниванием) нагрузки в используемых линиях. Такое объединение называют агрегированием каналов.

Etherchannel позволяет объединить до 8 портов в один логический канал. Каналом Etherchannel могут быть соединены два коммутатора или коммутатор и сервер. Интерфейсы, участвующие в агрегировании одного канала, должны быть настроены на одинаковую скорость и дуплексный режим.

Объединенный канал EtherChannel можно настроить не только вручную с помощью соответствующих команд, но и автоматически, при этом коммутатор автоматически согласовывает канал с другой стороной. при помощи протокола PAgP (*Port Aggregation Protocol*).

Настраиваться автоматически каналы EtherChannel могут с помощью PAgP-протокола, либо с помощью LACP-протокола. Протокол PAgP — это проприетарный (принадлежащий компании) Cisco протокол, который может работать только на коммутаторах Cisco и на коммутаторах, лицензированных для поддрежки PAgP, выпущенных другими лицензированными произ-

водителями. Протокол LACP (*Link Aggregation Control Protocol*) определен стандартом IEEE 802.3ad. LACP-протокол позволяет коммутаторам Cisco управлять Ethernet-каналами между всеми коммутаторами, которые соответствуют стандарту IEEE 802.3ad.

Настройка EtherChannel вручную производится при помощи команды **channel mode on.** Если настройка производится посредством автоматического согласования, коммутатор выполняет согласование параметров канала с дальним портом. Для выполнения данного действия коммутатор использует частный протокол объединения портов (PAgP) Cisco (при помощи команды **channel mode desirable**) или управления объединением каналов IEEE 802.3ad (LACP) (при помощи команды **channel mode active** или **channel mode passive**).

Пример 5.7. Выполнить вручную настройку канала EtherChannel на коммутаторах Cisco Sw1 и Sw2 путем объединения четырех портов с Fa0/11 по Fa0/14.

Перед настройкой агрегирования рекомендуется выключить физические интерфейсы. Для этого достаточно отключить их с одной стороны (в примере на Sw1), затем настроить агрегирование с двух сторон и включить интерфейсы.

```
!-- настройка EtherChannel на Sw1
Sw1(config)# interface range f0/11-14
!-- настройка интерфейса диапазона портов
Sw1 (config-if-range)# shutdown
!-- выключение диапазона портов
Sw1 (config-if-range)# channel-group 3 mode on
!-- создание агрегированного канала с номером 3
!--
!-- настройка EtherChannel на Sw2:
Sw2(config)# interface range f0/11-14
Sw2 (config-if-range)# channel-group 3 mode on
!-- включение физических интерфейсов на Sw1:
Sw1(config-if-range)# no sh
Sw1(config-if-range)# exit
                                !--
```

!-- просмотр созданной конфигурации

```
Sw1#show etherchannel 3 summary
```

Number of channel-groups in use:1
Number of aggregators: 1

```
Group  Port-      Protocol   Ports
```

```
      channel
1     Po3 (SU)        –       Fa0/11(P),Fa0/12(P),
                              Fa0/13P), Fa0/14(P)
```

Здесь Po — обозначение канала EtherChannel, которое является сокращением от “Port Channel” (канал портов), а Po3 – сокращенное обозначение канала портов EtherChannel 3. Флаг S показывает, что созданный канал второго уровня. Флаг U (in use) – порт используется.

Пример 5.8. Выполнить конфигурацию агрегированного канала между двумя коммутаторами D-Link по протоколу LACP путем объединения четырех портов коммутатора A (члены группы — порты 2, 4, 6 и 8) и четырех портов коммутатора коммутатора B (члены группы — порты 1, 3, 5 и 7).

Конфигурация коммутатора A

Создание группы агрегированных каналов

```
create link_aggregation group_id 1 type lacp
config link_aggregation algorithm mac_destination
```

Назначение членов группы

```
config link_aggregation group_id 1 master_port 2 ports 2,4,6,8
state enabled
config lacp ports 2,4,6,8 mode active
```

Конфигурация коммутатора B

Создание группы агрегированных каналов

```
create link_aggregation group_id 1 type lacp
config link_aggregation algorithm mac_source
```

Назначение членов группы

```
config link_aggregation group_id 1 master_port 1 ports 1,3,5,7
state enabled
```

Просмотр статуса LACP коммутатора A:

```
DGS-3427:4#show link_aggregation
Command: show link_aggregation
Link Aggregation Algorithm = Mac_destination
Group ID : 1
Type : LACP
Master Port : 2
Member Port : 2,4,6,8
Active Port : 2,4,6,8
Status : Enabled
Flooding Port : 2
```

```
Total Entries : 1
```

Просмотр статуса LACP коммутатора B:

```
DGS-3427:4#show link_aggregation
Command: show link_aggregation

Link Aggregation Algorithm = Mac_source
Group ID : 1
Type : LACP
Master Port : 1
Member Port : 1,3,5,7
Active Port : 1,3,5,7
Status : Enabled
Flooding Port : 3

Total    Entries: 1
```

5.9.5. Создание VLAN на основе коммутаторов Huawei

Пример 5.9.

Создать на коммутаторе две виртуальные сети VLAN 2 и VLAN 3 и отключить службы NDP и NTDP (Neighbor Discovery Protocol, применяется для получения сведений о подключенных соседях, а Network Topology Discovery Protocol предназначен для построения топологии в кластере).

Переключение коммутатора в привилегированный режим

```
< quidway>system-view
Enter system view, return user view with Ctrl+Z.
```

Настройка имени устройства

```
[quidway]sysname switch_1
```

Создание виртуальной сети номер 2

```
[switch_1]vlan 2
```

Указание типа интерфейса и способа доступа

```
[switch_1]interface Ethernet0/0/10
[switch_1-Ethernet0/0/10]port link-type access
```

Добавление порта в виртуальную сеть 2

```
[switch_1-Ethernet0/0/10]port default vlan 2
[switch_1-Ethernet0/0/10]quit
```

Создание и настройка виртуальной сети номер 3

```
[switch_1]vlan 3
[switch_1]interface Ethernet0/0/20
[switch_1-Ethernet0/0/20]port link-type access
```

Отключение протоколов NDP и NTDP

```
[switch_1]undo cluster enable
[switch_1]undo ntdp enable
[switch_1]undo ndp enable
```

Выход из режима конфигурации порта и просмотр результатов настройки

```
[switch_1]quit
<switch_1>display vlan
Total 3 VLAN exist(s).
 The following VLANs exist:
  1(default), 2, 3
```

6. Сетевые маршрутизаторы в компьютерных сетях

6.1. Архитектура маршрутизаторов

6.1.1. Общая характеристика маршрутизатора и его интерфейсов

Маршрутизатор является узловым элементом составной сети, главное назначение которого — объединение подсетей таким образом, чтобы каждый компьютер мог обмениваться пакетами с любыми другими компьютерами составной сети, независимо от их принадлежности к той или иной подсети [13,30,31].

В процессе функционирования маршрутизатор использует сведения об адресации сетевого уровня из пакета данных. В маршрутизаторе имеются программные модули, реализующие алгоритмы (протоколы) маршрутизации, с помощью которых он строит таблицы маршрутизации. В соответствии с этими таблицами определяется маршрут, по которому должен быть направлен пакет, чтобы достичь конечного пункта назначения. Если маршрутизатор различает несколько форматов адресов сетевого уровня и может работать с несколькими протоколами маршрутизации, он относится к многопротокольным устройствам.

Маршрутизатор может быть реализован либо полностью программным способом — в этом случае он представляет собой модуль операционной системы, установленной на компьютере общего назначения; либо программно-аппаратным способом — тогда он является специализированным вычислительным устройством, в котором часть функций выполняется специальными устройствами, а часть — программными модулями, работающими под управлением специализированной сетевой ОС.

На нижнем уровне маршрутизатор, как и любое устройство, подключенное к сети, обеспечивает физический интерфейс со средой передачи, включая согласование уровней электрических сигналов, линейное и логическое кодирование. Кроме того, для поддержки физического интерфейса он должен быть оснащен разъемом соответствующего типа [18]

Обычно маршрутизатор имеет от двух до нескольких десятков физических интерфейсов, называемых также портами. Интерфейсы (порты) маршрутизатора предназначены для работы с каналами глобальных (WAN) либо локальных (LAN) сетей. Каждый локальный порт функционирует по строго определенной сетевой технологии: например, *Ethernet, Token Ring* или *FDDI*. Для глобальных портов определяется лишь некоторый стандарт физического уровня, поверх которого могут работать различные протоколы канального уровня в зависимости от того, как этот порт сконфигурирован. Так например, глобальный порт с поддержкой протокола физического уровня V.35 может быть настроен для работы по одному из следующих протоколов канального уровня: LAP-B (для сетей X.25), PPP (для сетей IP), LAP-F (для сетей Frame

Relay), LAP-D (для сетей ISDN). Такое отличие в реализации интерфейсов локальных и глобальных сетей объясняется тем, что каждая технология локальных сетей опирается, как правило, на свои собственные стандарты физического уровня. С точки зрения пользователя, важнейшей потребительской характеристикой маршрутизатора является перечень физических интерфейсов, поддерживаемых той или иной моделью маршрутизатора.

Физический порт имеет на корпусе устройства внешний разъем, который используется для подключения к конкретной физической линии (каналу связи). Количество физических портов является одной из основных характеристик устройства. Все порты маршрутизатора обязательно поименованы и пронумерованы, причем отсчет интерфейсов начинается с нуля. При этом полное имя интерфейса маршрутизатора содержит его тип (например, Serial) и номер, отсчитываемый с нуля. На тех маршрутизаторах, которые имеют фиксированное количество интерфейсов, нумерация интерфейсов осуществляется в соответствии с их физическим расположением (порядком следования) на корпусе маршрутизатора. Так, например, ссылка на интерфейс Ethernet0 подразумевает ссылку на первый интерфейс локальной сети. На маршрутизаторах, которые позволяют выполнять смену интерфейсов полное имя интерфейса содержит, по крайней мере, два числа, разделенных наклонной чертой. Первое число определяет номер слота, в который устанавливается интерфейсный модуль, а второе является номером порта. Например, имя интерфейса Ethernet5/0 указывает на первый интерфейс Ethernet в пятом слоте маршрутизатора. В некоторых маршрутизаторах с сетевыми адаптерами на основе многоцелевого интерфейсного процессора определение интерфейса выполняется командой interface type slot/port adapter/port number, например:

```
Router(config)#interface ethernet 2/0/0.
```

Кроме физических портов, подключаемых к линиям связи, маршрутизатор имеет логические порты, реализуемые в виде программных процессов (модулей), с которыми может быть установлено логическое соединение. В отличие от физического порта, логический порт не имеет собственного внешнего разъема. Ему обычно присваивается некоторый идентификатор (номер).

Маршрутизатор должен работать с протоколами канального и физического уровней, используемыми в подсетях, к которым он будет непосредственно присоединен. Так типовая модель маршрутизатора фирмы Cisco имеет один Ethernet порт, подключаемый к концентратору (хабу) или коммутатору локальной сети, два последовательных синхронных порта (Serial 0, Serial 1) для подключения к каналам глобальной сети и несколько асинхронных последовательных портов для подсоединения низкоскоростных оконечных устройств.

Каждый порт маршрутизатора — это конечный узел для той подсети, к которой он присоединен. Поэтому, как и всем другим конечным узлам, пор-

там маршрутизатора назначаются один (или несколько) локальных (называемых также аппаратными) адресов и один (или несколько) сетевых адресов. Под локальным адресом понимается такой тип адреса, который используется для доставки данных средствами базовой технологии в пределах подсети, независимо от того локальная эта подсеть или глобальная. Так, локальным адресом порта маршрутизатора, к которому подключен сегмент Ethernet, является шестибайтовый MAC-адрес, например 12-B3-35-3B-A0-11, а если к порту подключена сеть X.25, то — адрес X.25, имеет, например, вид 25083930785708. Если для перемещения кадра в пределах подсети используется локальный адрес, то для продвижения пакета по составной сети необходим сетевой адрес. В частности, протокол IP оперирует с сетевыми IP-адресами, которые состоят из 4 байт, например 109.26.17.100, и содержат номер сети и номер узла. Сетевые адреса должны быть уникальны в пределах всей составной сети. Иногда порты маршрутизатора вообще не имеют ни локальных, ни сетевых адресов. С такой ситуацией можно встретиться, когда порты двух соседних маршрутизаторов связаны по соединению типа «точка — точка».

6.1.2. Функции маршрутизатора на физическом, канальном и сетевом уровнях

Функции физического и канального уровней реализуются интерфейсами маршрутизатора. Они выполняют полный набор функций физического и канального уровней по передаче кадров, включая электрическое согласование со средой передачи, получение доступа к среде (если это необходимо), формирование сигналов данных, прием и передачу кадров, буферизацию кадров в своей оперативной памяти, подсчет контрольной последовательности и ликвидацию поврежденных кадров. Обработка завершается исключением заголовка кадра и извлечением из поля данных межсетевого пакета, который передается модулю сетевого протокола маршрутизатора.

Функции сетевого уровня реализуются программным способом модулями сетевого протокола и маршрутизации. Модуль сетевого протокола анализирует содержимое полей заголовка пакета. Прежде всего, он снова вычисляет контрольную последовательность, но уже не для кадра, а для пакета или части пакета: в частности, в случае пакета IP вычисляется контрольная последовательность заголовка. Если пакет пришел поврежденным, то он отбрасывается. Далее определяется время жизни пакета и если допустимое время превышено, то пакет также отбрасывается. На этом же этапе уменьшается время жизни пакета и пересчитывается контрольная последовательность.

К сетевому уровню относится также задача фильтрация трафика. Обладая более высоким интеллектуальными способностями, нежели мосты и

коммутаторы, маршрутизатор позволяет задавать и может отрабатывать значительно более сложные правила фильтрации. Маршрутизаторы способны производить разбор и анализ отдельных полей пакета. Они оснащаются развитыми средствами пользовательского интерфейса, с помощью которых администратор может задавать сложные правила фильтрации: например, в корпоративную сеть могут вообще не допускаться пакеты, кроме пакетов, которые поступают из подсетей этого же предприятия. Фильтрация в данном случае производится по сетевым адресам отправителя, и все пакеты, адреса которых не входят в разрешенный диапазон, отбрасываются. Маршрутизаторы, как правило, в состоянии анализировать и заголовки транспортного уровня, поэтому фильтры могут не пропускать в сеть пакеты определенных прикладных сервисов, например сервиса telnet или ftp, задействующих конкретные программные порты, значения которых и используются при составлении правил фильтрации.

В случае если интенсивность поступления пакетов превышает скорость, с которой они обрабатываются маршрутизатором, пакеты помещаются в буферный накопитель — очередь. Программное обеспечение маршрутизатора может реализовать различные дисциплины обслуживания очередей: в порядке поступления по правилу FIFO «первый пришел — первым обслужен» (*First Input First Output*); со случайным ранним обнаружением перегрузки, когда обслуживание идет по правилу FIFO, но при достижении длины очереди некоторого порогового значения, вновь поступающие пакеты отбрасываются, а также с применением различных вариантов приоритетного обслуживания. За счет этого при перегрузках узла соблюдаются определенные гарантии качества обслуживания: в частности, на время задержки пакетов или на пропускную способность для определенного потока пакетов, при этом первоочередное обслуживание осуществляется с использованием того же набора признаков, что и при фильтрации пакетов.

Важнейшей задачей маршрутизатора, которая решается на сетевом уровне, является определение маршрута продвижения пакета. По номеру сети, извлеченному из поля адреса назначения заголовка пакета, модуль сетевого протокола находит в таблице маршрутизации строку, содержащую сетевой адрес следующего маршрутизатора и идентификатор своего порта, на который нужно передать данный пакет, чтобы он перемещался в нужном направлении. Если в таблице отсутствует запись о сети назначения пакета и к тому же нет записи об используемом по умолчанию транзитном маршрутизаторе, то данный пакет отбрасывается.

Чтобы пакет дошел до следующего маршрутизатора, он должен быть упакован в кадр той технологии, которую использует соответствующая подсеть. А это означает, что в поле адреса назначения заголовка кадра должен быть указан локальный адрес нужного маршрутизатора. Следовательно, сетевой адрес необходимо преобразовать в локальный адрес той технологии, которая используется в сети, где находится следующий маршрутизатор. Для

этого сетевой протокол обращается с запросом к протоколу разрешения адресов. Соответствие между сетевыми и локальными адресами устанавливается либо на основании заранее составленных таблиц, либо путем рассылки широковещательных запросов по подсети. Таблица соответствия локальных адресов сетевым адресам строится отдельно для каждого сетевого интерфейса. Помимо локального адреса назначения требуется сгенерировать и другие поля заголовка, в частности: контрольной суммы; локального адреса отправителя, в качестве которого маршрутизатор вставляет локальный адрес своего порта; типа протокола сетевого уровня, который переносит кадр, а также другие поля (их конкретный набор зависит от технологии, лежащей в основе работы соответствующего порта).

При передаче пакета между подсетями, где применяются разные технологии, и у которых не совпадают максимально допустимые значения длин поля данных кадра, может потребоваться разбить пакет на несколько фрагментов; каждый из них должен быть упакован в отдельный кадр. Функция фрагментации также выполняется средствами сетевого уровня маршрутизатора. С сетевого уровня пакет, локальный адрес следующего маршрутизатора и идентификатор выходного порта передаются вниз по иерархии модулю канального уровня. На основании идентификатора порта осуществляется перемещение этих данных в выходной буфер одного из интерфейсов маршрутизатора, а затем средствами канального уровня выполняется инкапсуляция пакета в кадр соответствующего формата. В поле адреса назначения заголовка кадра помещается локальный адрес следующего маршрутизатора. Готовый кадр отправляется в сеть.

На сетевом уровне выполняется процедура построения таблиц маршрутизации, на основе которых маршрутизатор определяет оптимальный путь прохождения пакетов. Для построения таких таблиц маршрутизаторы постоянно обмениваются информацией о топологии и текущем состоянии сети в соответствии со специальным служебным протоколом маршрутизации. Программный модуль маршрутизации помещает сообщения о состоянии линий связи в поле данных пакетов сетевого, а иногда даже транспортного уровня. Обычно в расчет принимается не только топология связей, но и их пропускная способность и рабочее состояние конкретных каналов. Маршрутизаторы строят по некоторым правилам, задаваемым протоколом маршрутизации, дерево связей составной сети, на основании которого для каждого адресата принимается решение о том, какому следующему маршрутизатору (через какой порт) следует отправить пакет, чтобы путь оказался оптимальным. Полученные данные заносятся в таблицу маршрутизации. При изменении конфигурации составной сети некоторые записи в таблице становятся недействительными. В таких случаях пакеты, отправленные по ложным маршрутам, могут зацикливаться и теряться. От того, насколько быстро протокол маршрутизации приводит в соответствие содержимое таблицы реальному состоянию сети, зависит качество работы всей сети.

6.1.3. Программно-аппаратная реализация маршрутизаторов

Существует множество вариантов построения маршрутизаторов. Не зависимо от производителя коммуникационной аппаратуры, принципы построения различных маршрутизаторов во многом схожи. Поэтому рассмотрим особенности архитектуры маршрутизаторов на примере устройств фирмы Cisco. Одной из распространенных модификаций является маршрутизаторы серии 7200. Эти маршрутизаторы имеют модульную конструкцию, которая позволяет применять разнотипные канальные интерфейсные адаптеры для сопряжения с различными средами передачи.

Структурная схема маршрутизатора Cisco 7200VXR изображена на рисунке 6.1 [13].

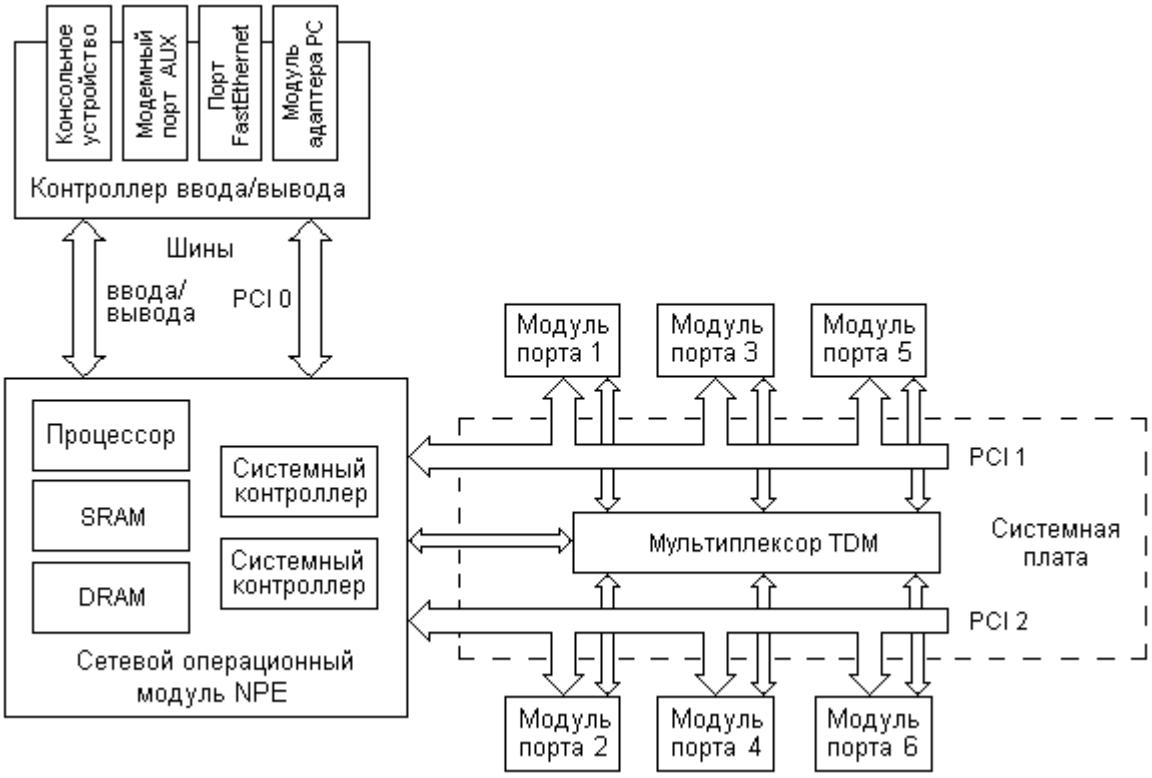


Рисунок 6.1 – Структурная схема модульного маршрутизатора

Маршрутизатор состоит из системной платы с установленной на ней модулями портов и временным мультиплексором TDM, сетевого операционного модуля NPE (*Network Processing Engine*), а также контроллера ввода/вывода и ряда слотов, в которые вставляются модули портов. В состав операционного модуля *NPE* входит процессор, статическая SRAM и динамическая DRAM память, контроллеры шин ввода/вывода и шины *PCI*. Маршрутизаторы серии 7200 используют три шины PCI. Шины PCI1 и PCI2 физи-

чески расположены между операционным модулем и системной платой и служат для соединения модулей портов с процессором и памятью. Шина PCI0 — это отдельная шина, соединяющая операционный блок с модулями управления контроллера ввода/вывода. Операционные модули обычно построены на основе RISC-процессоров с тактовой частотой от 100 до нескольких сот мегагерц (модуль NPE-300 – 300 МГц).

Контроллер ввода/вывода предназначен для подключения к процессору внешних устройств (модема, консоли, памяти NVRAM, загрузчика ROM и Flash, а также интерфейсов сети Ethernet и FastEthernet. Модули портов представляют собой независимые интерфейсные модули, содержащие приемопередатчики пакетов, поступающих из линии связи или передаваемые по ней. Интерфейсные модули строятся на основе специализированных микропроцессоров, осуществляющих высокоскоростную передачу данных по различным типам сред. Мультиплексор с временным разделением TDM обеспечивает взаимодействие портов, имеющих TDM-интерфейсы с процессором операционного модуля. Маршрутизаторы Cisco имеют три блока памяти: оперативное запоминающее устройство (ОЗУ), энергонезависимое ОЗУ NVRAM и флэш-память. Первые два из них служат для хранения конфигурации устройства, а третий блок предназначен для хранения команд операционной системы маршрутизатора IOS.

Состав программного обеспечения маршрутизатора показан на рисунке 6.3. В ОЗУ, в частности, размещаются таблицы маршрутизации, ARP-кэш, кэш быстрой коммутации, буферы пакетов (область ОЗУ совместного пользования) и очереди захваченных пакетов.

Рисунок 6.3 — Состав программного обеспечения типового маршрутизатора

При включенном питании ОЗУ также играет роль временной и/или рабочей памяти для конфигурационного файла. При отключении питания или перезапуске содержимое ОЗУ теряется. Кроме этого, ОЗУ также содержит копию сетевой операционной системы IOS корпорации Cisco.

Энергонезависимое ОЗУ NVRAM (*Non Volatile RAM)* хранит резервную копию конфигурационного файла маршрутизатора. При отключении питания или перезапуске его содержимое сохраняется.

Флэш-память реализована на основе стираемого перепрограммируемого ПЗУ. Содержимое флэш-памяти не теряется при отключении питания или перезапуске. В ней хранится образ операционной системы и микрокод. Флэш-память позволяет обновлять программное обеспечение устройства без удаления или замены микросхем на плате процессора. В маршрутизаторе может храниться несколько образов сетевой операционной системы IOS. Это зависит от объема установленной флэш-памяти и размера образов операционной системы. Кроме этого в маршрутизаторе имеется также ПЗУ, которое содержит программу диагностики устройства после включения питания, программу начальной загрузки IOS и программное обеспечение операционной системы. Для обновления версии программного обеспечения необходимо заменить на плате центрального процессора вставляемые микросхемы ПЗУ или, при возможности, перепрограммировать его.

Большинство маршрутизаторов имеет порт консоли, который используется для обращения к нему с помощью непосредственно подключаемого терминала. Порт консоли часто представляет собой порт интерфейса RS-232C или RJ-45 и обозначается надписью "Console" ("Консоль"). После начальной инсталляции маршрутизатор может конфигурироваться с консольного терминала, который представляет собой компьютер, подключенный к маршрутизатору через порт консоли. Маршрутизатор также позволяет выполнять операцию конфигурирования и с помощью других внешних источников. В частности, к нему можно подключиться посредством модема через порт дополнительного устройства (AUX). Еще одним вариантом настройки параметров маршрутизатора является конфигурация через каналы виртуального терминала с номерами от 0 до 4. Конфигурационный файл также может загружаться по сети с TFTP-сервера [2,8].

6.2. Операционная система и команды управления маршрутизаторами Cisco

В основе большинства популярных специализированных сетевых операционных систем маршрутизаторов лежит та или иная версия системы UNIX [16]. Наличие у маршрутизаторов сетевой операционной системы IOS и API для написания модулей протоколов позволяет достаточно просто изменять набор протоколов и дополнять список наличных протоколов новыми, обеспечивает высокую функциональность на сетевом уровне. Рассмотрим особенности построения сетевой операционной системы маршрутизатора Cisco IOS [4].

Все маршрутизаторы Cisco работают под управлением операционной системы Cisco IOS, однако на двоичном уровне образы IOS в разных моделях маршрутизаторов несовместимы. Для каждой модели маршрутизатора пред-

лагаются несколько разновидностей IOS. Версии IOS различаются своими функциональными возможностями. Минимальная функциональность включает в себя поддержку IP-интерфейсов, статическую и динамическую IP-маршрутизацию, поддержку мониторинга и управления по протоколу SNMP. Расширенные системы реализуют ряд дополнительных функций, в частности, поддержки технологии VoIP для передачи голоса по IP-сетям, функции межсетевого экрана, обнаружения атак IDS (*Intrusion Detection System*), криптозащиты трафика и др.

Ядром IOS является командный интерпретатор EXEC. Интерпретатор вначале идентифицирует введенную с клавиатуры команду, а затем выполняет соответствующие действия. Он состоит из двух модулей, обеспечивающих работу интерпретатора на двух уровнях. Основная интерпретация команд происходит на нижнем уровне. Работа интерпретатора на нижнем уровне выполняется в так называемом **пользовательском режиме** (*User Mode*), а работа на верхнем уровне – в **привилегированном режиме** (Privileged Mode). Ввведение двух уровней вызвано требованиями безопасности при использовании различных команд.

6.2.1. Краткое описание интерфейса пользователя

Конфигурирование маршрутизаторов фирмы Cisco, осуществляется посредством интерфейса командной строки *CLI* (*Command Line Interface*), который встроен в операционную систему *Cisco IOS*. Работать с интерфейсом командной строки можно с терминала, подключенного к маршрутизатору через консольный порт (*Console port*) или с помощью удаленного доступа по модему и Telnet-соединения по сети. Сеанс командной строки называется EXEC-сессией. Перед тем как будет возможным ввод команд исполнительного режима, необходимо осуществить вход в систему маршрутизатора.

Все команды управления маршрутизатором подразделяются на команды режима глобального и локального конфигурирования. Команды режима глобального конфигурирования действуют в отношении характеристик, которые определяют поведение коммуникационной системы в целом (общие настройки TCP/IP, установка статических маршрутов, создание списков доступа и др.). Они используются для общесистемного конфигурирования, требующего однострочных команд. Кроме того, инструкции режима глобального конфигурирования включают команды перехода в другие режимы конфигурирования, которые используются для создания конфигураций, требующих многострочных команд. Команды локального режима задают параметры, определяющие поведение конкретного устройства.

В качестве источника команд конфигурации пользователь может задать терминал, энергонезависимую память или файл, хранящийся на сетевом сервере. По умолчанию команды вводятся с терминала консоли. Консольный терминал представляет собой компьютер, подключенный к маршрутизатору

через порт консоли. При нажатии клавиши <Ввод> начинается процедура конфигурирования с терминала консоли.

Команды для активизации конкретного типа маршрутизации или конкретной функции интерфейса начинаются с команд глобального конфигурирования. В целях безопасности маршрутизаторы Cisco имеют два уровня доступа к командам.

• *Уровень пользовательского режима,* в котором выполняются типовые задачи, включая проверку состояния маршрутизатора, внесение изменений в настройки терминала, просмотр системной информации. Однако изменять конфигурацию маршрутизатора в этом режиме не возможно.

• *Уровень привилегированного режима EXEC,* на котором разрешается выполнять типовые задачи и дополнительно изменять конфигурацию маршрутизатора, задавать параметры операционной системы, получать подробную информацию о состоянии маршрутизатора, производить отладку и тестирование маршрутизатора.

Маршрутизатор интерпретирует вводимые с клавиатуры команды и выполняет соответствующие операции. Перед тем как пользователь сможет вводить команды, он должен зарегистрироваться в системе. При включении маршрутизатора на экран дисплея выводится командная строка пользовательского режима (пример 6.1). Команды, исполняемые на пользовательском уровне, представляют собой подмножество команд, доступных в привилегированном режиме. Большей частью эти команды дают возможность выводить на экран информацию без изменения установок конфигурации маршрутизатора.

При конфигурации для каждого устройства следует задавать пароль. Пароль является ключом для входа в привилегированный режим. Рекомендуется использовать для установки пароля не устаревший метод enable password, а новый — **enable secret**. При вводе цепочки символов пароля в строке enable secret символы обрабатываются специальным разработанным компанией Cisco алгоритмом шифрования. Это позволяет увеличить степень защиты последовательности символов пароля.

Чтобы получить доступ к полному набору команд, необходимо активизировать привилегированный режим. Для этого нужно ввести команду **enable** и затем ввести пароль. О переходе в **привилегированный** режим будет свидетельствовать появление в командной строке знака #. С привилегированного уровня также можно получить доступ к режиму глобального конфигурирования и другим специальным режимам конфигурирования, включая режимы конфигурирования интерфейса, подинтерфейса, линии связи, маршрутизатора, карты маршрутов и несколько дополнительных режимов конфигурирования. Для возврата из привилегированного режима в непривилегированный следует ввести команду режима EXEC **disable** (пример 6.1).

Пример 6.1. Начало и завершение работы с маршрутизатором Cisco.

```
Router>
!--- пользовательский режим
Router> enable
Password:
Router#
!--- маршрутизатор переключился в привилегированный
!--- режим
Router# disable
Router>
Router> exit
```

Вход в режим глобального конфигурирования можно произвести путем ввода из привилегированного режима команды **configure**. При поступлении этой команды режим EXEC запрашивает источник команд конфигурирования.

6.2.2. Команды пользовательского и привилегированного режимов

При вводе в командной строке пользовательского или привилегированного режима знака вопроса (**?**) на экран выводится список общеупотребительных команд. Например, если в командной строке Router> ввести символ ?, то результатом будет список команд пользовательского режима, который показан в таблице 6.1.

Таблица 6.1

Команды пользовательского режима

Команда	**Описание**
clear	Сброс функций
connect	Открытие терминального соединения
disable	Отключение исполнения привилегированных команд
disconnect	Разрыв существующего соединения в сети
enable	Включение исполнения привилегированных команд
exit	Выход из режима EXEC
hel	Выдача описания интерактивной системы помощи
login	Вход в систему под именем конкретного пользователя
logout	Выход из режима EXEC
ping	Посылка эхо-сообщений
show	Показ текущих рабочих установок системы

Для входа в привилегированный режим EXEC необходимо набрать на клавиатуре команду **enable**, а также ввести пароль. Ввод знака вопроса (?) в командной строке привилегированного режима Router# ? приведет к выводу на экран более длинного списка команд. Наиболее широко используемые из этих команд приведены в таблицах 6.2 – 6.4.

Таблица 6.2

Команды привилегированного режима

Команда	**Описание**
`clear`	Сброс функций
`configure`	Вход в режим конфигурирования
`connect`	Открытие терминального соединения
`disable`	Отключение исполнения привилегированных команд
`disconnect`	Разрыв существующего соединения в сети
`enable`	Включение исполнения привилегированных команд
`exit`	Выход из режима EXEC
`help`	Выдача описания интерактивной системы помощи
`rlogin`	Открытие соединения удаленного входа в систему
`sdlc`	Посылка тестовых SDLC-кадров
`telnet`	Открытие Telnet-соединения
`terminal`	Установка параметров терминального канала

Все команды и параметры при вводе с командной строки могут быть сокращены (например, "enable" — "en", "configure terminal" — "conf t"); если сокращение окажется неоднозначным, маршрутизатор сообщит об этом, а по нажатию клавиши табуляции выдаст варианты, соответствующие введенному фрагменту.

Таблица 6.3.

Команды для конфигурирования глобальных параметров

Команда	**Назначение**
`configure terminal`	Задает режим конфигурации
`hostname` *`name`*	Задает имя маршрутизатора
`enable secret` *`password`*	Устанавливает пароль в режиме secret
`ip subnet-zero`	Установка адресации на нулевую подсеть
`no ip domain-lookup`	Деактивирует функции маршрутизатора поиска по DNS, которые в большинстве случаев не требуются для выполнения стандартных операций

Имена сетевых интерфейсов также могут быть сокращены, например, вместо "ethernet0/1" достаточно написать "e0/1", а вместо FastEthernet 0/1 – fa 0/1.

Таблица 6.4

Команды для конфигурирования глобальных параметров

Команда	**Назначение**
`interface ethernet 0`	Включает режим конфигурации для Ethernet- интерфейса
`ip address` *`ip-address mask`*	Задает IP-адрес и маску подсети для Ethernet- интерфейса
`no shutdown`	Активирует Ethernet- интерфейс, переводит из состояния «Down» в «Up»
`exit`	Выключает режим конфигурации Ethernet- интерфейса

В любом месте командной строки для получения помощи может быть использован вопросительный знак ? (Таблица 6.5).

Таблица 6.5

Примеры запроса помощи

Команда	**Комментарий**
`router#?`	список всех команд с комментариями
`router#co?`	список всех слов в этом контексте ввода, начинающихся на "co"; пробел перед "?" не ставить
`router#conf?`	список всех параметров, которые могут следовать за командой config — перед "?" ставить пробел

6.2.3. Конфигурирование маршрутизаторов

Под конфигурированием маршрутизатора понимают процедуру настройки его параметров и режимов работы путем занесения команд конфигурации в память маршрутизатора. Различие между командами конфигурирования и операционной системой заключается в том, что команды конфигурирования служат для задания параметров и режимов работы (формирования конфигурации) маршрутизатора, а операционная система — это программное обеспечение, исполняемое на данном устройстве и обеспечивающее его функционирование в соответствии с назначением.

После подачи питания на маршрутизатор запускается программа начальной загрузки, находящаяся в его ПЗУ. В дальнейшем, во время работы маршрутизатора, для хранения информации используется ОЗУ. В начале работы программа начальной загрузки выполняет ряд тестов и затем загружает в ОЗУ межсетевую операционную систему IOS. Одной из частей ОС IOS яв-

ляется модуль управления исполнением команд EXEC, который принимает и выполняет команды, вводимые в маршрутизатор.

Кроме этого, в памяти маршрутизатора также содержится активный файл конфигурации, списки адресов маршрутизации, таблицы маршрутизации. Содержимое конфигурационного файла может быть выведено на экран удаленного терминала или на экран консоли. Сохраненная версия этого файла хранится в энергонезависимом ОЗУ. Каждый раз при инициализации маршрутизатора выполняется обращение к этому сохраненному файлу и его загрузка в основную память. Конфигурационный файл содержит информацию об общесистемных настройках, настройках процессов и интерфейсов, которая непосредственно определяет работу маршрутизатора и его интерфейсных портов.

Образ операционной системы не может быть выведен на экран терминала, обычно он исполняется из основного ОЗУ и загружается из одного из нескольких источников. Операционная система организована в виде подпрограмм, которые обрабатывают различные задачи, связанные с сетевыми протоколами, перемещением данных, управлением таблицами и буферами, маршрутизацией пакетов и выполнением команд пользователя.

Как уже отмечалось выше, независимо от того, каким образом осуществляется обращение к маршрутизатору, через консоль или в рамках сеанса протокола Telnet через порт вспомогательного устройства, маршрутизатор может быть установлен в один из нескольких режимов. Интерфейс пользователя ОС IOS обеспечивает доступ к режимам выполнения команд, каждый из которых обладает различными функциями.

• *Пользовательский режим EXEC* — это режим просмотра, в котором пользователь может только просматривать определенную информацию о маршрутизаторе, но не может ничего менять. В этом режиме используется командная строка вида **Router>.**

• *Привилегированный режим EXEC* — поддерживает команды отладки и тестирования, детальную проверку маршрутизатора, манипуляции с конфигурационным файлом и доступ к режимам конфигурирования. В нем используется командная строка вида **Router#.**

• *Режим начальной установки (setup)* — обеспечивает диалоговое взаимодействие с подсказками через консоль, которое позволяет новому пользователю создать начальную базовую конфигурацию.

• *Режим глобального конфигурирования* — реализует однострочные команды, решающие простые задачи конфигурирования. В нем используется командная строка вида **Router (config) #.**

• *Другие режимы конфигурирования* — в них выполняется более сложное многострочное конфигурирование.

В таблице 6.6 представлены используемые режимы конфигурации маршрутизатора и соответствующий вид командной строки.

Таблица 6.6

Режимы конфигурирования и виды командной строки

Режим конфигурирования	**Вид командной строки**
Интерфейса	`Router (config-if)#`
Подынтерфейса	`Router (config-subif)#`
Контроллера	`Router (config-controller)#`
Карты виртуальных каналов	`Router (config-map-list)#`
Карты классов	`Router (config-map-class)#`
Канала	`Router (config-line)#`
Маршрутизатора	`Router (config-router)#`
IPX	`Router (config-ipx-router)#`
Карты маршрутов	`Router (config-route-map)#`

Для перехода на один уровень назад необходимо с клавиатуры ввести слово **exit** ("выход"). Ввод слова **exit** в одном из специальных режимов конфигурирования возвращает пользователя в режим глобального конфигурирования.

Нажатие комбинации клавиш <Ctrl+Z> приводит к полному выходу из режима конфигурирования и возвращает маршрутизатор в привилегированный режим EXEC.

6.3. Примеры конфигурирования маршрутизаторов Cisco

6.3.1. Задание имени и настройка паролей

Для присвоения имени маршрутизатору необходимо в сценарии конфигурации выполнить следующую последовательность команд:

```
Router>
Router>enable
Router#
Router#configure terminal
Router(config)#
Router(config)#hostname SevNTU-IS
SevNTU-IS(config)#
```

Чтобы отменить назначенное имя и вернуться к имени по умолчанию (`Router`) следует ввести и выполнить команду no hostname:

```
SevNTU-IS(config)#no hostname Router(config)#
```

Для защиты маршрутизатора Cisco используются пять паролей. Первые два пароля служат для установки разрешенного пароля, который защищает

привилегированный режим. Такое название пароль получил потому, что он запрашивается у пользователя после ввода команды `enable`. Остальные три пароля служат для настройки паролей для доступа пользователя через консольный порт, вспомогательный порт и по протоколу Telnet.

Кроме разрешенного существует и секретный пароль. Особенностью секретного пароля **enable secret** является то, что он хранится в Cisco IOS зашифрованным, в то время как все остальные пароли хранятся открытыми.

1. Задание разрешенного пароля для доступа к привилегированному режиму
```
Router(config)# enable password Cisco
!-- задание пароля Cisco
```

2. Задание секретного пароля для доступа к привилегированному режиму.
```
Router(config)# enable secret Cisco
!-- задается пароль Cisco
```

3. Настройка пароля доступа к консоли маршрутизатора. Для установки пароля консоли служит команда line console 0.
```
Router(config)# line console 0
Router(config-line)# login
Router(config-line)# password Cisco
!-- задается пароль Cisco для доступа с консольного порта
!-- к маршрутизатору
```

4. Настройка пароля доступа к дополнительному порту маршрутизатора AUX.
```
Router(config)# line aux 0
Router(config-line)# login
Router(config-line)# password Cisco
!-- задается пароль Cisco  для доступа с дополнительного консольного
!-- порта к маршрутизатору.
```

5. Настройка пароля виртуальных терминалов маршрутизатора. Для установки пароля пользовательского режима при доступе по Telnet к маршрутизатору служит команда `line vty`. Маршрутизаторы, которые не исполняют версию Enterprise операционной системы Cisco IOS, по умолчанию имеют пять линий VTY (от 0 до 4).
```
Router(config)# line vty 0 4
Router(config-line)# login
Router(config-line)# password Cisco
!-- установка пароля Cisco для доступа через Telnet.
```

В целях безопасности рекомендуется устанавливать различные пароли на разных уровнях доступа. При установке пароля необходимо обеспечить высокий уровень сложности пароля, опираясь на следующие рекомендации:

• задавать пароли длиной не менее восьми символов;

• использовать комбинацию цифр и символов в верхнем и нижнем регистре;

• избегать применения одинаковых паролей на разных устройствах;

• не допускать использования слов типа „password“ и „administrator“, так как такие „пароли“ легко угадываются.

6.3.2. Начальная конфигурация интерфейсов

Конфигурация интерфейсов является наиважнейшей процедурой маршрутизатора. К конфигурационным параметрам интерфейса относятся: адрес сетевого уровня, тип среды передачи, полоса пропускания и другие административные характеристики.

Все интерфейсы маршрутизатора после запуска устройства автоматически находятся в режиме административного отключения. Для включения отключенного интерфейса используется команда `Router (config-if)# no shutdown`. Отключение интерфейса производится посредством команды `Router(config-if)# shutdown`. Ввод последовательности команд для сохранения параметров конфигурации в памяти маршрутизатора должен заканчиваться командой `exit`.

Чтобы узнать, количество и номера интерфейсов, нужно в командной строке задать вид интерфейса и ввести знак вопроса. Так, например, при проверке последовательных портов serial и портов локальной сети Ethernet нужно ввести следующие команды.

```
Router(config)#int serial ?
<0-9> Serial interface number
```

!-- Показывает, что маршрутизатор располагает десятью последовательными портами с номерами от 0 до 9.

После выбора нужного номера интерфейса происходит переключение в конфигурацию этого интерфейса. Например, для выбора последовательного порта 5 следует ввести следующую команду:

```
Router(config)#int serial 5
Router(config-if)#
```

Аналогично можно просмотреть наличие и количество Ethernet –портов:

```
Router(config)#int ethernet ?
<0-0> Ethernet interface number
```

!-- Сообщение `<0-0>` показывает, что маршрутизатор располагает только !-- одним портом Ethernet с номерами 0.

```
Router(config)#int ethernet 0
Router(config-if)#
```

Подачей соответствующих команд можно установить параметры функционирования портов Ethernet, Token Ring или последовательного (Serial) порта. На возможность выполнения процедуры конфигурирования указывает появление командной строки вида **Router (config-if)#.** Для начала процедуры конфигурирования интерфейса необходимо подать глобальную команду **interface,** а за ней следуют ввести интерфейсные подкоманды, которые уточняют параметры интерфейса. В качестве типа интерфейса используются значения **serial, ethernet, fastethernet, token ring** и др.

Для настройки последовательного интерфейса нужно знать его особенности. Интерфейс подключается к устройству типа CSU/DSU (см. рисунок 1.2), которое обеспечивает тактовую частоту в линии. При использовании конфигурации "точка-точка" только один участник соединения должен предоставлять тактовую частоту. Это может быть оконечное устройство канала данных DCE. Маршрутизатор Cisco по умолчанию является устройством DTE, поэтому необходимо явно указать интерфейсу на предоставление тактовой частоты, если этот интерфейс работает в режиме DCE. Настройка последовательного интерфейса на режим DCE выполняется командой clockrate. В связи с этим, если интерфейс должен обеспечить генерацию тактовых импульсов, то с помощью команды **clockrate** необходимо задать частоту тактовых импульсов. Для изменения значения полосы пропускания (скорости передачи), установленной проектировщиками по умолчанию, применяется команда **bandwith** (пример 6.2).

Пример 6.2

```
Router# configure terminal
Router(config)# interface serial 1/0
!--- последовательный интерфейс, 0-й порт 1-й слот
Router(config-if)# bandwith 56
!--- пропускная способность 56 кбит/с
Router(config-if)# clockrate 56000
!--- тактовая частота передачи 56 кГц
Router(config-if)# exit
```

Один интерфейс маршрутизатора Cisco может поддерживать несколько виртуальных каналов (постоянных или коммутируемых). В этом случае каждый виртуальный канал рассматривается как отдельный интерфейс, называемый *подинтерфейсом.* Подинтерфейсы могут быть реализованы для любой технологии компьютерной сети, использующей виртуальные каналы.

При задании подинтерфейса после команды **int** указывается технология сети, а для установления номера подинтерфейса после номера порта ставится точка и номер подинтерфейса. Процедура задания подинтерфейса для сети Fast Ethernet представлена в примере 6.3.

Пример 6.3.

```
Router(config)#int Fa0/0.?
!--- Просмотр возможных номеров подинтерфейсов
<0-4294967295> FastEthernet interface number
Router(config)#int Fa0/0.1
!--- Приглашение меняется на Router(config-subif)#
Router(config-subif)#
```

6.3.3. Конфигурация интерфейсов глобальных сетей

Подключение маршрутизаторов к глобальным сетям осуществляется посредством последовательных портов. Для этого каждый из маршрутизаторов снабжается несколькими последовательными интерфейсами (портами), которые обозначаются serial 0, serial 1 и т.д.

Коммуникационные устройства Cisco поддерживают практически все типы протоколов глобальных сетей и удаленного доступа к сети по коммутируемым каналам связи [17,23,28]:

- HDLC (*High-Level Data Link Control*);
- PPP (*Point-to-Point Protocol*);
- FR (*Frame Relay*);
- ATM (*Asynchronous Transfer Mode*);
- DSL (*Digital Subscriber Line*).

Формат передаваемых данных и тип протокола канального уровня для определенного интерфейса зависит от вида инкапсулирования, который устанавливается с помощью подкоманды конфигурирования интерфейса **`encapsulation`** [16].

Конфигурирование интерфейса PPP. Для активирования на интерфейсе последовательной передачи данных serial 1 синхронного варианта протокола PPP, используется подкоманда конфигурирования интерфейса **`encapsulation ppp`**. В примере 6.4 приведен сценарий конфигурирования интерфейса serial l/1 маршрутизатора с именем Router на работу с синхронным протоколом PPP:

Пример 6.4.

```
Router#configure
Router(config)#nterface serial 1/1
Router(config-if)#encapsulation ppp
Router(config-if)# ^Z
```

Конфигурация портов Frame Relay. При работе по каналам сети Frame Relay нужно использовать последовательный интерфейс маршрутизатора, например, serial0. Для его конфигурации следует подать подкоманду

конфигурирования интерфейса **encapsulation frame-relay.** Затем необходимо связать с интерфейсом идентификатор канального соединения DLCI и указать его номер, например, 100. Данное действие реализуется подкомандой `frame-relay interface-dlci`. Устройства Cisco по умолчанию используют на интерфейсах Frame Relay протокол Cisco LMI (*Local Management Interface*). Однако с помощью подкоманды конфигурации интерфейса **frame-relay lmi-type** можно явно установить тип стандартного интерфейса LMI. Сценарий конфигурации интерфейса Frame Relay представлен в примере 6.5.

Пример 6.5.

```
Router#configure
Router(config)#interface serial 0
Router(config-if)#encapsulation frame-relay
Router(config-if)#frame-relay interface-dlci 100
Router(config-if)#frame-relay interface lmi-dlci
Router(config-if)#^Z
```

Последняя строка — комбинация клавиш CNTL/Z означает завершение процедуры конфигурации.

Конфигурирование интерфейсов ATM. Интерфесы глобальной сети с асинхронным режимом доступа в маршрутизаторах компании Cisco реализованы в виде многоцелевых интерфейсных процессоров VIP (*Versatile Interface Processor*) или адаптеров порта для VIP-карт. Это означает, что для ATM-интерфейса нет необходимости использовать подкоманду конфигурирования интерфейса **encapsulation**. Сама аппаратная часть маршрутизатора поддерживает процедуру инкапсуляции кадров только по протоколу ATM. Поэтому сетевой администратор должен лишь задать виртуальные каналы, сушествующие на данном интерфейсе. Для этого применяется интерфейсная подкоманда atm pvc. В примере 6.6 приведен сценарий конфигурирования постоянного виртуального канала для соединения уровня AAL5 с нулевым виртуальным путем и виртуальным каналом номер 100.

Пример 6.6.

```
Router#configure
Router(config)#interface atm 2/0
Router(config-if)#atm pvc 1 0 100
Router(config-if)#^Z
```

Работоспособность настроек физического и канального уровней интерфейсов можно проверить командой

router# show interface <интерфейс>

Работоспособность интерфейса индицируется двумя состояниями (up или down). Сообщение "interface up/down" информирует, функционирует ли

физический уровень, а "line protocol up/down" — канальный уровень. В штатном режиме оба уровня должны находиться в положении "up". Если интерфейс находится в состоянии "down", то наиболее вероятная причина — не подсоединенный или поврежденный кабель. Кроме того, интерфейс может находиться в состоянии "administratively down", в которое он переходит по команде shutdown.

Если выдается сообщение "line protocol down", то наиболее вероятные причины следующие:

- отсутствие сквозного соединения (линия разорвана, удаленный модем или маршрутизатор не работают) или связь работает только в одном направлении;
- несоответствие протоколов на разных концах линии;
- при использовании непромышленных кабелей — неверно спаянный кабель.

6.3.4. Настройка IP-адреса интерфейса и протокола маршрутизации

Настройка IP-адреса осуществляется в привилегированном режиме. Для установки IP-адреса интерфейса служит команда **ip address <адрес> <маска сети>**, вводимая в режиме конфигурирования интерфейса.

Пример 6.7. Сконфигурировать маршрутизатор, в котором имеются интерфейсы типа FastEthernet. Интерфейс Fa0/0 подключен к сети Интернет. Провайдером выделен публичный адрес класса С вида 237.12.17.4. Второй интерфейс Fa1/0 соединен с локальной сетью с частным адресом 192.168.44.0.

```
Router(config)# interface interface Fa0/0
Router(config-if)# ip address 237.12.17.4 255.255.255.0
!-- указывается адрес и сетевая маска
Router(config-if)# no shutdown
!-- производится административное включение интерфейса
Router(config-if)# exit
!-- сохранение конфигурации
Router(config)# interface interface Fa1/0
Router(config-if)# ip address 192.168.44.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# exit
Router# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Для удаления команды конфигурирования из устройства в начало команды конфигурирования добавляется ключевое слово **no**. В примере 6.8 показано удаление IP-адреса, присвоенного интерфейсу FastEthernet0/0:

Пример 6.8.

```
Router# configure
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CTRL+Z.
Router(config)#interface Fa0/0
Router(config-if)#no ip address 237.12.17.4 255.255.255.0
Router(config-if)#^Z
Router#
```

Проконтролировать включение интерфейса можно с помощью команды **show interface Fa0/0**. В результате ее исполнения отображается состояние данного интерфейса (выключен или включен).

Если ввести другой IP-адрес и нажать «Ввод», то будет заменен существующий IP-адрес и маска подсети. В случае необходимости назначения интерфейсу второго адреса подсети, следует применить команду secondary.

```
Router(config-if)#ip address 172.16.20.2 255.255.255.0
secondary
Router(config-if)#^Z
```

Проверить конфигурирование обоих адресов интерфейса можно с помощью команды **show running-config** (сокращенная форма: sh run). Фрагмент сообщения, выдаваемого на экран дисплея в результате выполнения команды, имеет вид:

```
Router# show running-config
Building configuration...
Current configuration:
interface Ethernet0
ip address 172.16.20.2 255.255.255.0 secondary
ip address 172.16.10.2 255.255.255.0
```

При необходимости можно использовать безклассовую адресацию CIDR (*Classless Inter-Domain Routing*). Тогда команда будет выглядеть следующим образом:

```
Router(config-if)#ip address 192.168.100.1/24
```

Если нужно настроить интерфейс WAN на использование протокола DHCP для автоматического получения IP-адреса, то следует ввести следующие команды:

```
Router(config)#interface FastEthernet4
```

```
Router(config-if)#ip address dhcp
```

Для задания номер IP-сети или подсети, определенной в качестве пункта назначения по умолчанию применяется команда

```
ip default-network <номер сети>
```

Для конфигурации протокола маршрутизации (например, RIP и IGRP) используется приглашение `(config-router)#`.

```
Router#config t
Enter configuration commands, one per line. End with
CNTL/Z.
Router(config)#router rip
Router(config-router)#
```

6.3.5. Создание списков управления доступа

В процессе конфигурации маршрутизаторов или коммутаторов третьего уровна достаточно широко применяются списки управления доступом ACL (*Access-control-lists*). Они используются в процедурах трансляции адресов, для фильтрации информационных потоков, указание при определении класов пакетов и регламентации доступа в процессе реализации политики безопасности. Общие сведения о списках доступа кратко рассмотрены в подразделе 4.4. В данном подразделе освещаются особенности создания и конфигурации списков управления доступом.

Как уже отмечалось в пп.4.4 списки доступа подразделяются на стандартные и расширенные. Спискам доступа назначаются определенные номера. Стандартные списки могут нумероваться только в диапазоне 1-99. Они предназначены для фильтрации пакетов только по IP-адресу источника. Расширенные списки доступа могут фильтровать пакеты по адресам источников и получателей, а также по видам протоколов 3-го и 4-го уровней и номерам портов. Расширенным спискам присваиваются стандартные номера только в диапазоне от 100 до 199. Стандартным и расширенным спискам вместо номеров могут быть присвоены символические имена, которые облегчают работу администратора сети.

Для создания **стандартного списка доступа** для маршрутизаторов Cisco применяется команда **access-list**, которая вводится в следующем формате:

```
access-list <номер_списка> {deny|permit} <адрес отправителя>
[маска шаблона адреса] [log]
```

Маска шаблона (англ. *wildcard mask*) указывает маршрутизатору на те биты в шаблоне адреса отправителя, которые следует сравнивать с поступившим в порт маршрутизатора адресом отправителя, и те, которые нужно

проигнорировать [12,13]. Как и маска в схеме адресации протокола IP, маска шаблона в списке доступа состоит из 32-х битов, записанных в точечно-десятичной форме. Например, маска шаблона 0.0.0.255 соответствует двоичному представлению 00000000.00000000.00000000.11111111. Однако запись маски шаблона в списках доступа, в отличие от метода записи маски адреса на сетевых интерфейсах, записана инверсно, т.е. единицами отмечены биты адреса, которые НЕ будут проверяться. Нулевые биты в маске списка доступа предписывают маршрутизатору необходимость сравнения соответствующих битов IP-адреса в проверяемом пакете с аналогичными битами в шаблоне адреса. Соответственно, единичные биты указывают на то, что сравнение производить не нужно. Таким образом, маска 0.0.0.0 вынуждает маршрутизатор сравнивать все 32 бита адреса пакета на соответствие их битам шаблона, заданного в списке доступа.

Ключевое слово "log" инициирует выдачу записи о совпадении пакета с данным предписанием на консоль и в системный лог-файл. Часто используемое описание фильтра, которому удовлетворяет любой адрес 0.0.0.0 255.255.255.255, имеет специальное обозначение "any":

```
access-list <access-list-number> {deny | permit} any
```

В **расширенном списке** перед полем адреса источника можно указывать тип протокола, а после адреса источника указываеются (при необходимости) адрес хоста назначения и порт. Общий формат расширенного списка доступа имеет следующий вид:

access-list номер-списка {permit | deny} {протокол} {адрес источника}[маска-источника][адрес получателя] [маска-получателя] [оператор номер порта] [established] [log]

Параметры списка могут принимать значения:
оператор — it, gt, eq, neq (меньше чем, больше чем, равно, не равно);
established — разрешает прохождение TCP-потока если он использует установленное соединение (т. е. если бит АСК в заголовке сегмента установлен). Частные случаи записи могут иметь вид:

access-list access-list-number {deny|permit} протокол any any

или

access-list access-list-number {deny | permit} протокол host source host destination

Если в качестве протокола указано "tcp" или "udp", то описания source- и destination-wildcard могут включать номера портов для данных протоколов с ключевыми словами "eq" (*equal*) — равно, neq (*not equal*) — не равно, "lt" (*less than*) — меньше чем, "gt" (*greater then*) — больше чем, "range" — указание диапазона номеров портов. Для протокола "tcp", возможно также применение слова "established" для выделения только установленных tcp-сессий. Ключевое слово "hostsource" эквивалентно записи: "source 0.0.0.0".

При использовании именованных списков в список добавляется оператор, указывающий на стандартный (*standard*) или расширенный (*extended*) список доступа. Синтаксис такого списка имеет вид:

```
ip access-list {standard | extended} {<номер ACL> и <имя ACL>}
```

Пример 6.9. Запретить прохождение через маршрутизатор пакетов с рабочей станции с IP-адресом 235.12.60.23 и пропустить все остальные.

В связи с тем, что запрет осуществляется только по адресу источника, используем стандартный список доступа, присвоив ему номер 4.

```
access-list 4 deny host 235.12.60.23
access-list 4 permit any
```

Для удаления списка доступа необходимо сначала ввести команду `no ip access-group` с номером списка для каждого интерфейса, на котором он использовался, а затем команду `no access-list` с номером списка.

При составлении сценариев конфигурации маршрутизаторов следует помнить, что команды всех видов списков доступа вводятся в режиме конфигурирования маршрутизатора, который индицируется промптом: `Router(config)#.`

6.3.6. Просмотр, проверка и сохранение конфигурации

После завершения процедуры настройки IOS маршрутизатора выводит приглашение на сохранение созданной конфигурации. Если ответить **yes**, то конфигурация будет записана в память DRAM (т.е. станет исполняемой конфигурацией), в память NVRAM или в файл с именем startup-config. Можно вручную скопировать файл из DRAM в NVRAM командой

```
Copy running-config startup-config.
```

Краткая форма данной команды: **`Router#copy run start.`**

Для просмотра файла конфигурации следует выполнить команду `show running-config или show startup-config` в привилегированном режиме. В результате выполнения команды `Router#show running-config` (краткая форма `sh run`) отобразится текущая конфигурация. При выпонении команды `Router#show startup - config` (краткая форма `sh start`) выведется объем памяти, используемой NVRAM для хранения файла `startup-config` и отобразится конфигурация, которая будет использоваться при следующей перезагрузке маршрутизатора.

На начальном этапе проверки конфигурации осуществляется ее просмотр (командой `show running-config`) на предмет выявления очевидных ошибок, сделанных при вводе команд. С помощью команды `show`

startup-config можно проверить конфигурацию, установленную для загрузки при следующем перезапуске маршрутизатора.

На втором этапе с помощью команды show interface необходимо выполнить промотр каждого из интерфейсов телекоммуникационных устройств и проверить корректность установки их параметров. Наиболее важными в листинге команды show interface являются сведения о выходных линиях связи и о статусе протокола канального уровня. Если включен интерфейс Ethernet0, то включены канальные протоколы и работает сама линия. Если же линия включена, но выключен протокол (Serial0 is up, line protocol is down), то возникают проблемы с тактовой частотой или кадрами. Необходимо проверить значение параметра keepalive на обоих концах связи. Эти значения должны совпадать, также должны быть установлены частоты тактовых импульсов (при необходимости) и совпадать тип инкапсуляции на обоих концах соединения. Еще одним важным конфигурационным параметром является время поддержания жизни маршрутизатора (keepalive), который по умолчанию равен 10 с. Любой маршрутизатор посылает своему соседу сообщение keepalive через каждые 10 с. Если оба маршрутизатора не настроены на одинаковый интервал keepalive, то взаимодействие маршрутизаторов не возможно.

На третьем этапе следует убедиться в правильности конфигурации оборудования путем пингования устройств и просмотра трассировки пути, по которому перемещаются пакеты (утилиты Ping и Trace). На заключительном этапе для тестирования правильности настройки целесообразно использовать утилиту службы Telnet, в которой для создания сеанса с удаленным хостом на сетевом уровне используется протокол IP, а на транспортном уровне — TCP. Если к устройству можно обратиться по Telnet, следовательно подключение его по IP является правильным. В приглашении маршрутизатора не обязательно вводить команду telnet. Если в командной строке ввести имя хоста или IP-адрес, то по умолчанию предполагается использование Telnet.

6.4. Конфигурирование интерфейсов для реализации процедур трансляции адресов

6.4.1. Команды статической и динамической трансляции адресов

Настройка процедуры NAT на маршрутизаторах Cisco, работающих под управлением IOS включает в себя следующие шаги.

1. Назначить внутренний (Inside) и внешний (Outside) интерфейсы.
2. Определить какие IP-адреса нужно транслировать.
3. Выбрать вид трансляции (статический или динамический).

4. Выполнить проверку корректности трансляций.

Внутренним интерфейсом обычно выступает тот, к которому подключена локальная сеть, а внешним — к которому подключена внешняя сеть, например сеть Интернет-провайдера.

Для обозначения интерфейса в качестве внешнего (*outside*) или внутреннего (*inside*) применяется команда

```
ip nat inside|outside .
```

При статической NAT один адрес из внутренней сети преобразуется в один адрес внешней сети. Задание режима статической трансляции осуществляется путем ввода команды

```
ip nat inside source static <локальный адрес> <глобальный адрес>
```

При этом транслироваться будут только пакеты, поступающие на обозначенный интерфейс.

Динамическая трансляция предполагает назначения диапазона адресов (адресного пула) с указанием начального и конечного адресов и маски сети. В случае необходимости трансляции клиентам, выходящим во внешнюю сеть, будут выделяться адреса из этого пула. Формат команды назначения адресного пула имеет следующий вид:

```
ip nat pool <имя> <первый адрес> <последний адрес> netmask
<маска подсети> или prefix-length <длина префикса> .
```

Определение стандартного списка доступа, задающего адреса, подлежащие трансляции, выполняется командой:

```
Router(config)#access-list <номер> permit <адрес или блок
адресов> .
```

Для разрешения динамической трансляции адресов внутренних источников применяется команда:

```
Router(config)#ip nat inside source list <номер списка до-
ступа> pool <имя> [overload] .
```

Ключевое слово [overload] разблокирует трансляцию порта для сеансов UDP и TCP. Пакеты, отправляемые из адресов, соответствующих адресам в списке простого доступа, транслируются, используя глобальные адреса, распределяемые из указанного пула.

Процедура NAT потребляет значительное процессорное время маршрутизатора. Поэтому часто возникает необходимость в ограничении временных или количественных характеристик данной процедуры. В частности, можно ограничить максимальное количество пользователей, за одним IP-адресом или время действия (время жизни) процедуры NAT.

Процесс динамической трансляции можно запретить (блокировать) после окончания определенного временного интервала отсутствия работы. Так,

если трансляция порта не установлена, то по умолчанию трансляция в соединениях TCP отключается после 24 часов работы. Время блокирования можно настраивать путем задания команды

```
Router(config)#ip nat translation timeout <секунд>
```

или следующих ее вариантов:

```
Router(config)#ip nat translation udp-timeout < секунд >;
Router(config)#ip nat translation dns-timeout < секунд >;
Router(config)#ip nat translation tcp-timeout < секунд >;
Router(config)#ip nat translation finrst-timeout < секунд >.
```

В случае необходимости протоколирования процедуры трансляции адресов следует воспользоваться командой **syslog**:

```
Router(config)# ip nat log translations syslog
Router(config)# no ip natlog translations syslog
                !-- отключить процедуру протоколирования.
```

Проверка корректности трансляции адресов осуществляется путем просмотра таблицы трансляции адресов, которая выводится на монитор в результате выполнения команды

```
Router#show ip nat translations .
```

6.4.2. Последовательность реализации процедур трансляции адресов при конфигурации интерфейсов

Для конфигурации статической трансляции необходимо выполнить следующие действия:

1) установить режим статической трансляции между внутренним локальным адресом и внутренним глобальным адресом;

   ```
   ip nat inside source static <локальный адрес> <глобальный адрес>
   ```

2) указать внутренний интерфейс;

   ```
   interface <тип> <номер>
   ```

3) пометить данный интерфейс, как принадлежащий внутренней сети;

   ```
   ip nat inside
   ```

4) указать внешний интерфейс;

   ```
   interface <тип> <номер>
   ```

5) пометить данный интерфейс, как принадлежащий внешней сети;

   ```
   ip nat outside .
   ```

Для конфигурации динамической трансляции нужно выполнить следующие действия:

1) определить пул глобальных адресов;

   ip nat pool <имя> <первый адрес> <последний адрес> [net-mask <маска подсети> или prefix-length <длина префикса>]

2) определить стандартный список доступа, регламентирующий адреса, подлежащие трансляции;

   access-list <номер> permit <адрес или блок адресов>

3) установить динамическую трансляцию на основе списка доступа, определенного на предыдущем шаге;

   ip nat inside source list <номер списка доступа> pool <имя>

4) указать внутренний интерфейс;

   interface <тип> <номер>

5) пометить данный интерфейс, как принадлежащий внутренней сети;
   ip nat inside

6) указать внешний интерфейс;

   interface <тип> <номер>

7) пометить данный интерфейс, как принадлежащий внешней сети.
   ip nat outside .

Пример 6.10. Маршрутизатор имеет два порта типа Ethernet. К интерфейсу Ethernet1 подключена локальная сеть с адресом 192.168.1.0, а к интерфейсу Ethernet0 – линия Интернет-провайдера. Составить сценарий конфигурации маршрутизатора, чтобы обеспечить выход в Интернет всем компьютерам, входящим в локальную сеть 192.168.1.0 . Провайдером для выхода в Интернет выделена группа адресов 171.69.233.208/28.

Запись адреса 171.69.233.208/28 означает, что первым адресом в группе публичных адресов будет 171.69.233.209, а последним 171.69.233.222 (двоичный эквивалент 208 равен 11010000, поэтому при сетевом префиксе длиной 28 бит на адресацию выделено 4 бита). Адреса хостов 0000 и 1111 не используются.

Сценарий конфигурации имеет следующий вид:

```
ip nat pool net-16 171.69.233.209 171.69.233.222 netmask
255.255.255.240
access-list 1 permit 192.168.1.0 0.0.0.255
ip nat inside source list 1 pool net-16 overload
!--
interface Ethernet1
ip nat inside
!--
interface Ethernet0
ip nat outside
```

6.5. Примеры конфигурации маршрутизаторов для реализации политики безопасности

Для реализации политики безопасности на основе списков доступа необходимо вначале создать список управления доступом, а затем применить его к интерфейсу. Рассмотрим процедуры создания различных видов списков доступа на примере настройки маршрутизаторов фирмы Cisco. Конфигурирование маршрутизаторов других производителей отличается незначительно. Примеры конфигурации таких маршрутизаторов приводятся в технической документации на это оборудование. В ряде устройств конфигурирование списков доступа упрощено и осуществляется путем задания параметров в меню.

Пример 6.11. Составить список доступа, на основании которого маршрутизатор разрешает прохождение трафика с рабочей станции (хоста) сети, имеющей адрес 192.168.3.2.

Запись команды списка доступа должна иметь следующий вид:

```
access-list 1 permit 192.168.3.2 0.0.0.0 .
```

Важно помнить, что списки доступа являются однонаправленными. Когда администратор применяет список доступа к интерфейсу, он должен указать направление передачи пакетов. В этом случае маршрутизатор будет сравнивать соответственно входящие или покидающие интерфейс пакеты. Если направление не указано, по умолчанию подразумевается исходящий трафик (**out**). В случае необходимости фильтровать как входящий, так и исходящий трафик, следует создать и применить два отдельных списка доступа.

Пример 6.12. Разрешить прохождение пакетов через маршрутизатор от всех хостов сети класса С с адресом 140.12.11.0, кроме хостов 140.12.11.5 и 140.12.11.6, а также разрешить прохождение всего остального трафика через интерфейс, на котором установлен список доступа:

```
access-list   2  deny        host          140.12.11.5
access-list   2  deny        host          140.12.11.6
access-list   2  permit      140.12.11.0     0.0.0.255
access-list   2   permit any  any
```

Отсутствие последнего оператора привело бы к тому, что через интерфейс пропускались бы только пакеты из сети 140.12.11.0 (кроме хостов 140.12.11.5 и 140.12.11.6), а остальной трафик блокировался неявным оператором **deny any**, который присутствует в каждом списке по умолчанию.

Рассмотрим несколько примеров задания расширенного списка доступа.

Пример 6.13. Отказать протоколу FTP в доступе к интерфейсу E0.

```
access-list 101 deny tcp 172.16.4.0 0.0.0.255 eq 20
 172.16.3.0 0.0.0.255 eq 21
access-list 101 permit ip 172.16.4.0 0.0.0.255 0.0.0.0
 255.255.255.255
!-- неявно отказывает в доступе всем остальным;
!-- в тексте это не отображается
!-- access-list 101 deny ip 0.0.0.0 255.255.255.255 0.0.0.0
255.255.255.255
!
interface E0
access-group 101
```

Параметры команды имеют следующие значения:

- номер списка управления доступом **101** указывает, что это расширенный список;
- **deny** — поток данных, удовлетворяющий условию, будет блокирован;
- **tcp** — протокол транспортного уровня;
- **172.16.4.0** и **0.0.0.255** — адрес и маска источника, первые три октета должны отвечать условию (предписанию), последний не имеет значения;
- **172.16.3.0** и **0.0.0.255** — адрес и маска получателя, первые три октета должны отвечать условию, последний не имеет значения;
- **eq 21** — указывает на известный номер порта для протокола FTP;
- **eq 20** — указывает на известный номер порта для данных протокола FTP;
- команда **interface E0 access-group 101** связывает 101-й список управления доступом с выходным интерфейсом **E0**.

Отметим, что этот список не блокирует (не запрещает) поток данных FTP, а блокируются только порты 20 и 21. На серверах FTP легко может быть установлена конфигурация для работы на различных портах.

Пример 6.14. Блокировать (запретить) доступ TCP пакетов к серверу с IP-адресом источника 140.12.11.10

```
access-list 102 deny TCP 0.0.0.0 255.255.255.255 140.12.11.10 0.0.0.0
```

или сокращенная запись:

```
access-list 102 deny TCP any host 140.12.11.10
```

Следующий пример иллюстрирует использование логических операций:

```
access-list 103 permit TCP any host 140.12.11.10 eq www
access-list 103 permit ICMP any host 140.12.11.10 eq 8
```

Первая команда разрешает передачу пакетов TCP с любого узла на компьютер с адресом 140.12.11.10, если эти пакеты принадлежат типу Web.

Вместо мнемонического кода WWW можно задать число 80, так как трафик Web использует порт 80.

Вторая команда разрешает все адресованные указанному узлу сообщения ping — эхо запросы ICMP, которым назначен тип ICMP, равный 8. Синтаксис расширенных списков доступа позволяет задавать в конце оператора специфические для каждого протокола параметры; в частности, для протокола ICMP задаются не номера портов, как для протоколов UDP или TCP, а тип и если нужно — код сообщений ICMP. С учетом неявного оператора `deny any` в конце списка доступа весь остальной без исключения трафик будет блокироваться.

Для применения списка доступа после его создания необходимо связать его с каким-либо интерфейсом маршрутизатора, так как он начинает действовать только после связи его с интерфейсом. Применение списка доступа реализуется командой `ip access-group`. Общий формат этой команды имеет следующий вид:

ip access-group access-list-number [in|out]

Параметр `access-list-number` указывает номер списка доступа, который команда `access-group` ставит в соответствие конфигурируемому интерфейсу. Параметры `in` или `out` указывают, в каком направлении будут фильтроваться пакеты, т. е. определяют, к какому трафику — входящему или исходящему — применяется фильтр.

К каждому интерфейсу можно применить только один список доступа, который может быть либо **in** (*inbound*) — проверяется, когда пакет поступает на вход интерфейса снаружи, либо **out** (*outbound*) — проверка происходит, когда пакет приходит изнутри маршрутизатора на выходной интерфейс. Для этого необходимо войти в конфигурацию нужного нам интерфейса и прописать список доступа (в данном случае как **group** — "группа"). Последовательность команд конфигурации применения ACL для входящего IP-трафика интерфейса Ethernet 0/0 имеет следующий вид:

```
Router# configure terminal
Router(config)# interface ethernet 0/0
Router(config-if)# ip access-group 1 in
```

Для определения **временных списков доступа** в маршрутизаторах Cisco используется команда `time-based access list`. Она не создает новый тип списка доступа, а делает существующий список зависящим от времени, расширяя его функциональность. Временные списки могут быть нумерованными или именованными.

Процедура составление временного списка доступа состоит из двух этапов. На первом этапе задается диапазон времени, а на втором - ссылку на него в соответствующем списке доступа с использованием ключевого слова time-range. При задании диапазона времени сначала ему назначается имя, а

после этого определяется диапазон времени с помощью одного или нескольких интервалов времени.

Интервалы времени бывают двух типов — абсолютный (*absolute*) или периодический (*periodic*). В последнем случае диапазон времени может состоять более чем из одного временного интервала. Соответствующие команды показаны в следующем примере.

```
time-range time-range-name
absolute [[start] time date][end time date]
periodic days-of-the-week hh:mm to [days-of-the-week]hh:mm
```

Здесь в квадратных скобках приведены необязательные параметры.Для удобства администрирования сети присвоенное имя должно говорить о функциональном назначении временного диапазона или связываемого с ним списка доступа.

Время в командах следует вводить в 24-часовом формате, причем, сначала идет час, затем минуты (hh:mm). Дата вводится в формате: день, месяц, год. В случае периодических временных списов доступа в качестве параметров используются дни недели. Допустимыми аргументами являются какой-либо один день недели, например Monday (понедельник), или сразу несколько дней — Saturday and Sunday (суббота и воскресенье). Можно использовать параметры, указывающие сразу на несколько дней — daily, weekdays или weekend (все дни недели, рабочие или выходные дни).

Следует учитывать, что время в списках доступа всегда измеряется с помощью внутренних часов маршрутизатора. Поэтому чтобы списки доступа работали правильно, часы маршрутизатора должны быть настоены точно по местному времени.

Кроме того, использование абсолютных и периодических параметров временного интервала должно подчиняться определенным правилам. Так время и дата начала временного интервала должны предшествовать времени и дате его завершения. Если же используется одновременно абсолютный и периодический временной интервалы, то следует учитывать, что периодический интервал начнет действовать только после начала абсолютного — так же как и перестанет действовать после его окончания. Если начальное время абсолютного временного периода не указано, то он начнет действовать немедленно после определения. Если же конечное время не зафиксировано, то такой временной интервал будет длиться бесконечно.

Пример 6.15. В компьютерной сети организации имеется две подсети FastEthertnet с адресами 192.168.2.0 и 192.168.3.0, подключенные к глобальной сети через маршрутизатор как показано на рисунке 6.3. Согласно политике безопасности организации требуется запретить доступ к Internet в зависимости от времени суток сотрудникам, находящимся в сети 192.168.2.0 в рабочее время (с 8.00 до 17.00) и разрешить выход в Internet в рабочие дни во

время обеденного перерыва (с 12.00 до 13.00). Такой режим доступа должен включиться с 1 октября 2014 г., а срок действия не определен.

Для пользователей подсети LAN2 разрешен только доступ к серверу с адресом 192.168.2.100, находящемуся в подсети LAN1 лишь по рабочим дням с 8:00 до 17:00. Такая политика должна вступить в действие немедленно и закончиться к концу календарного года.

Требуется составить сценарий конфигурации маршрутизатора для реализации политики безопасности организации.

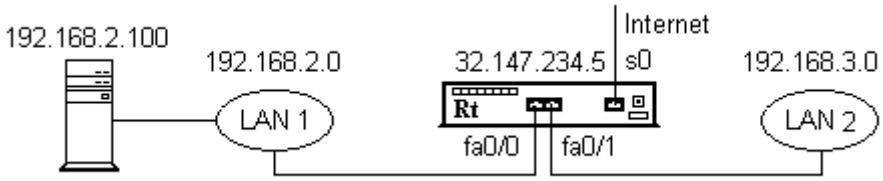


Рисунок 6.3 Схема подсетей FastEthertnet с доступом в Internet

В связи с тем, что сеть LAN1 подсоединена к маршрутизатору через FastEthernet-порт fa0/0 и трафик для маршрутизатора является входящим (in), назначим список доступа интерфейсу fa0/0. Так как в списке доступа должен быть указан Internet-протокол (http), то список доступа — расширенный (номер должен находиться в диапазоне 100 … 199).

```
interface fa0/0
ip access-group 101 in
                !- применение списка с номером 101 этому интерфейсу
time-range allow-http
      !- указание имени временного диапазона
absolute start 12:00 1 Oktobre 2014
periodic weekdays 12:00 to 13:00
      !- задание параметров временного диапазона
      !- время окончания не задано, список будет действовать
      !- пока не будет удален
access-list 101 permit tcp any any eq 80
time-range allow-http
      !- задание списка доступа с указанием символического параметра
      !- установленного ранее временного диапазона
interface fa0/1
ip access-group 102 in
time-range server
absolute end 24:00 31 December 2014
periodic weekdays 08:00 to 17:00
access-list 102 permit any host 192.168.1.100
time-range server!-
```

Часть 2
Методические рекомендации по проектированию компьютерных сетей

7. Техническое задание на проектирование сети

7.1. Цели работы и порядок её выполнения

Цели работы подразделяются на две составляющие: цель преподавателя — руководителя курсового проектирования и цель разработчика проекта — студента. Целью руководителя является углубление студентами знаний теоретических основ построения локальных и корпоративных компьютерных сетей и привитие студентам практических навыков создания компьютерных сетей предприятий (организаций) различного масштаба. Цель курсового проекта студента — разработка структуры локальной компьютерной сети предприятия (организации) с возможностью выхода пользователей в сеть Интернет, выбор оборудования и составление сценариев конфигурирования телекоммуникационного оборудования, обеспечивающего надежное функционирование сети в соответствии с техническим заданием.

Компьютерная сеть предназначена для обеспечения возможности информационного взаимодействия между автоматизированными рабочими местами, серверами, средствами сетевой печати в здании центрального офиса и с филиалами предприятия.

Общая схема расположения организации определяется номером варианта задания и приведена в приложении А1. Порядок и сроки выполнения проекта регламентируются календарным планом работ.

Общая продолжительность выполнения проекта определяется календарным планом, составляемым руководителем проекта. Завершается процедура проектирования публичной защитой проекта.

В зависимости от программы дисциплины, в рамках которой выполняется курсовой проект, направления обучения и специализации студентов, количества часов, выделенных на изучаемую дисциплину, руководитель проекта может исключать или дополнять отдельные пункты технического задания, изменять входные параметры и их количество, изменять количество и объем разделов пояснительной записки, вид и количество обязательного графического материала, объем сценариев конфигурации оборудования, среду моделирования сети и т.д.

7.2. Общие требования к проектируемой сети

На этапе проектирования компьютерных сетей организаций (предприятий) к ним предъявляется как общие требования, характерные для всех видов сетей, так и частные, определяемые спецификой компьютеризируемого предприятия и требованиями технического задания. К общим требованиям относятся:

- реализация телекоммуникационного центра, размещенного в здании, на основе высокопроизводительного и перспективного оборудования;
- выбор магистральных линии и линий уровня рабочих групп необходимой пропускной способности для устойчивой работы сети при пиковых нагрузках;
- закладка высокоскоростного канала передачи данных необходимой пропускной способности для работы головного подразделения организации с ее отделениями и филиалами;
- обеспечение безопасной работы сотрудников предприятия с сетью Интернет;
- реализация возможности простой реконфигурации активного оборудования на логическом и физическом уровнях;
- предусмотрение возможности управления сетью унифицированным образом через Web-интерфейс с учетом повышенной сложности сети;
- обеспечение возможности сбора статистики о сети (мониторинг сети) наиболее экономичным и надежным способом.

7.3. Характеристика производственного объекта, исходные данные и требования к сети предприятия

1. Сеть предназначена для обслуживания рабочих групп персонала организации, которые должны быть между собою логически разделены.

2. Каждый из пользователей рабочей группы должен иметь потенциальную возможность доступа к глобальной сети Интернет. Реальная возможность доступа к Интернет определяется списком доступа.

3. Тип разрабатываемой политики безопасности определяется техническим заданием на основании номера варианта (Приложение А1).

4. В сети устанавливается несколько серверов (приложение А1), которые должны размещаться в отдельном помещении с ограниченным доступом.

5. Предприятие располагается в *L*-этажном здании (см. чертежи этажей Приложение А4), с размерами в плане *M* х *N* (15 х 48,7) м. Высота этажа составляет *H* (3.5) м, общая толщина перекрытий равна *D* (30) см, толщина капитальных (несущих) стен принимается равной 40 см. На всех этажах здания рабочие помещения имеют разные размеры. Во всех помещениях здания (кроме помещений цокольного этажа) имеется подвесной потолок с высотой

свободного пространства P (35) см. Внутренние (не несущие) стены помещений изготовлены из обычного кирпича и покрыты штукатуркой. Общая толщина таких внутренних стен равна 20 см. Строительным проектом предусмотрен вертикальный технологический канал для прокладки кабелей, проходящий через все этажи. На каждом этаже имеются свободные служебные помещения, в которых может быть расположено коммуникационное оборудование сети общего использования (см. планы этажей здания).

6. Количество потенциальных пользователей сети предприятия $N_{\text{п}}$ определяется площадью помещений, занимаемых этим предприятием. Количество серверов предприятия $N_{\text{сп}}$ (2-4) и серверов рабочих групп $N_{\text{срг}}$ (4-6) задается техническим заданием.

7. Средняя и пиковая нагрузка, создаваемая пользователем сети $V_{\text{п}}$ (Мбайт/с) может быть дополнительно указана рукодителем проекта.

8. Число структурных подразделений предприятия $N_{\text{спп}}$ определяется количеством его сотрудников и областью деятельности. Эти сведения выясняются разработчиком сети в процессе знакомства с предприятием и собеседованием с его руководством. В случае отсутствия таких данных предполагается, что количество структурных подразделений (рабочих групп) определяется общей площадью помещения и их количеством. В данном проекте предполагается, что в комнате площадью до 40 м^2 располагаются сотрудники одной рабочей группы, а в помещении площадью свыше 40 м^2 — две рабочие группы.

9. Используемые сетевые сервисы на предприятии могут быть указаны в техническом задании (WWW; FTP: E-Mail; Data Base; передача мультимедийных данных и др.).

10.Применяемый протокол маршрутизации в проектируемой сети определяется выбирается разработчиком или может быть задан вариантом технического задания (RIP, IGRP, EGRP, OSPF).

11.Для связи с филиалами предприятия используется выделенная медная или волоконно-оптическая линия или каналы глобальной коммуникационной сети, тип которой указан в таблице вариантов (Frame Relay, ATM, FastEthernet или GEthernet).

12.Кабельная инфраструктура сети должна соответствовать требуемой пропускной способности с учетом перспектив развития сети и коммуникационного оборудования.

13.Структурированная кабельная система локальной компьютерной сети должна по возможности максимально использовать декоративные пластиковые короба с учетом допустимого количества кабелей и норм укладки.

14.Необходимость резервирование серверного оборудования и маршрутизаторов указывается в техническом задании на проектирование.

15.В процессе проектирования следует предусмотреть возможность расширения сети при увеличении численности сотрудников предприятия.

16.Варианты выделенных предприятию IP-адресов приведены в приложении А3.

17.Варианты списков доступа задаются преподавателем.

18.Тип и производитель коммуникационного оборудования выбирается в соответствии с техническим заданием (Cisco, D-Link, 3Com и пр.), либо по критерию минимальной стоимости сети.

7.4. Содержание работ, выполняемых в процессе проектирования

В процессе проектирования разработчик должен выполнить:

1. Определить количество и месторасположение серверных и кроссовых пунктов, а также телекоммуникационных розеток на планах помещений организации (предприятия).
2. Разработать логическую структуру корпоративной сети, в которой компьютеры сотрудников каждого из функциональных подразделений предприятия (рабочих групп), не зависимо от их места расположения в здании, должны быть включены в одну и ту же виртуальную сеть. При этом должна быть обеспечена возможность взаимодействия пользователей и/или серверов локальной сети с глобальными сетями.
3. Определить количество и типы коммуникационного оборудования, необходимого для построения компьютерной сети предприятия с учетом нагрузки, создаваемой пользователями сети.
4. Составить топологию всей сети и произвести конфигурацию используемого оборудования, которая обеспечивает заданное качество обслуживания и безопасность работы.
5. Выполнить моделирование сети в пакете Packet Tracer, Boson, или др. на предмет ее корректного функционирования и, при необходимости, осуществить коррекцию схемы и конфигурации оборудования.
6. Составить схему прокладки и подключения соединительных кабелей.
7. Выбрать типы кабелей и необходимых соединителей, рассчитать длины кабельных сегментов.
8. Выбрать тип и рассчитать размер кабельных коробов, используемых для прокладки кабелей.
9. Выбрать тип и размер коммуникационных шкафов и другого пассивного телекоммуникационного оборудования.
10. Разработать политику безопасности в сети при: а) взаимодействии пользователей с Интернетом; б) управлении доступом к ресурсам сети и других условиях работы (согласно номера варианта ТЗ, приложение А1).
11. Предусмотреть наличие демилитаризованной зоны и установку межсетевых защитных экранов и обеспечить фильтрацию пакетов в соответствии с номером варианта технического задания.

7.5. Перечень документов, входящих в состав проекта

В состав проекта входят следующие документы:

1) техническое задание на разработку с календарным планом выполнения проектных работ;
2) пояснительная записка с описанием технических и программных решений.
3) схемы чертежей:
   - 3.1) логическая структура сети;
   - 3.2) электрическая (физическая) схема или таблица подключения оборудования и кабельной системы.

7.6. Содержание пояснительной записки

Пояснительная записка содержит текстовое изложение особенностей проектируемой сети, администрирования и электропитания. Типовая пояснительная записка должна включать перечисленные ниже разделы. Этот перечень может быть расширен путем введения дополнительных разделов.

1. Введение.
2. Постановка задачи.
3. Определение количества и месторасположения кроссовых, серверных помещений и телекоммуникационных розеток сети.
4. Разработка логической структуры сети. Создание виртуальных сетей.
5. Назначение сетевых адресов коммуникационному оборудованию и подсетям.
6. Обоснование выбора и расчет кабельной системы и сетевого оборудования.
7. Список доступа и закрепления за интерфейсами подсетей отдельных служб.
8. Таблица настройки параметров маршрутизатора. Режимы работы коммутаторов.
9. Программы (сценарии) конфигурации телекоммуникационного оборудования.
10. Разработка физической структуры сети.
11. Политика безопасности в сети.
12. Компьютерное моделирование функционирования сети.
13. Заключение.

    Библиографические ссылки.

8. Выполнение разделов проекта и составление пояснительной записки

Ниже указаны названия разделов пояснительной записки и примерное их содержание. Во многих разделах приведены примеры описаний и расчетов, относящиеся к этим частям проекта. Примеры в тексте выделены шрифтом.

8.1. Введение

Во введении пояснительной записки коротко освещается актуальность использования сетевых технологий на предприятиях и в организациях, формулируется цель работы и задачи, которые предстоит выполнить при достижении поставленной цели, приводится структура пояснительной записки с указанием содержания каждого раздела.

8.2. Постановка задачи

В этом разделе следует подробно описать структуру организации, для которой проектируется компьютерная сеть: количество рабочих комнат и рабочих мест в них, расположение помещений в здании (количество этажей, комнат на этажах), наличие и месторасположение технических помещений, которые могут быть использованы для размещения коммуникационного оборудования; перечислить основные приложения, с которыми работают сотрудники, используемые операционные системы, необходимые сервисы Интернет, наличие собственных адресов Интернет, требования по доступу к информационным ресурсам предприятия.

В качестве исходного материала к этому разделу используются данные технического задания. При этом допускается введение проектировщиком по согласованию с руководителем дополнительных условий (изменение числа рабочих групп, расширение или изменение списка доступа пользователей к информационным ресурсам, количество и тип серверов, а также место их расположения, дополнительные условия фильтрации пакетов и т.п.).

Затем в постановке задачи подробное излагается, что конкретно необходимо спроектировать (с учетом варианта технического задания и введенных дополнительных требований, сформулированных в результате изучения особенностей предприятия). В качестве примера ниже приведен фрагмент описания ситуации на предприятии.

Пример 8.1.

«Группа сотрудников предприятия работает на одном (или двух, планируется расширение) этажах здания. Основная работа у всех сотрудников — тексты в

MS Word и таблицы в MS Excel (составление отчетов о проделанной работе), довольно частое общение с клиентами посредством электронной почты. Небольшая группа сотрудников работает с 1С бухгалтерией, еще одной небольшой группе сотрудников нужна правовая система "Консультант-плюс", одна (основная и достаточно большая) группа сотрудников использует две узкоспециализированные расчетные подсистемы. Небольшая группа сотрудников занимается скачиванием и рассылкой аудио- и видеофайлов в реальном времени.

Все сотрудники, в большей или меньшей степени используют Интернет. Т.е. всем им необходимо размещать, искать, просматривать и скачивать в Интернете какую-то информацию. Для этого на одном из компьютеров установлен ADSL-модем и работа с Интернет возможна только с одного компьютера. Интернетом пользуются не очень активно. Основная работа происходит в локальной сети.

На предприятии имеется:

- 46 сотрудников, но планируется расширение приблизительно до 100 сотрудников;
- 12 помещений, но предполагается занять еще один этаж и дополнительно 30 помещений;
- доступ в Интернет выполняется только с одной рабочей станции и т. п.»

8.3. Определение количества и месторасположения кроссовых, серверных помещений и телекоммуникационных розеток сети

В этом разделе необходимо спланировать расположение кроссовых и серверных помещений, рассчитать количество рабочих групп и требуемое количество телекоммуникационных розеток проектируемой сети. Исходным материалом для выполнения этой работы является план размещения предприятия в здании (зданиях), количество и площадь занимаемых помещений. Пример такого плана приведен на рисунке 8.1. При расчете количества рабочих групп в данном проекте предполагается, что в комнате площадью до 40 м^2 располагаются сотрудники одной рабочей группы, а в помещении площадью свыше 40 м^2 — две.

Если организация располагается в нескольких зданиях, то число рабочих групп принимается равным их количеству в здании центрального офиса.

Для того чтобы определить, сколько кроссовых должно быть в здании и где они должны располагаться, следует помнить, что максимальная длина горизонтального кабеля типа "витая пара" в локальной вычислительной сети не может превышать 90 метров.

Международный стандарт EIA/TIA-569A [41] требует, чтобы для расположения серверов и коммутационного оборудования выделялось минимум одно специальное служебное помещение на этаж. Кроме того, он устанавливает необходимость наличия дополнительного помещения (распределительного пункта) для коммутационного оборудования на каждые 1000 квадратных метров, если обслуживаемая площадь этажа превышает 1000 квадратных

метров или если протяженность горизонтальной кабельной системы больше 90 метров.

Если организация занимает не один этаж, а также если она располагается в нескольких зданиях, то выделяется специальное помещение для распределительного пункта здания, а этажные и распределительные пункты других зданий исполняют роль промежуточных распределительных пунктов. Распределительные пункт здания (РПЗ) и пункты этажей (РПЭ) соединяются между собой магистральной кабельной системой. При расположении организации в нескольких зданиях, в одном из них оборудуется распределительный пункт комплекса (РПК), который назначается главным коммутационным узлом сети предприятия.

Сети небольших зданий рекомендуется проектировать по принципу централизованной архитектуры. При этом если диаметр сети не превышает 200 метров, достаточно одного пункта коммутации, а все активное оборудование целесообразно размещать в одном месте. Важным преимуществом централизованной архитектуры является то, что она позволяет установить систему кондиционирования сетевого оборудования в единственном помещении. Это снижает расходы на эксплуатацию системы.

Такую же простейшую топологию целесообразно выбрать и в случае объединения в сеть ресурсов компании, арендующей всего несколько комнат. Если пользователи находятся в удаленных помещениях или на разных этажах, то следует организовать два и более пунктов коммутации. В этом случае часть портов или панелей будет задействована для подключения магистралей, соединяющих распределительные пункты.

В случае, когда требуется просто объединить рабочие места в составе одной структурной единицы предприятия (отдела, службы и т.п.), используется простая рабочая группа компьютеров. Но если рабочей группе требуется повышенная информационная безопасность или нужно дисковое пространство, выделение которого на головном сервере предприятия представляется нецелесообразным, то в этом случае для рабочей группы следует устанавливать отдельный сервер, который выполняет также функции сервера приложений. Рабочая группа с собственным сервером является обособленной в составе сети предприятия и, как правило, выделяется в отдельный домен (виртуальную сеть). Взаимоотношения с основным доменом устанавливаются исходя из целей и задач, решаемых рабочей группой.

В магистральной подсистеме целесообразно планировать не более двух уровней коммутации. Это позволит ограничить искажение сигналов в пассивном оборудовании и упростить администрирование. На пути от РП этажа до РП комплекса должен быть один распределительный пункт. Распределительные пункты магистральной кабельной системы могут располагаться в телекоммуникационных помещениях или аппаратных.

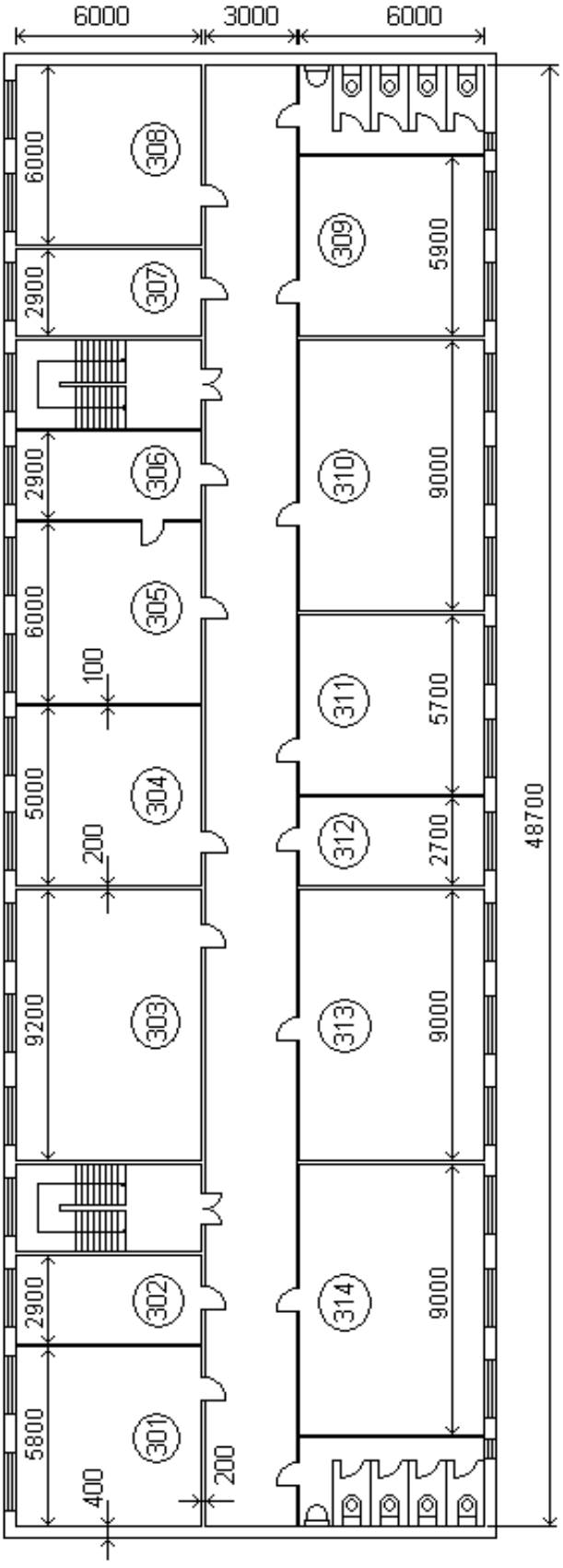


Рис. 8.1. План помещений, занимаемых организацией

Используемые организацией серверы следует разделить на две отдельных группы: **сервер(ы) предприятия** (*Enterprise servers*) **и серверы рабочих групп** (*Workgroup servers*), а затем разместить их в сети согласно ожидаемому характеру потока данных пользователей и исполняемым функциям. Сервер предприятия поддерживает всех пользователей сети, предоставляя им различные службы, такие как электронная почта, служба доменных имен (DNS) и т.д. Сервер рабочей группы обслуживает определенную группу пользователей и предоставляет им такие службы, как обработка текстов или совместный доступ к файлам, то есть функции, которые могут понадобиться только некоторым группам пользователей.

Серверы предприятия целесообразно размещать на распределительном пункте комплекса — **главной распределительной станции.** В этом случае поток данных на серверы предприятия будет идти только к РПК, не проходя через остальные сети.

В идеальном случае серверы рабочих групп следует располагать на **промежуточных распределительных станциях —** РПЭ, по возможности ближе к пользователям, использующим приложения этих серверов. Если серверы рабочих групп установить поближе к пользователям, то поток данных будет проходить по инфраструктуре сети прямо к РПЭ, не затрагивая других пользователей в этом сегменте [2].

При планировании расположения серверного оборудования следует учесть, что одним из случаев удобного и достаточно простого распределения серверов являются **серверы отделов**. Данные устройства могут быть непосредственно подключены к блоку распределения сети, которую они обслуживают. Как правило, такие серверы подключаются непосредственно к этажному коммутатору, обслуживающему данный отдел, либо подсоединяются к коммутаторам распределительного пункта здания. В таком случае также предоставляется возможность создания небольшой серверной группы (серверной фермы) в РПЗ каждого здания. Файловые серверы и серверы печати отделов могут подключаться там, где в централизованной серверной группе могут быть расположены серверы предприятия и высокопроизводительные устройства хранения и обработки данных.

В последнее время широко применяются централизованные **серверные группы** (фермы). *Группа серверов* обычно располагаются в аппаратном помещении с контролируемыми условиями эксплуатации, т. е. это помещение имеет специальное оборудование для фильтрации и стабилизации колебаний силового напряжения и поддержания температуры в заданном диапазоне. Создание группы серверов позволяет сэкономить средства, поскольку некоторое оборудование (например, фильтры питания, источники бесперебойного питания и пр.) могут обслуживать целое помещение, и их не нужно покупать отдельно для каждого хоста и сервера. Кроме того, расположение серверной фермы в одной комнате облегчает защиту от несанкционированного доступа. Однако следует учитывать, что такие серверные группы могут

создавать повышенную нагрузку на совместно используемую среду передачи данных, поскольку скорость обработки информации в них может быть чрезвычайно высокой. Поэтому каналы, связывающие серверы и сетевое оборудование, должны быть высокоскоростными, и их следует изолировать от тех сегментов, в которых располагаются рабочие станции. Наличие скоростных каналов обеспечит полосу пропускания, достаточную для всех пользователей, обращающихся к серверам. Изолируя серверы от других сегментов, можно также обеспечить избыточность сети тем самым повысить ее надежность.

Следует принять во внимание, что в некоторых случаях в крупных организациях окажется предпочтительнее размещать серверы так, чтобы они отражали структуру отделов или подразделений. При таком подходе серверами управляют администраторы, имеющиеся в каждом подразделении, благодаря чему эксплуатация ресурсов может учитывать специфику конкретного подразделения. Однако и в таком случае серверы желательно размещать в отдельных помещениях, в частности, в распределительных пунктах этажей.

Программные продукты общего пользования и базы данных целесообразно размещать на головном сервере предприятия. Такое решение позволяет упорядочить логическую структуру сети и упростить ее администрирование и поиск данных, уменьшить стоимость.

Управление типовой локальной вычислительной сетью среднего и крупного предприятия осуществляется, как минимум, группой нескольких серверов, включающей:

- **головной сервер** (*Main*), отвечающий за распределение ресурсов, хранение информации и политику безопасности, с подключенным к нему дисковым массивом;
- **резервный сервер** (*Backup*), который исполняет роль вторичного контроллера домена и отвечающий за резервное копирование информации;
- **Web-сервер**, на котором размещается Web-сайт предприятия;
- **Почтовый сервер** (*Mai*l) и служба электронной почты.

Кроме того, в группу серверов входит рабочее место администратора сети. К служебным компьютерам относятся сервер доступа, обеспечивающий защиту локальной сети от несанкционированного доступа извне.

Количество пользователей сети предприятия определяется техническим заданием на разработку, которое определяется желанием и возможностями заказчика. С учетом возможного роста сети целесообразно увеличить количество телекоммуникационных розеток не менее чем на 10%, относительно заданного числа пользователей. При отсутствии в техническом задании количества рабочих мест пользователей общее число рабочих мест, определяется из расчета 5 $м^2$ на одно место.

Среднее рабочее место рассчитывается следующим образом: 1 розетка телекоммуникационная, 1 розетка телефонная, 3 розетки электрические. На

каждое помещение дополнительно предусматривается 4 электрические розетки (2 для бытовых нужд, 1 на кондиционер и 1 на факс) и одна телефонная для подключения факсимильного аппарата.

Распределение рабочих мест по этажам целесообразно представить в форме таблицы (например, таблица 8.1).

Таблица 8.1

Распределение рабочих мест по этажам

Этаж	Наличное количество рабочих мест	Резерв на развитие	Общее количество телекомуникационных розеток
1	30	3	33
2	28	3	31
3	47	5	52
Всего	105	11	116

Затем следует распределить телекоммуникационные розетки (разъемы) по помещениям и определить среднюю длины кабеля от розетки до кроссового оборудования.

Следует иметь в виду, что высокая плотность установки телекоммуникационных разъемов повышает гибкость сети и облегчает изменения телекоммуникационных ресурсов рабочих мест. Допускается установка розеток одиночно или группами, однако каждое рабочее место должно иметь не менее двух разъемов. На каждом рабочем месте необходимо предусмотреть, по крайней мере, один разъем, терминированный симметричным кабелем с волновым сопротивлением 100 или 120 Ом (предпочтение отдается кабелям 100 Ом). Другие разъемы можно устанавливать на симметричном либо на оптоволоконном кабеле. Симметричный кабель должен иметь две или четыре пары проводников, причем все пары должны быть подсоединены к контактам телекоммуникационной розетки.

В пояснительной записке следует обосновано и подробно описать план размещения оборудования. Пример фрагмента такого описания приведен ниже.

Пример 9.2.

"Организация, занимающаяся предоставлением услуг предприятиям и населению располагается в многоэтажном здании и занимает весь этаж (чертеж СевГУ ХХХ). На данном этаже имеется 10 помещений, размеры которых указаны на чертеже. Общая протяженность коридора, согласно чертежу, равна 48 м. В центре здания имеется помещение №7 площадью 13 кв.м., которое может быть использовано для технических нужд сети в качестве аппаратной.

Выполним расчет площадей помещений, на основании которого определим количество телекоммуникационных розеток (ТР), подлежащих установке в каждой из комнат, а также число рабочих групп организации. Число компьютеров в рабо-

чей группе не должно превышать 14-ти (из расчета 4 двоичных разряда на нумерацию компьютеров в группе). Расчетные данные сведем в таблицу 8.2.

Таблица 8.2

Количество ТР и номера рабочих групп

№ комнаты	**Площадь помещения, м^2**	**Количество ТР**	**Номера рабочих групп**	**Примечания**
1	15,7	3	2	Зам. директора Гл. бухгалтер
2	46,8	9	3	
3	15,2	3	1	Администратор сети Программисты
4	38	8	4	
5	34	7	5	
6	56	11	6	
7	13	2	1	Аппаратная
8а	6	1	2	Секретарь
8б	9	2	2	Директор
9	32,5	6	5	
10	48,6	10	7	
Итого общее количество:		62	7 групп	

В результате анализа плана этажа и расчетных данных предлагается для размещения администратора сети и технического персонала выделить комнату №3, а помещение №7 использовать в качестве аппаратной, в которой будет установлено активное телекоммуникационное оборудование. В связи с тем, что организация занимает только один этаж, в аппаратной целесообразно установить оборудование горизонтальной и вертикальной подсистем СКС, а также серверное оборудование рабочих групп и организации.

Для защиты распределительных панелей и активного коммуникационного оборудования от влаги и электромагнитного излучения, проникновения пыли и грязи, а также для ограничения несанкционированного доступа к этим устройствам, в комнате №7 должен быть установлен один 19-дюймовый телекоммуникационный шкаф напольного исполнения.

В телекоммуникационном шкафу монтируются коммутационные панели (патч-панели) для разделки горизонтальных кабелей, а также могут быть установлены оптические распределительные полки для подключения оптоволоконных кабелей подсистемы вертикальных магистралей. Кроме этого в телекоммуникационный шкаф помещаются центральный и этажные коммутаторы, маршрутизатор(ы), серверы приложений, а также источник бесперебойного питания.

В этом же помещении монтируется распределительный щит силового питания компьютеров и другого офисного оборудования, находящегося в помещениях. Схема расположения телекоммуникационного шкафа и щита электропитания показана на чертеже размещения компонентов сети (чертеж СевГУ 09.03.02.03КП).

Телекоммуникационные розетки закрепляются в кабельных коробах на высоте 80 см от уровня пола. Расположение телекоммуникационных и электрических розеток в каждом из помещений с указанием установочных размеров показано на чертеже 1. Для определения минимальной L_{min} и максимальной L_{max} длины кабелей горизонтальной подсистемы построим профили кабельных трасс для планов помещений. Примеры профилей кабельных трасс изображены на рисунках 9.2а) и б) для минимальной и максимальной длин соответственно.

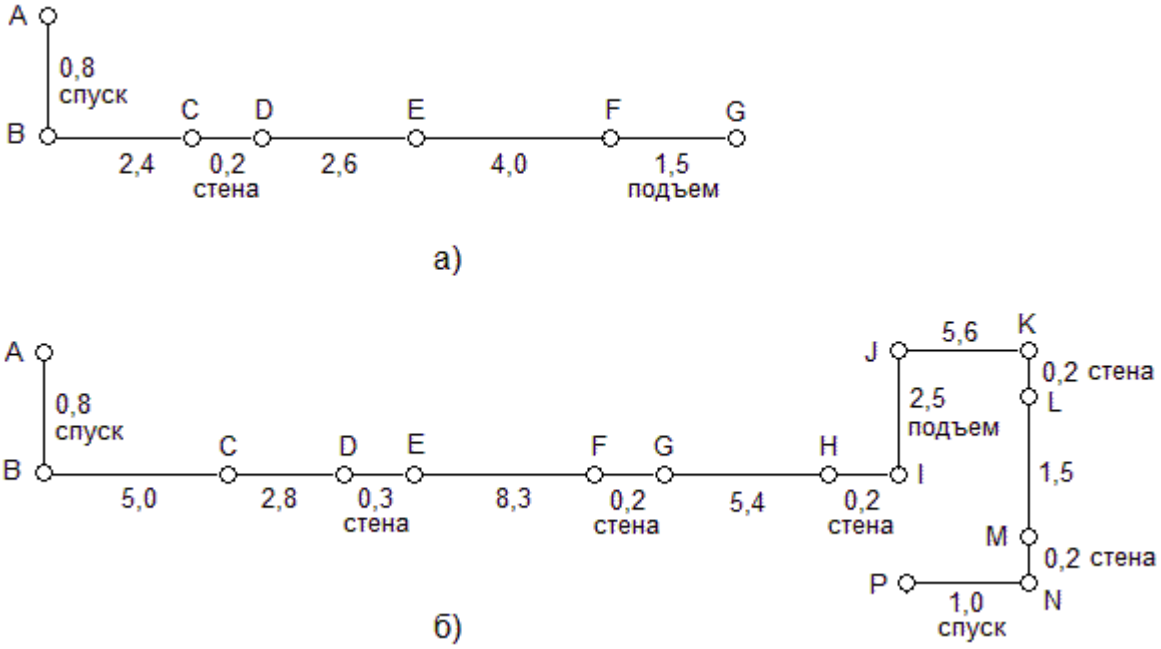


Рисунок 8.2 - Примеры построения профилей кабельных трасс

Из рисунков 8.2 находим L_{min} =11,5 м и L_{max} = 35 м. Эти данные впоследствии используются для расчета потребности в кабельной продукции».

8.4. Разработка логической структуры сети и создание виртуальных сетей

8.4.1. Выбор и обоснование структуры сети

В данном разделе приводятся возможные варианты структур локальной сети предприятия, часть из которых рассмотрены в подразделе 2, анализируются их достоинства и недостатки и обосновывается логическая структура проектируемой компьютерной сети. Здесь же должен быть представлен чертеж логической структуры и его подробное описание (состав и функционирование). Фрагмент примера этого подраздела приведен ниже.

Пример 8.3. «Составим схему сети предприятия для рассмотренного выше примера. В состав сети входит 62 рабочие станции, объединенные в 7 рабочих

групп. Согласно техническому заданию сеть должна обеспечить выход в Интернет для внутренних пользователей сети в определенное время. Из внешней сети должен быть предоставлен доступ только к почтовому, FTP- и Web-серверу.

В связи с предъявленными требованиями, все серверы, связанные с Интернет, выносим в отдельную подсеть — демилитаризованную зону (DMZ). В локальной сети будут находиться файловый сервер, сервер печати, сервер авторизации, DHCP-сервер и DNS-сервер локальной сети, а также все рабочие станции. Так как количество рабочих станций достаточно велико, то на уровне доступа необходимо использовать несколько коммутаторов. С целью обеспечения необходимой информационной безопасности сети и уменьшения взаимной загрузки сегментов, выделим компьютерам каждой из рабочих групп отдельную виртуальную сеть — VLAN. Для реализации возможности обмена информацией между пользователями функциональных подразделений предприятия коммутаторы уровня доступа должны соединяться через маршрутизатор или маршрутизирующий коммутатор (коммутатор третьего уровня).

Локальная сеть и демилитаризованная зона будут общаться между собой через маршрутизатор, который собственно и будет иметь выход в Интернет. На маршрутизаторе будет установлен соответствующий межсетевой защитный экран (файрвол) и сервер преобразования адресов NAT, что позволит организации работать с сетью Интернет через один реальный адрес.

С учетом изложенного, логическая схема проектируемой сети имеет вид, изображенный на рисунке 8.3.

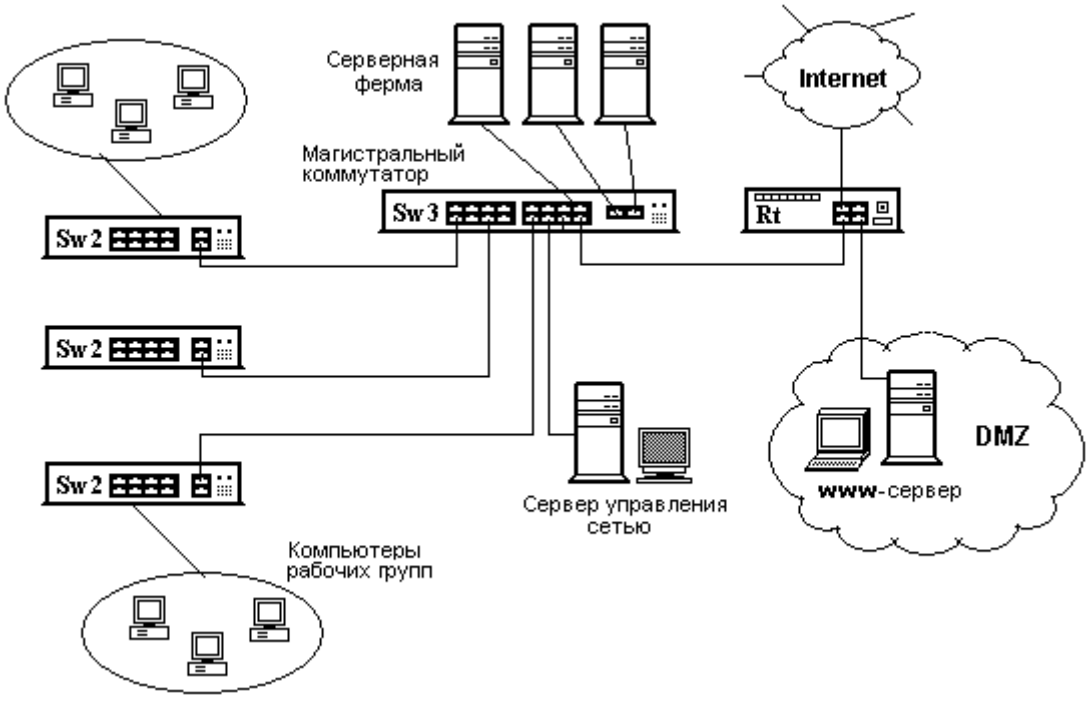


Рисунок 8.3. Пример реализации логической структуры сети предприятия

В качестве коммутаторов уровня доступа (SW 2) применяются три однотипных коммутатора, имеющие по 24 порта FastEthernet. На уровне распределения

установлен маршрутизирующий коммутатор третьего уровня (SW 3). Связь с сетью Интернет по выделенной телефонной линии обеспечивает ADSL-модем со встроенным маршрутизатором, который, кроме функций маршрутизации, выполняет роль защитного экрана и NAT-сервера.»

8.4.2. Деление сети предприятия на независимые виртуальные сети

Для достижения максимальной производительности сети и повышения защищенности отдельных рабочих групп всю сеть целесообразно разделить на независимые логические сегменты. Одним из эффективных способов такого разделения является создание виртуальных логических сетей (VLAN).

В данном подразделе пояснительной записки нужно показать, каким образом рабочие станции (клиентские компьютеры) объединяются в виртуальные сети. При этом следует помнить, что в виртуальную сеть могут быть включены клиентские компьютеры, не зависимо от их пространственного положения, т.е., в виртуальную сеть могут входить компьютеры, расположенные не только в одной комнате, но и в различных комнатах одного или разных этажей. На практике вопросы включения компьютеров в ту или иную изолированную виртуальную сеть решаются на основе рекомендаций администрации или службы безопасности предприятия.

В настоящем учебном проекте для упрощения, предполагается, что количество и состав виртуальных сетей определяются рабочими группами пользователей. Таким образом, для рассматриваемого примера сети количество VLAN задаем равным 7. Номера виртуальных сетей в данном случае совпадают с номерами рабочих групп (таблица 8.2). В VLAN1 включим рабочие станции администратора сети, станцию, расположенную в аппаратном (серверном) помещении и компьютеры системных программистов. Во вторую виртуальную сеть VLAN2 включим компьютеры администрации предприятия: директора и его секретаря, заместителя директора и главного бухгалтера. В остальные виртуальные сети войдут компьютеры сотрудников соответствующих рабочих групп.

8.5. Назначение сетевых адресов коммуникационному оборудованию и подсетям

В данном подразделе необходимо назначить сети внешний IP-адрес и сетевую маску, а также присвоить адреса и сетевые маски всем виртуальным сетям и рабочим станциям. Внешний IP-адрес и сетевая маска выделяется провайдером Интернет-услуг по запросу предприятия (указан в таблице вариантов, Приложение А3). Пусть согласно варианту предприятию выделен в постоянное пользование один бесклассовый адрес 83.221.169.36/30.

Известно, что для внутреннего использования в локальных сетях рекомендованы следующие частные адреса (таблица 8.3).

Таблица 8.3

Диапазоны частных адресов

Класс	Начальный адрес	Конечный адрес	Число сетей
A	10.0.0.1	10.255.255.255	1
B	172.16.0.0.	172.31.255.255	16
C	192.168.0.0.	192.168.255.255	255

Если предприятие располагается в нескольких многоэтажных зданиях, то для удобства администрирования в качестве адреса сети целесообразно выбрать адрес 10.B.G.C с сетевым префиксом длиной 24 бита. Десятеричное значение символа B отображает номер здания; G — рабочей группы, а C — номер компьютера в группе. Таким образом, в рабочую группу можно объединить до 254-х компьютеров. Диапазон адресов компьютеров организации (предприятия) для рассмотренного выше примера (7 рабочих групп) представлен в таблице 8.4.

Таблица 8.4

Диапазон сетевых адресов проектируемой сети

Начальный адрес	10.	1.	0.	1
	00001010	00000001	00000000	00000001
Конечный адрес	10.	1.	254.	254
	00001010	00000001	00000001	11111110

Адреса с нулевой группой целесообразно использовать для присвоения адресов портов маршрутизаторам и портам управления коммутаторов. Таким образом, адреса для коммуникационного оборудования, расположенного в первом здании, находятся в следующих диапазонах: 10.1.0.1 — 10.1.0.254.

Для портов маршрутизатора выделено два частных адреса. Адрес 10.1.0.1 присвоим порту, соединенному с локальной сетью организации, а адрес 10.1.0.2 — порту, подключенному к серверу демилитаризованной зоны. Интернет-адрес 83.221.169.36 сети предприятия выделен провайдером. В связи с тем, что в соответствии с ТЗ предприятию выделен только один внешний адрес, то для обеспечения выхода пользователей сети в Интернет необходимо применить процедуру трансляции адресов.

Далее необходимо привести таблицу с адресами всех компьютеров, расположенных в помещениях организации, для которой проектируется сеть. В этой таблице целесообразно указать номера коммутаторов / маршрутизаторов и номера портов, к которым подключаются клиентские компьютеры и серверы. Фрагмент таблицы адресов с номерами портов для рассматриваемого примера представлен в таблице 8.5.

Таблица 8.5

Распределение адресов

№№ комнат	Номер/название рабочей группы	Номер ТР (компьютера)	Адрес	Устройство / порт	Примечание
3	1/Инф.поддержки	31	10.1.1.1	Sw1-Fa0/2	Админ. сети
3	1	32	10.1.1.2	Sw1-Fa0/3	
3	1	33	10.1.1.3	Sw1-Fa0/4	
7	1	71	10.1.1.4	Sw1-Fa0/5	
7	1	72	10.1.1.5	Sw1-Fa0/6	
1	2/Дирекция	11	10.1.2.1	Sw1-Fa0/7	
1	2	12	10.1.2.2	Sw1-Fa0/8	
1	2	11	10.1.2.3	Sw1-Fa0/9	
8а	2	81	10.1.2.4	Sw1-Fa0/11	Секретарь
8б	2	82	10.1.2.5	Sw1-Fa0/10	Директор
8б	2	83	10.1.2.6	Sw1-Fa0/11	
3	3/Финансовая	31	10.1.3.1	Sw2-Fa0/2	
3	3	32	10.1.3.2	Sw2-Fa0/3	
3	3	33	10.1.3.3	Sw2-Fa0/4	
3	3	34	10.1.3.4	Sw2-Fa0/5	
3	3	35	10.1.3.5	Sw2-Fa0/6	
3	3	36	10.1.3.6	Sw2-Fa0/7	
3	3	37	10.1.3.7	Sw2-Fa0/8	
3	3	38	10.1.3.8	Sw1-Fa0/9	
3	3	39	10.1.3.9	Sw1-Fa0/11	
:	:	:	:		:
7	Сервер внутр.		10.1.1.30		LAN
	:	:	:		
	Сервер внутр.		10.1.7.30		
7	Сервер внеш.		10.1.0.2		DMZ
7	Маршрут-р		83.221.169.36	S1	ISP
7	Коммутатор1		10.1.0.3		
7	Коммутатор2		10.1.0.4		
7	Коммутатор3		10.1.0.5		
7	Коммутатор4				
10	7/Маркетинг	101	10.1.7.1	Sw3-Fa0/2	
10	7	102	10.1.7.2	Sw3-Fa0/3	
:	:	:	:		:
10	7	110	10.1.7.10	Sw3-Fa0/11	

При этом следует помнить, что необходимо зарезервировать адреса для портов маршрутизатора(ов) и портов управления коммутаторов.

Для маршрутизатора выделено два частных адреса. Адрес 10.1.9.225 выделен для порта, соединенного с локальной сетью организации, а адрес

10.1.9.226 — для порта, соединенного с сервером демилитаризованной зоны.

8.6. Разработка физической структуры сети

8.6.1. Схема размещения компонентов СКС

В этом разделе пояснительной записки проекта проводися разработка структурированной кабельной системы (СКС) и схема размещения и соединения телекоммуникационного оборудования. При этом учитываются требования и нормы международных и национальных стандартов [41-44]. Основные положения проектирования СКС освещены в подразделе 3. Расчет кабельной системы можно выполнять вручную или использовать автоматизированную систему [www.netwizard.ru]. Результатом разработки схемы является чертеж, на котором указаны места размещения телекоммуникационных розеток, розеток электропитания, ввода телекоммуникационных и силовых кабелей в помещение с указанием геометрических размеров и текстовое описание. Собственно схема размещения выполняется на чертеже формата А1 в соответствии с требуемыми стандартами и нормативами [40]. Пример выполнения фрагментов такого чертежа приведен на рисунках 8.5 и 8.6.

Текстовая часть обоснования и описания схемы размещения может быть представлена в следующем виде.

Пример 8.4.

"Схема размещения компонентов сети разрабатывается на основе поэтажных чертежей здания, в котором располагается предприятие или организация. Во всех помещениях на каждом рабочем месте устанавливаются телекоммуникационные розетки (ТР) с двумя гнездами типа 8Р8С (RJ-45) и по три силовых розетки с напряжением 220 В. Количество ТР, рассчитанное на основании соответствующих технических норм, приведено в таблице 8.2. Телекоммуникационные розетки закрепляются в кабельных коробах на высоте 80 см от уровня пола. Расположение телекоммуникационных и электрических розеток и других компонентов сети в каждом из помещений предприятия с указанием установочных размеров показано на рисунке 8.5.

Все телекоммуникационные кабели прокладываются в декоративных пластмассовых кабельных каналах (коробах), которые закрепляются на стене помещения. Кабельный канал разделен на две секции. Одна служит для укладки телекоммуникационных кабелей, а вторая — для силовых кабелей. Телекоммуникационные розетки монтируются на корпусе короба, либо на стене. Силовые розетки в количестве 3 шт на каждое рабочее место закрепляются на расстоянии 0,8 м от уровня пола. На такой же высоте устанавливаются и телекоммуникационные розетки.

Вывод пучка кабелей горизонтальной подсистемы осуществляется через металлический патрубок (кондуит) диаметром 80 мм, который пропускается через

стену помещения на расстоянии 0,2 м от потолка. В коридоре коммуникационные кабели укладываются в кабельный лоток, который закреплен между потолочным перекрытием и подвесным потолком. Силовые кабели выводятся через отдельный собственный кондуит и укладываются в межпотолочном пространстве в лоток силовых кабелей.

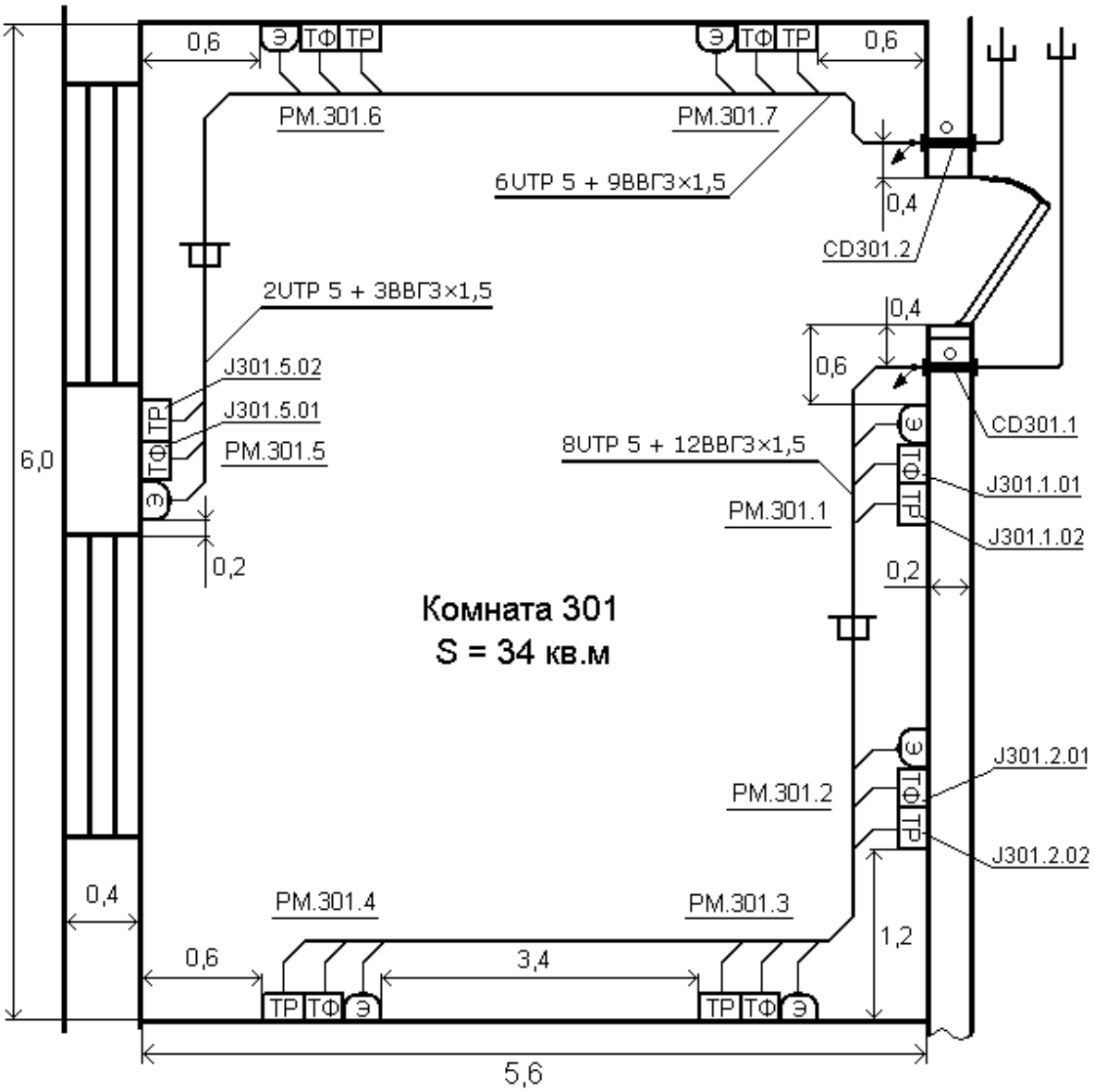


Рисунок 8.5 — Схема размещения компонентов компьютерной сети в помещении 301

На рисунке 8.6 изображена схема размещения компонентов и оборудования сети в техническом помещении, используемом в качестве распределительного пункта этажа (серверной). В этом помещении установлен телекоммуникационный шкаф, в котором устанавливаются распределительные (патч) панели, коммутаторы канального и сетевого уровней, маршрутизатор, а также серверное оборудование. Здесь же располагается щит силового электропитания. Расстояние между коммуникационным шкафом и стеной помещения выбрано таким

образом, чтобы обеспечить доступ к распределительным панелям при монтаже или замене кабелей. Коммуникационные кабели и силовые заводятся в помещение через раздельные кондуиты.

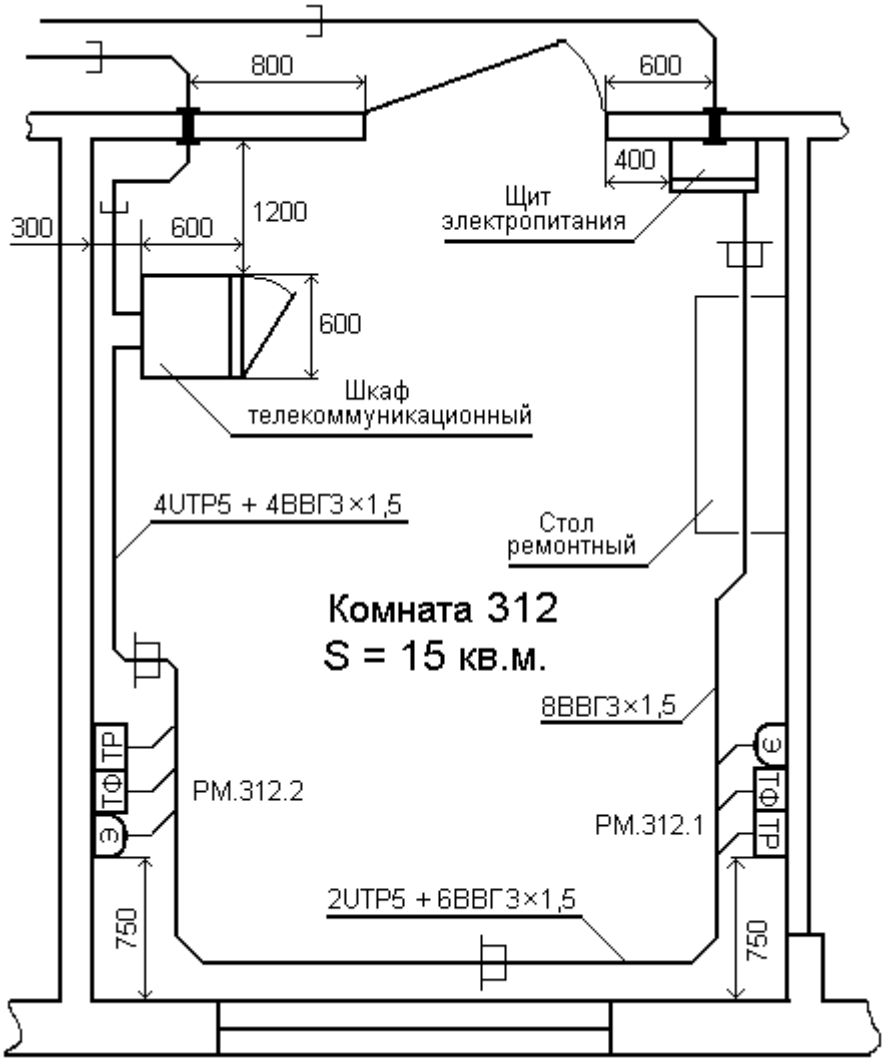


Рисунок 8.6 – Схема размещения компонентов СКС в техническом помещении

Ввод коммуникационных кабелей в шкаф осуществляется через верхнее входное отверстие, имеющееся в его крыше. Кабели подводятся сверху в лотке и затем через верхний вводной люк водятся внутрь шкафа. При этом способе к кабелям нет доступа, и они хорошо физически защищены. Четыре кабеля силового питания типа ВВГ 3 сечением 1,5 мм^2 каждый и 4 телекоммуникационных кабеля, идущих от рабочих мест РМ.301.1 и РМ.301.2, подводятся к телекоммуникационному шкафу в пластмассовом коробе и вводятся в него через нижний вводной люк.

В помещении также оборудовано два рабочих места: одно для администратора сети или лица, выполняющего его функции, а второе — для инженера-электронщика. Телекоммуникационные и силовые розетки рабочих мест закреп-

ляются на стене, на высоте 0,8 м от уровня пола. Остальные установочные размеры показаны на чертеже. Для тестирования и ремонта оборудования установлен специальный стол монтажника».

8.6.2. Выбор типов кабелей и расчет величины расхода кабеля

Обоснование и выбор типов кабелей для проектируемой компьютерной сети осуществляется на основе рекомендаций, изложенных в подразделе 3.2. Как уже отмечалось выше, выбор кабельной подсистемы в целом для любой из подсистем СКС определяется типом сети и выбранной топологией.

Наиболее рациональным для горизонтальной кабельной подсистемы является применение медных неэкранированных кабелей типа UTP. Оптоволоконный кабель целесообразно использовать в основном в кампусных и вертикальных подсистемах. Однако, следует иметь в виду, что хотя по мере развития технологий цены на кабели категорий 6 и 7 снижаются, однако параллельно дешевеют и оптоволоконные системы и оптоволоконные кабели становятся все более конкурентноспособными по отношению к медным кабелям даже на уровне подключения рабочих станций к сети.

Медные кабели для СКС характеризуются рядом параметров, в частности:

- волновое сопротивление (*Impedance*);
- затухание (*Attenuation*);
- переходная помеха на ближнем конце NEXT (*Near End Cross Talk*);
- переходная помеха на дальнем конце FEXT (*Far End Cross Talk*);
- нормированное (приведенное к уровню полезного сигнала) значение FEXT — ELFEXT;
- характеристики взаимных помех между парами *PowerSum FEXT*, *Power-Sum ELFEXT* и *PowerSum NEXT*;
- защищенность от переходных помех ACR (*Attenuation to Crosstalk Ratio*);
- задержка распространения сигнала (*Propagation Delay*);
- неравномерность задержки распространения сигнала (*Delay Skew*).

В данном подразделе следует в краткой форме (в виде таблиц) представить данные об электрических и стоимостных характеристиках современных медных кабелей 5-7 категорий и оптоволоконных одномодовых и многомодовых кабелей и обосновать выбор того или иного типа кабеля. При защите проекта студент должно хорошо представлять физическую суть этих параметров и уметь пояснить влияние их на информационные характеристики компьютерной сети.

В данный подраздел можно включить обоснование следующего содержания.

Пример 8.5.

«С учетом того, что на уровне доступа передача данных выполняется преимущественно со скоростью 100 Мбит/с и с учетом возможности в перспективе увеличения скорости передачи для горизонтальной подсистемы выбираем кабель типа UTP4-C6-SOLID-GY. Это кабель 6-й категории типа неэкранированная витая пара (UTP), состоящий из 4 пар одножильных (*Solid*) медных проводников. Кабель соответствует стандарту пожарной безопасности UL 444 и UL 1581 и имеет следующие технические характеристики:

- диаметр проводника: 0,54 ± 0,01 мм (24 AWG);
- изоляция — полиэтилен повышенной плотности, минимальная толщина 0,18 мм;
- диаметр провода в изоляции 0,99 ± 0,02 мм;
- цвет витых пар: синий-белый/синий, оранжевый-белый/оранжевый, зеленый-белый/зеленый, коричневый-белый/коричневый;
- 4 витые пары с полиэтиленовым разделителем, покрыты поливинилхлоридной оболочкой (PVC) с минимальной толщиной оболочки 0,4 мм;
- внешний диаметр кабеля равен 6,2 ± 0,2 мм;
- рабочая температура кабеля от 20ºС до +75ºС;
- радиус изгиба кабеля: 8 диаметров (8х∅) во время инсталляции, 6х∅ при вертикальном каблировании, 4 диаметра при горизонтальном каблировании;
- стандартная упаковка размером 21,5 × 42 × 42 см (Ш×В×Г) — 305 м;
- вес кабеля без упаковки 12,9 кг.

Кабель характеризуется следующими электрическими параметрами:

- максимальное сопротивление проводника при температуре 20° С равно 9,38 Ом/100 м;
- дисбаланс сопротивления (относительная разность сопротивлений жил) не превышает 5%;
- емкостной дисбаланс пары по отношению к земле равен 330 пФ/100 м;
- сопротивление на частоте от 0,772 до 100 МГц составляет 85-115 Ом;
- максимальная рабочая емкость равна 5,6 нФ/м;
- неравномерность задержки 45 нс/100 м;
- задержка распространения <536 нс/100 м.

Таблица 8.6

Частотно-зависимые параметры кабеля

Частота МГц	Затухание дБ/100 м	NEXT дБ	ACR дБ/100м	PS NEXT дБ	EL-FEXT дБ/100м	PS EL-FEXT дБ/100м	RL дБ
31,25	11,4	45,9	34,6	42,9	33,9	30,9	23,6
62,5	16,5	41,4	25,8	38,4	27,8	24,8	21,5
100	21,3	38,3	19,0	35,3	23,8	20,8	20,1
155	27,2	35,5	10,8	32,5	19,9	16,9	18,7

Оптические параметры многомодового и одномодовых волоконно-оптических линий приведены в таблицах 8.6 и 8.7 соответственно.

Таблица 8.7

Оптические параметры многомодового оптоволокна

Тип волокна	Длина волны, нм	Затухание (среднее/ максимальное), дБ/км	Коэффициент широко-полосности, МГц·км	Дальность передачи для Ethernet, м		Коэфф. преломления
				1GbE	10 GbE	
62,5/125	850	3,0/3,2	>200	275	33	1,495
OM1	1300	0,7/0,9	>600	550	–	1,490
50/125	850	2,6/2,8	>600	550	82	1,481
OM2	1300	0,6/0,9	>1200	550	–	1,476

Таблица 8.8

Оптические параметры одномодового оптоволокна ITU-G.652B

Тип волокна	Диаметр, мкм	Длина волны, нм	Затухание (среднее/максимальное), дБ/км	Дисперсия, пс/(нм·км)	PMD, пс/км$^{1/2}$	Коэфф. преломления
9/125	9,2±0,4 125±0,5	1310	0,35/0,5	< 3,5	–	1,467
		1550	0,21/0,3	<18	<0,2	1,467

Параметр поляризационная модовая дисперсия PMD (*Polarization Mode Dispersion*) — это дисперсия, вызываемая небольшой асимметричностью поперечного сечения волокна. Асимметричность приводит к тому, что одна из двух основных ортогональных поляризованных мод передается по оптическому каналу связи быстрее, чем другая. Приемное устройство принимает комбинацию этих двух мод. В результате импульс на входе приемника становится шире импульса, генерируемого передатчиком, что приводит к необходимости снижения скорости передачи».

Общая потребность кабеля для реализации сети рассчитывается по методике, изложенной в разделе 3.2. При этом учитывается, что наибольшая длина кабеля горизонтальной подсистемы не должна превышать 90 м.

Пример 8.6.

«Рассчитаем количество кабеля, необходимое для прокладки горизонтальных линий связи для каждого этажа (включая цокольный) 6-этажного здания. Требуемое количество кабеля рассчитывается с использованием эмпирического метода [22, 24], основанного на предположении, что рабочие места распределены по обслуживаемой площади равномерно. Средняя длина $L_{ср}$ кабельных трасс вычисляется по формуле:

$$L_{ср} = (L_{max}+L_{min})/2,$$

где L_{min} и L_{max} — соответственно длины кабельной трассы от точки размещения кроссового оборудования до телекоммуникационного разъема самого близкого и самого далекого рабочего места, посчитанные с учетом технологии прокладки кабеля, всех спусков, подъемов, поворотов и особенностей здания. Величины L_{min} и L_{max} рассчитываются по плану здания и помещений, в которых размещается организация (см. подраздел 8.3).

При определении длины трасс необходимо добавить технологический запас величиной 10% от $L_{ср}$ и запас X для процедур разводки кабеля в распределительном узле и телекоммуникационном разъеме. С учетом сделанных дополнений формула нахождения общей длины кабельных трасс L принимет вид:

$$L= (1{,}1L_{ср}+X)\, N_р\ ,$$

где $N_р$ — количество розеток на этаже.

Дробные значения при расчетах округляем в большую сторону до целых.

Пусть для цокольного этажа измеренные длины L_{min} и L_{max} равны соответственно 29 и 45 метров, а количество коммуникационных розеток на этаже равно $N_р$= 7. Тогда

$$L_{ср} = (29+45)/2 = 37 \text{ м.}$$
$$L = (1{,}1\times37+2) \times7= 299 \text{ м.}$$

Для первого этажа L_{min} = 23 м; L_{max} = 60 м; $N_р$ = 21.

$$L_{ср} = (23+60)/\ 2= 42 \text{ м.}$$
$$L = (1{,}1\times42+2) \times21 = 1012 \text{ м.}$$

Для второго этажа L_{min} = 24 м; L_{max} = 69 м; $N_р$ =54.

$$L_{ср} = (24+69)/\ 2= 47 \text{ м.}$$
$$L = (1{,}1\times47+2) \times54 = 2900 \text{ м.}$$

Для третьего этажа L_{min} = 11 м; L_{max} = 21 м; $N_р$ = 20.

$$L_{ср} = (11+21)/\ 2= 16 \text{ м.}$$
$$L = (1{,}1\times16+2) \times20 = 392 \text{ м.}$$

Для четвертого этажа L_{min} = 6 м; L_{max} = 38 м; $N_р$ = 68.

$$L_{ср} = (6+38)/\ 2= 22 \text{ м.}$$
$$L = (1{,}1\times22+2) \times68 = 1782 \text{ м.}$$

Для пятого этажа L_{min} = 6 м; L_{max} = 30 м; $N_р$ =66.

$$\mathrm{L}_{ср} = (6+30)/\ 2= 13 \text{ м.}$$
$$\mathrm{L} = (1{,}1\times13+2) \times66 = 1076 \text{ м.}$$

Для шестого этажа L_{min} = 7 м; L_{max} = 35 м; $N_р$ = 68.

$$L_{ср} = (7+35)/\ 2= 21 \text{ м.}$$
$$L = (1{,}1\times21+2) \times68 = 1707 \text{ м.}$$

В итоге для горизонтальной подсистемы необходимо:

$L_{общ}$ = 299+1012+47+2900+392+1782+1076+1707 = 9215 м кабеля.

Известно, что в стандартной кабельной бухте содержится 305 метров кабеля. Тогда для создания горизонтальной подсистемы нужна 31 (9215/305=30,21) бухта, или 9455 метров кабеля (31×305=9455).

Кабели оканчиваются (терминируются) встраиваемыми в короб телекоммуникационными розетками RJ-45, способными подключать также телефонные коннекторы RJ-11. Для подсоединения оборудования рабочих мест СКС укомплектовывается патч-кордами.

Для выполнения силовой проводки целесообразно применить трехжильный медный кабель типа ВВГ 3×1,5 (Виниловая оболочка, Виниловая изоляция, Гибкий). Сечение кабеля должно составлять 1,5 мм^2. Такая величина выбирается из расчета максимального потребляемого тока 15 А (мощность 3,3 кВт) на одну розетку». Общая длина силового кабеля рассчитывается по тем же формулам, которые используются для расчета длины телекоммуникационного кабеля.

8.6.3. Расчет габаритных размеров декоративного кабельного короба

При расчетах диаметр горизонтального кабеля категории 5е принимается равным 5,2 мм, что соответствует площади поперечного сечения кабеля $S_{каб}$ =21,2 мм^2.

Коэффициент использования площади выбирается равным k_i = 0,5, а коэффициент заполнения — средним по стандарту TIA/ EIA-569-A и равным k_z = 0,45. При такой степени заполнения существенно упрощается эксплуатация кабельной системы и становится возможной при необходимости установка дополнительных ТР с прокладкой новых кабелей в существующих декоративных коробах. В случае острой необходимости иногда допускается увеличение этого параметра, но не выше максимального значения, установленного стандартом. В случае необходимости укладки в коробе и силового кабеля, следует выбирать многосекционный (минимум двухсекционные) декоративный короб. При этом также необходимо просчитать требуемые габариты секции короба для такого кабеля. Таким образом, требуемое сечение короба определяется по формуле

$$S_{крб} = (\sum S_{jкаб}) / (k_i k_z).$$

Результаты расчетов габаритов короба следует свести в таблицу 8.9.

После определения суммарного сечения кабелей выбирается стандартный тип короба с сечением, не меньше рассчитанного. На практике наиболее широко используются секции короба стандартной длины 2 м и сечением 40×16 мм, 60×16 мм и 75×20 мм.

Из расчетных данных следует, что в СКС требуется использовать короба типа NCT1050 двух типоразмеров: 60×16 мм и 75×20 мм, которые позволяют выполнять монтаж корпусов информационных и силовых розеток

рядом с коробом на поверхности стены. Две секции короба будут служить для прокладки горизонтальных информационных кабелей, а одна — для двух силовых кабелей (один для системы гарантированного электропитания компьютерного оборудования, другой обеспечивает подключение розеток бытового электроснабжения).

Таблица 8.9

Параметры декоративного кабельного короба

Наименование параметров	**Значение параметров**			
Количество обслуживаемых ТР	2	3	6	8
Количество горизонтальных кабелей	4	6	12	16
Требуемая площадь короба, мм^2	376	565	1130	1507
Габаритные размеры короба, мм	60×16	60×16	75×20	75×20

Кроме собственно короба для организации кабельных каналов требуется также ряд вспомогательных элементов: заглушки, соединители и плоские уголки, соединяющие короба при их поворотах на 90^0. Количество уголков и соединителей рассчитывается исходя из стандартной длины секции короба, равной 2-м метрам и количества поворотов кабельных трасс. Итоговые данные по элементам кабельного канализационного оборудования сводятся в таблицу спецификации комплектующих элементов кабельных каналов. Пример такой спецификации показан в таблице 8.10.

Таблица 8.10

Спецификация комплектующих элементов кабельных каналов

Тип	**Наименование компонентов**	**Ед. изм**	**Кол-во**
NCT1050	Короб 100×50	м	400
NCI1050	Соединитель 100×50	шт	190
NJC1050	Заглушка на шов 100×50	шт	190
NAF1050	Плоский угол 100×50	шт	20
NWP1050	Заглушка внутренняя 100×50	шт	40
YEP4	Заглушка 40×25	шт	65
YAF4	Плоский угол 40×25	шт	130

8.6.4. Выбор коммуникационного оборудования

В этом подразделе следует привести соображения, на основании которых было выбрано активное и пассивное телекоммуникационное оборудова-

ние. При обосновании необходимо, кроме технических характеристик, учитывать надежность и стоимость оборудования, пожелания и финансовые возможности Заказчика.

В настоящем проекте рекомендуется в качестве активного оборудования выбирать устройства (коммутаторы и маршрутизаторы) корпорации Cisco. Однако, это не исключает обоснованный выбор оборудования других производителей.

При выборе оборудования следует обращать внимание на новые и перспективные изделия. Следует избегать использования устройств, производство которых уже прекращено или выпуск которых прекращается в ближайшее время. Информацию о таком оборудовании можно получить на официальных сайтах производителей или дистрибьюторов.

В данном пособии в примерах конфигурации зачастую используется оборудование, снятое с производства, которое, однако функционирует в современных сетях. Это сделано преднамеренно для исключения копирования студентами рассмотренных примеров. Студенты же должны использовать модели, выпускаемые взамен устаревших или включать в состав проектируемой сети более перспективные аналоги рассмотренного оборудования.

После обоснования выбора нужно привести все технические и эксплуатационные параметры выбранных устройств. Пример обоснования и выбора пассивного и активного сетевого оборудования приведен ниже.

Пример 8.7.

«В качестве коммутационного оборудования для медных кабелей выберем 24-портовые коммутационные патч-панели типа «21-R0-45H024D0-2N1N» категории 5е для разделки кабелей горизонтальной подсистемы. Для подключения кабелей к коммутаторам и маршрутизатору через патч-панели предусмотрены соединительные шнуры (патч-корды) с разъемами типа 8P8C-8P8C (RJ45-RJ45) на обоих концах. Длина соединительных шнуров 1 м.

В качестве кросса для оптоволоконной части подсистемы внутренних магистралей выбираем оптические одномодовые распределительные полки с 8 разъемами типа SC-AS. Для обеспечения возможности укладки избытка соединительных коммутационных шнуров под оптическими полками предусмотрены организаторы кабеля, имеющие форму пластины с держателями кабеля.

При монтаже оптоволоконной части подсистемы внутренних магистралей предполагается использовать технологию сварки, которая обеспечивает минимальные потери в точке сращивания оптических волокон и наибольшую надежность соединения.

Перечень пассивного оборудования спроектированной сети приведен в таблице 8.11.

Пример обоснования выбора активного коммуникационного оборудования приведен ниже в примере 8.8.

Пример 8.8.

«В локальных компьютерных сетях на уровне доступа пользователей к сети целесообразно использовать коммутаторы фирмы Cisco типа Catalyst 29xx. Коммутаторы этой серии представляют собой полнофункциональную линию коммутаторов 10/100 Ethernet с автоматическим выбором скорости передачи и с поддержкой технологии создания виртуальных сетей. Устройства этой серии обеспечивают наилучшее соотношение цена/производительность среди устройств данного класса.

Таблица 8.11

Спецификация пассивного оборудования локальной сети

№№	Наименование компонентов	Ед. изм	Кол-во
1	EuroLAN MiNi настенная информационная розетка RJ45, кат.5e, 2-х портовая	шт	70
2	Кабель UTP 4PR–1583	м	5490
3	Кабель ВО 2–х жильный, 62,5/125	м	80
4	19" Патч-панель, 24×RJ45, 21-R0-45H024D0	шт	6
5	19" Оптическая пполка 24xSC-AS	шт	1
6	ST-MM Оптический коннектор	шт	8
7	Организатор кабельный горизонтальный	шт	4
8	Организатор кабельный вертикальный	шт	2
9	Модуль вентиляторный потолочный, 380×380 мм, 2 вент	шт	1
10	Шкаф напольный 41U, 2050×600×600, стеклянная дверь в стальной раме, ручка с замком с трёхточечной фиксацией	шт	1

Коммутаторы Catalyst 29XX имеют высокую производительность, простоту в эксплуатации и гибкостью в использовании. Эти устройства могут применяться как для создания высокопродуктивных рабочих групп, так и для объединения групп серверов и коммутаторов предыдущего уровня, например, Catalyst 1900/2820. Коммутаторы серии Catalysl 29XX поставляются с пожизненной гарантией, которая предусматривает бесплатный заводской ремонт оборудования в течение всего времени поддержки устройства.

Для проектируемой компьютерной сети для обеспечения подключения на уровне доступа 62-х рабочих станций выбраны сетевые коммутаторы типа Cisco Catalyst 2950-24. Коммутатор Catalyst 2950C-24 — это 25-х портовый коммутатор уровня доступа, предназначенный для построения малых и средних локальных сетей. Устройство рассчитано на круглосуточную работу и характеризуется высокой производительностью и широкими функциональными возможностями.

Коммутатор автоматически определяет скорость передачи на каждом порту (10/100 Мбит/с), поддерживает протокол качества обслуживания (QoS), предоставляет возможность управления группой коммутаторов и допускает соединения коммутаторов в стек. Основные технические параметры коммутатора типа Catalyst 2950 приведены в таблице 8.12.

Для решения задач маршрутизации был выбран маршрутизатор Cisco 3640. Выбор обосновывается следующими причинами:

- модульность маршрутизатора позволяет легко набрать необходимое количество интерфейсов локальных и глобальных сетей;
- многопротокольность маршрутизатора дает возможность обрабатывать трафик IP и IPX;

Таблица 8.12

Технические характеристики коммутатора доступа

Параметр	**Значение**
Тип сети	Fast Ethernet Ethernet
Количество базовых портов	24 (24 макс.)
Буфер памяти (на один порт)	8 МБ
Скорость передачи по UPLINK	100 Мбит/с
Индикаторы	- активное соединение - полнодуплекс / полудуплекс - состояние соединения - электропитание
Поддерживаемые стандарты	- IEEE 802.3 (Ethernet) - IEEE 802.3u (Fast Ethernet)
Размер таблицы MAC адресов (L2)	8192
Методы коммутации	store-and-forward
Протоколы удаленного управления	- SNMP - Telnet - Console
Пропускная способность	6,8 Гбит/с
Среда передачи	Ethernet 10/100BaseT - категория 5 НВП
Параметр	**Значение**
	- скорость передачи до 100 Мбит/с - длина сегмента до 100 м Ethernet 100baseFX - MMF 62,5 микрон - скорость передачи до 100 Мбит/с - длина сегмента до 2 км
Интерфейсы	- 24 × Ethernet 10/100BaseT • RJ-45 (half / full duplex mode); - 2 × Ethernet 100baseFX • MT-RJ (half / full duplex mode)
Электропитание	- встроенный блок питания; 200 …240 В (переменный ток); - потребляемая мощность 30 Вт
Габариты (Высота × Ширина × Глубина), Вес	44,5 × 4,36 × 24,18 мм, 3 кг

- поддержка фильтров IPX в Cisco IOS позволяет контролировать доступ к ресурсам в сети Novell Netware;
- высоко производительный RISC процессор, установленный в Cisco 3640, обеспечивает обработку трафика без потерь при подключении ЛВС на скорости l00 Мбит/с».

Аналогичное обоснование следует привести и для коммутаторов уровня распределения.

Пример 8.9. Вариант описания размещения оборудования и схемы подключения кабелей.

«Для размещения коммутационного оборудования СКС и активного оборудования ЛВС в здании предусмотрено техническое помещение (комната №312). В этом помещении устанавливается 19"-й телекоммуникационный шкаф, в который в соответствии с логической схемой сети вмонтируются:

1) одна 19" оптическая панель 24×ST высотой 1U;
2) 3 патч-панели на 24 портов RJ-45 для терминирования кабелей горизонтальной подсети;
3) 3 патч-панели на 24 портов RJ-45 для терминирования кабелей телефонной связи;
4) 4 горизонтальных кабельных органайзеров высотой 1U каждый;
5) 2 вертикальных кабельных органайзера;
6) два коммутатора Cisco Catalyst 2950 на 12 портов каждый 10/100 RJ-45 высотой 1U каждый;
7) маршрутизатор Cisco 3640 высотой 1U;
8) два сервера высотой 2U каждый;
9) блок бесперебойного питания высотой 4U;
10) блок электрических розеток высотой 1U;
11) панель вентиляторов потолочная на 2 вентилятора высотой 1U;

В итоге для размещения оборудования в шкафе требуется высота 29U. С учетом 30-процентного запаса требуемая высота шкафа составляет 40U. На основании этого выбираем телекоммуникационный шкаф со стандартной высотой 41U (2030 мм). Для закрытия неиспользуемого пространства шкафа предусмотрим панели заглушки общей шириной 10U. Для коммутации шкаф укомплектовывается патч-кордами длиной 0,5, 1 и 1,5 м. Схема размещения оборудования в телекоммуникационном шкафу изображена на рисунке 3.10.

Точки подключения коммуникационных кабелей приведены в таблице 8.13.

Как видно из таблицы, кабель с нечетным номером С301.1.1 подсоединяется в комнате 301 на рабочем месте к телефонной розетке J301.1.01, а кабель с четным (С301.1.2) – к телекоммуникационной розетке J301.2.02. В распределительном пункте этажа (комната 312) телефонный кабель подсоединяется к порту 01 распределительной телефонной кросс-панели с индексом МС. 312.28. Кабель данных, имеющий четный номер С301.1.2, в телекоммуникационном шкафу кодсоединяется к порту 01 патч-панели МС. 312.23. Принцип подключения остальных кабелей аналогичен.

Таблица 8.13

Таблица кабельных соединений

ID кабеля	Трасса	Позиция начального терминирования / позиция конечного терминирования	Рабочая комната / кроссовая	Тип кабеля / длина кабеля в метрах	Приложение / оборудование
C301.1.1	CD301.1	J301.1.01 / MC. 312.28-01	301 / 312	Категория 5/ 18	ТФ01
C301.1.2	CD301.1	J301.2.02 / MC. 312.23-01	301 / 312	Категория 5/ 18	PC 01
- - -	- - -	- - -	- - -	- - -	- - -
C301.7.1	CD301.2	J301.7.01 / MC. 312.28-07	301 / 312	Категория 5/ 14	ТФ07
C301.7.2	CD301.2	J301.7.02 / MC. 312.23-07	301 / 312	Категория 5/ 14	PC 07

Кабели с рабочих мест с 1-го по 4-е проходит через кондуит CD301.1, а кабели с рабочих мест с 5-го по 7-е – через кондуит CD301.2».

8.7. Разработка политики информационной безопасности в сети предприятия

8.7.1. Формулирование требований к безопасности проектируемой сети

В этом подразделе нужно подробно расписать процессы взаимного обмена информацией между пользователями, между пользователями и различными службами и приложениями, а также выделить направления и пути информационных потоков, запрещенных в данной сети. Необходимо также сформулировать общие требования к безопасности проектируемой сети. Кроме этого, в данном подразделе разрабатываются и подробно описываются положения специфических политик безопасности для отдельных видов обслуживания, указанных в варианте задания.

На этом этапе проектировщик сети должен тесно сотрудничать с руководством и со службой безопасности предприятия (в учебном проекте с руководителем проекта). Именно они определяют, кто с кем и в какое время

могут обмениваться данными, к каким службам и типам данных им разрешен доступ. Результатом такого взаимодействия являются списки доступа.

При разработке общих требований к обеспечению безопасности компьютерной сети предприятия указывается, что в компьютерной сети должен быть реализован ограниченный доступ сотрудников к ресурсам сети в соответствии с должностными обязанностями, а также зарыт доступ из вне к ресурсам локальной сети предприятия, за исключением сервера предприятия, установленного в демилитаризованной зоне. Указано, что должен быть четко установлен и соблюдаться регламент взаимодействия сотрудников с Интернетом, использоваться пароли, обеспечивающие достаточную степень защиты, а сами пароли регуляно обновляться. В состав программного обеспечения сети обязательно должен входить пакет антивирусной защиты, а вирусные базы регулярно обновляться [14,19,26].

8.7.2. Примеры разработки специфических политик для отдельных сервисов

В соответствии с таблицей вариантов задания на проектирование необходимо разработать детальные политики безопасности для отдельных видов обслуживания (Приложение А1), в частности:

- при удаленном доступе к ресурсам предприятия;
- при взаимодействии с Интернет;
- при получении доступа к сетевым ресурсам;
- при выборе и использовании паролей;
- при защите от вирусов.

В данном разделе записки должны быть разработаны и размещены тексты инструкций, реализующих те или иные требования политики безопасности. Ниже приведены образцы примеров специфических политик безопасности. Большинство из этих примеров являются выдержками из политик безопасности конкретных предприятий или организаций. [www.compdoc.ru/network/internet/politicians_of_safety/].

Пример 8.10. Политика удаленного доступа.

«1. Сотрудник предприятия несет ответственность за последствия неправильного использования удаленного доступа.

2. Высокоскоростной удаленный доступ через каналы сетей ATM и Frame Relay разрешается только сотрудникам службы безопасности сети, администратору сети, главным специалистам предприятия, другим специалистам предприятия, выезжающим в служебную командировку и сотрудникам службы сбыта.

3. Сотрудники, менеджеры продаж и выездные специалисты компании, обладающие удаленным доступом к корпоративной сети предприятия, несут такую же ответственность как и в случае локального подключения к сети компании.

4. Перед осуществлением удаленного доступа к корпоративной сети следует ознакомиться по роспись в журнале учета со следующими политиками безопасности:

а) допустимого шифрования;

б) организации виртуальных частных сетей;

в) безопасности беспроводного доступа;

г) допустимого использования.

5. Защищенный удаленный доступ должен постоянно контролироваться. Ответственность за контроль возлагается на начальника службы безопасности.

6. Требуемый уровень безопасности должен обеспечивается посредством использования однократных паролей или инфраструктуры открытых ключей.

7. Сотрудники, имеющие привилегию удаленного доступа к корпоративной сети, не имеют права использовать адреса электронной почты компании для ведения собственного бизнеса.

6. Сотрудник компании несет личную ответственность за то, чтобы член его семьи не нарушил правила политик безопасности компании, не выполнил противозаконные действия и не использовал удаленный доступ для достижения собственных деловых интересов.

7. Сотрудникам запрещается передавать или посылать по электронной почте свой пароль на вход в систему, включая членов семьи.

8. Сотрудники, имеющие право удаленного доступа должны гарантировать, что их компьютеры, которые удаленно подключены к сети, не подключены в то же самое время ни в какую другую сеть, за исключением домашних сетей, которые находятся под полным управлением сотрудника.

9. Для членов семьи сотрудника компании доступ к Internet через сеть компании разрешается только в случае оплаты трафика самим сотрудником.

10. Маршрутизаторы для выделенных ISDN линий, сконфигурированные для доступа к корпоративной сети, должны использовать для аутентификации, как минимум, процедуру CHAP.

11. Для получения дополнительной информации относительно удаленного доступа, включения и отключения услуги, поиска неисправностей и т.д., следует обращаться на вебсайт службы организации удаленного доступа к информационным ресурсам компании».

Перечень требований данной политики может быть расширен и дополнен. Другим примером фрагмента политики безопасности по разграничению доступа в локальную вычислительную сеть (ЛВС) является следующий [www.zahist.narod.ru/securelan4.htm].

Пример 8.11. Разграничение доступа в сеть.

«1. Каждый персональный компьютер должен иметь "владельца" или " системного администратора", который является ответственным за работоспособность и безопасность компьютера, и за соблюдение всех политик и процедур, связанных с использованием данного компьютера.

2. Пользователи должны быть обучены и обеспечены соответствующими руководствами так, чтобы они могли корректно соблюдать все политики и процедуры безопасности.

3. Все механизмы защиты сервера ЛВС должны находиться под монопольным управлением местного администратора и местного персонала Администраторов ЛВС.

4. Программное обеспечение должно быть лицензированым и является безопасным.

5. За все изменения (замены) программного обеспечения и создание резервных копий данных на серверах отвечают Администраторы ЛВС.

6. Каждому пользователю должен быть назначен уникальный ИДЕНТИФИКАТОР ПОЛЬЗОВАТЕЛЯ и начальный пароль (или другая информация для идентификации и аутентификации), только после того, как закончено оформление надлежащей документации.

7. Пользователям запрещается совместно использовать назначенные им ИДЕНТИФИКАТОРЫ ПОЛЬЗОВАТЕЛЯ.

8. Пользователи должны аутентифицироваться в ЛВС перед обращением к ее ресурсам.

9. ИДЕНТИФИКАТОР ПОЛЬЗОВАТЕЛЯ должен удаляться после продолжительного периода неиспользования.

10. Использование аппаратных средств мониторинга ЛВС, маршрутизаторов или регистраторов трафика должно быть авторизовано и проводиться под контролем Администраторов ЛВС.

11. Служащие, ответственные за управление, функционирование и использование ЛВС предприятия должны пройти курс обучения в области компьютерной безопасности и правил работы на компьютере.

11. Отчеты о безопасности ЛВС должны готовиться и рассматриваться ежедневно».

На каждом предприятии, использующем сетевые информационные технологии, должны быть разработаны правила предоставления доступа к информационным ресурсам. Такие правила разрабатываются персоналом службы безопасности и являются обязательными для каждого пользователя компьютерной сети. Ниже приведе пример таких правил.

Пример 8.12. Доступ к ресурсам.

«Для предоставления доступа к информационным ресурсам пользователи направляют в подразделение информационных технологий (ИТ) заявку в установленной форме с ходатайством непосредственного руководителя заявителя и визой владельца информационного ресурса (В заявке указываются Ф.И.О. пользователя, наименование ресурсов и обоснование необходимости). В случае доступа к информационному ресурсу категории конфиденциально «К» обязательна подпись администратора информационной безопасности.

С целью получения доступа к внешним информационным ресурсам, пользователь направляет в подразделение информационных технологий письмо по установленной форме, с ходатайством непосредственного руководителя, согласованное со службой сетевой безопасности. (Данное письмо необходимо для тех организаций, где доступ в Интернет и использования электронной почты требует отдельного разрешения).

1. При наличии технической возможности специалисты соответствующих подразделений ИТ производят подключение пользователя к информационному ресурсу с внесением необходимых изменений в терминальное и коммуникационное оборудование (присвоением компьютеру пользователя сетевого имени, выдача соответствующего идентификатора, имени пользователя, пароля и т.д.).

2. При работе на одном компьютере нескольких пользователей, каждый из них должен применять свою учетную запись для доступа к информационному ресурсу.

3. Каждый пользователь обязан хранить свой пароль в тайне и изменять его по мере необходимости (для информации категории «К» не реже 1 раза в месяц).

4. Заявки пользователей на создание учетных записей и на предоставление доступа к информационному ресурсу хранятся в подразделении ИТ в течение времени действия учетной записи пользователя.

5. Пользователям запрещается несанкционированно использовать информационные ресурсы, доступа к которым он не имеет. Контроль доступа обеспечивается средствами операционных систем, средствами контроля доступа специализированных приложений, сертифицированными средствами защиты от несанкционированного доступа, а также средствами сетевого мониторинга и аудита.

Пример 8.13. Аннулирование доступа.

1. В случае увольнения или перевода в другое подразделение (отдел, бюро и т.д.) сотрудника, являющегося пользователем информационного ресурса, его непосредственный руководитель обязан известить соответствующего администратора объекта информатизации для аннулирования доступа к информационному ресурсу.

2. Не информирование администратора влечет за собой дисциплинарную ответственность.

3. Сверка по увольнениям и перемещениям сотрудников должна осуществляться не реже 1 раза в месяц.

Пример 8.14. Обслуживание информационных систем.

Пользователям запрещается использовать информационные ресурсы предприятия и средства вычислительной техники (СВТ) в целях, не связанных с выполнением должностных обязанностей.

Установка и настройка программного обеспечения.

1. К установке на СВТ разрешается только программное обеспечение (ПО), включенное в реестр протестированного и разрешенного службой ИТ к применению программного обеспечения.

2. Подразделение ИТ составляет и обновляет реестр системного и прикладного ПО, разрешенного к установке на СВТ пользователей и пользователей сети. Реестр обновляется в соответствии с потребностями пользователей и тенденциями в развитии программного обеспечения.

3. Любой пользователь может быть инициатором внесения в реестр новых программных продуктов. Для внесения программного продукта в реестр пользователи направляют заявку.

4. Программный продукт, указанный в заявке, тестируется специалистами ИТ, после чего принимается решение о включении его в реестр.

5. Установку и переустановку любого общесистемного, сетевого и антивирусного программного обеспечения, а также всех информационных систем, разрабатываемых на предприятии, на СВТ пользователей и пользователей сети производят только службы ИТ в соответствии со спецификой ПО. Самостоятельно устанавливать и переустанавливать программные продукты пользователям запрещается.

6. Пользователям запрещается менять настройки применяемого ПО без согласования с администратором сети. Изменение настроек общесистемного, сетевого и антивирусного ПО запрещено без согласования с администратором сети.

7. Допускается самостоятельная установка и переустановка прикладного ПО пользователями по согласованию с системным администратором сети.

Обмен данными.

1. Пользователи при обмене данными с применением внешних носителей информации обязаны производить проверку носителей на наличие вирусов перед началом работы с данными, содержащимися на них.

2. Наличие на компьютерах сетевых пользователей ресурсов общего доступа (доступ «полный», «на чтение», «определяется паролем») не допускается. Обмен информацией осуществляется посредством почтового сервера предприятия или через информационные ресурсы, расположенные на серверах предприятия. Весь почтовый обмен производится только через электронные почтовые ящики, открытые на почтовом сервере предприятия.

3. Пользователям запрещается хранить на СВТ, а также на информационных ресурсах, открытых на серверах для обмена и хранения данных, информацию и программные средства не связанные с выполнением должностных обязанностей.

4. При обмене и передачи информации, отнесенной к категории «К», должны применяться сертифицированные средства криптозащиты информации и электронная цифровая подпись.

Обеспечение сохранности данных.

1. Является обязательным архивирование критически важных данных для обеспечения деятельности предприятия. Для архивирования применяются специальные аппаратно-программные средства.

.2. Ответственность за утерю, порчу и сохранность информации, хранящейся на накопителях различного типа, возлагается на пользователя. Для резервного хранения информации пользователям сети могут предоставляться специальные информационные ресурсы на серверах. Информационные ресурсы создаются по заявке, направляемой в центр информационных технологий от имени начальника подразделения. В заявке на создание информационного ресурса необходимо указать размер информационного ресурса, ответственного за ресурс, необходимость и периодичность резервного сохранения данных. В заявке на предоставление ресурса можно указать прочих пользователей, доступ для которых к данному ресурсу открыт.

3. Помимо информационных ресурсов для хранения на серверах сети, для резервного копирования пользователи сети могут использовать внешние носители информации.

Пример 8.15. Антивирусная защита.

1. Применение антивирусной защиты на рабочих станциях и серверах является обязательным.

2. Ответственность за обновление антивирусного ПО и антивирусных баз данных возлагается на системного администратора сети.

3. Ответственность за установку и настройку антивирусного ПО на компьютерах пользователей сети возлагается на подразделения информационных технологий (ИТ). На компьютерах пользователей в обязательном порядке должна быть установлена программа антивирусной защиты, работающая в фоновом режиме, отслеживающая все операции по открытию, копированию и перемещению файлов на компьютере, а также автоматически производящая ежедневную проверку всех дисков и памяти ПЭВМ на наличие вирусов.

4. Ответственность за антивирусную защиту информации на компьютере пользователей возлагается на пользователя, за которым закреплен данный компьютер. Пользователи обязаны обратиться в подразделения ИТ для получения действующего на предприятии антивирусного ПО.

Пользователь сети обязан:

- перед началом работы убедиться, что программа антивирусной защиты на его компьютере запущена;
- не допускать использования и хранения на своем рабочем месте автономных носителей информации не проверенных на наличие вирусов;
- при обнаружении вируса произвести его лечение средствами антивирусной защиты, установленными на компьютере пользователя и сообщить об обнаружении вируса системному администратору сети и администратору информационной безопасности.
- пользователям запрещается распространять, хранить и создавать вредоносные программы.

Пример 8.16. Обеспечение конфиденциальности информации.

1. Пользователи обязаны принять все возможные меры для предотвращения несанкционированного доступа со стороны посторонних лиц к хранящейся на СВТ конфиденциальной информации.

2. Администратор информационной безопасности при необходимости получения доступа к ресурсам ПЭВМ, при проведении служебных проверок, обязан поставить в известность пользователя данного ПЭВМ или руководителя подразделения пользователя.

3. Все пользователи обязаны принимать участие в обеспечении режима информационной безопасности при работе с информационными ресурсами предприятия и на компьютере, а именно:

- предотвращать возможность несанкционированного доступа посторонних лиц к информации, хранящейся на информационных ресурсах и на ПЭВМ;
- выполнять требования «Инструкции о пропускном режиме» в части автономных носителей информации (дискеты, CD-R, CD-RW,DVD-RW, Flash-memory, сотовые телефоны, цифровые диктофоны, фотоаппараты и видеокамеры) и элементов компьютерной техники;

• немедленно информировать администраторов объектов информатизации о случаях нарушения режима информационной безопасности, в том числе, связанных как с аварийными (сбойными) ситуациями при эксплуатации компьютерной техники, так и с появлением реальных каналов утечки информации путем умышленного разрушения программно-аппаратных механизмов защиты информационных ресурсов;

• магнитные диски и иные носители информации (дискеты, CD-R, CD-RW, DVD-, Flash-memory, сотовые телефоны, цифровые диктофоны, фотоаппараты и видеокамеры), получаемые от других сотрудников или других организаций, перед использованием должны быть подвергнуты обязательному входному контролю на наличие программных вирусов.

Пользователям информационных ресурсов и ПЭВМ запрещается:

• производить очистку журнала аудита;

• самостоятельно изменять аппаратные конфигурации и подключать периферийные внешние устройства;

• несанкционированное копирование информации (файлов) на внешние носители;

• нерегламентированный просмотр, вывод на печать и т.п. информации ограниченного распространения;

• оставлять без присмотра закрепленную за ним компьютерную технику без ее отключения или блокировки на время отсутствия пользователя, или без установки специального программного обеспечения поддержки дежурного режима (хранители экрана) с обязательной установкой пользователем произвольного пароля, неизвестного другим лицам;

• оставлять на рабочих столах в свое отсутствие автономные носители информации, содержащие данные конфиденциального характера».

Помимо представленных выше документов можно создать инструкции для пользователей и администраторов по отдельным видам деятельности. Например, по работе в Интернет, работе с почтой, архивированию данных и т.д.

8.7.3. Разработка правил доступа персонала к информационным ресурсам

В этом подразделе формулируются конкретные права доступа к сетевым ресурсам каждого их сотрудников предприятия. На практике такие правила составляются на основании требований и пожеланий руководства организацией и ее службы безопасности. Затем эти правила оформляются в форме таблиц доступа, в которых указывается, с каких сетей разрешается доступ к другим сетям, кому и в какое время разрешается доступ к тому или иному ресурсу, а к каким ресурсам доступ запрещается. Формы таких таблиц могут иметь следующей вид (Таблица 8.13). В этой таблице показан пример взаимодействия между рабочими группами, регулируемого на уровне телекоммуникационных устройств (маршрутизаторов и коммутаторов). Разграниче-

ние доступа на уровне серверов и клиентских компьютеров осуществляется отдельными установками, не входящими в задачу данного проекта.

Таблица 8.13

Регламентация взаимодействия между виртуальными сетями

Рабочая группа / VLAN	**Разрешен доступ к виртуальным сетям**					
	Админ. 1/VLAN	Управл. 2/VLAN	3/VLAN	4/VLAN	5/VLAN	6/VLAN
1/VLAN1	Да	Нет	Нет	Нет	Нет	Нет
2/VLAN2	Да	Да	Нет	Нет	Нет	Нет
3/VLAN3	Да	Да	Да	Нет	Нет	Нет
4/VLAN4	Да	Да	Нет	Да	Нет	Нет
5/VLAN5	Да	Да	Нет	Нет	Да	Нет
6/VLAN6	Да	Да	Да	Нет	Нет	Да
7/VLAN7	Да	Да	Нет	Да	Да	Нет

В таблице взаимодействия отмечено, что сотрудникам группы информационной поддержки разрешается доступ к компьютерам всей сети организации (предприятия). Это объясняется необходимостью осуществления технической и программной поддержки инфраструктуры компьютерной сети. Разрешение доступа из одних сетей в другие предоставляется на основании производственной необходимости и с учетом политики информационной безопасности.

Таблица 8.14

Регламентация доступа к сети Интернет

Ф.И.О.	**Должность**	**Запрещенные типы файлов**	**Дни доступа**	**Время доступа**
Иванов А.Б.	Директор		1-7	6.00-24.00
Бондарь В.В.	Гл.бухгалт.	mp3; avi; exe	1-6	8.00-22.00
Гонтарь С.П.	Нач. отдела		1-5	8.00-18.00
Репин А.И.	Сет.админ.		1-7	Не огран.
Аулова Д.С.	Бухгалтер	mp3; avi; exe	1-5	8.00-18.00
Янин А.П.	Менеджер	mp3; avi; exe	1-5	8.00-18.00
Кобзарь И.Г.	Инженер		1-5	8.00-18.00
Бадов Р.П.	Техник	mp3; avi; exe	1-5	8.00-18.00
Бадов Р.П.	Техник	mp3; avi; exe	1-5	8.00-16.00
Другие служащие		exe	1-5	12.00-13.00

Следующим регламентируемым видом доступа является доступ сотрудников организации в Интернет. Правила доступа должны регулировать доступ к ресурсам Интернета отдельным сотрудникам, либо группам пользователей. Этими правилами могут быть установлены типы протоколов, ви-

ды данных, разрешенных к приему и передаче, разрешен или запрещен доступ к отдельным сайтам, указано время и дни недели, в которые разрешено выходить в Интернет и другие ограничения.

В таблице 8.14, в качестве примера, указаны ограничение на доступ в Интернет по дням недели и времени и на виды передаваемых или принимаемых файлов, а в таблице 8.15 внесены временные ограничения на доступ к внутренним серверам корпоративной сети.

Таблицы доступа могут иметь другой вид и содержать иные ограничения, ограничения по размеру входящих и (или) исходящих сообщений, на наличие вложенных и исполняемых файлов и т.п.

Таблица 8.15

Регламентация доступа к внутренним серверам

Ф.И.О.	**Должность**	**Доступ разрешен/ запрещен (+ / –)**		**Дни доступа**	**Время доступа**
		Сервер 1	Сервер 2		
Иванов А.Б.	Директор	+	+	1-7	7.00-22.00
Бондарь В.В.	Гл. бухгалт.	+	–	1-7	7.00-22.00
Гонтарь С.П.	Нач. отдела	–	+	1-6	7.00-20.00
Репин А.И.	Админ.	+	+	1-7	0.00-24.00
Аулова Д.С.	Бухгалтер	–	–	1-5	8.00-18.00
Янин А.П.	Менеджер	–	+	1-5	8.00-18.00
Кобзарь И.Г.	Инженер	–	+	1-5	8.00-18.00
Бадов Р.П.	Техник	–	+	1-5	8.00-18.00
Другие служащие		–	–	1-5	12.00-13.00

8.8. Разработка скриптов конфигурации коммуникационного оборудования

В данном подразделе необходимо изобразить логическую схему сети с указанием типа оборудования, адресов виртуальных подсетей, рабочих станций, интерфейсов маршрутизаторов и коммутаторов. Пример такой схемы показан на рисунке 8.7.

Затем приводятся полные тексты сценариев (скриптов) конфигурации оборудования, которое входит в состав разработанной компьютерной сети. Для каждого типа оборудования составляются соответствующие сценарии конфигурации с учетом применяемой в нем сетевой операционной системы. Составление скриптов следует начинать с оборудования уровня доступа. В начале каждого скрипта должна быть освещена суть процедуры, а затем следует соответствующий сценарий конфигурации. Все скрипты должны сопровождаться подробными комментариями.

Сценарии должны включать следующие разделы:

- начальная конфигурация устройств;
- настройка интерфейсов;
- создание подсетей или виртуальных сетей;
- обеспечения взаимодействия подсетей;
- просмотр и контроль созданной конфигурации.

При конфигурировании оборудования Cisco следует иметь в виду, что в нем отсутствует заводская установка IP адреса по умолчанию, а вся конфигурация выполняется вручную с консоли через консольный порт устройства.

Ниже приведены примеры разработки сценариев (скриптов) для гипотетической локальной сети предприятия, схема которой показана на рисунке 8.7.

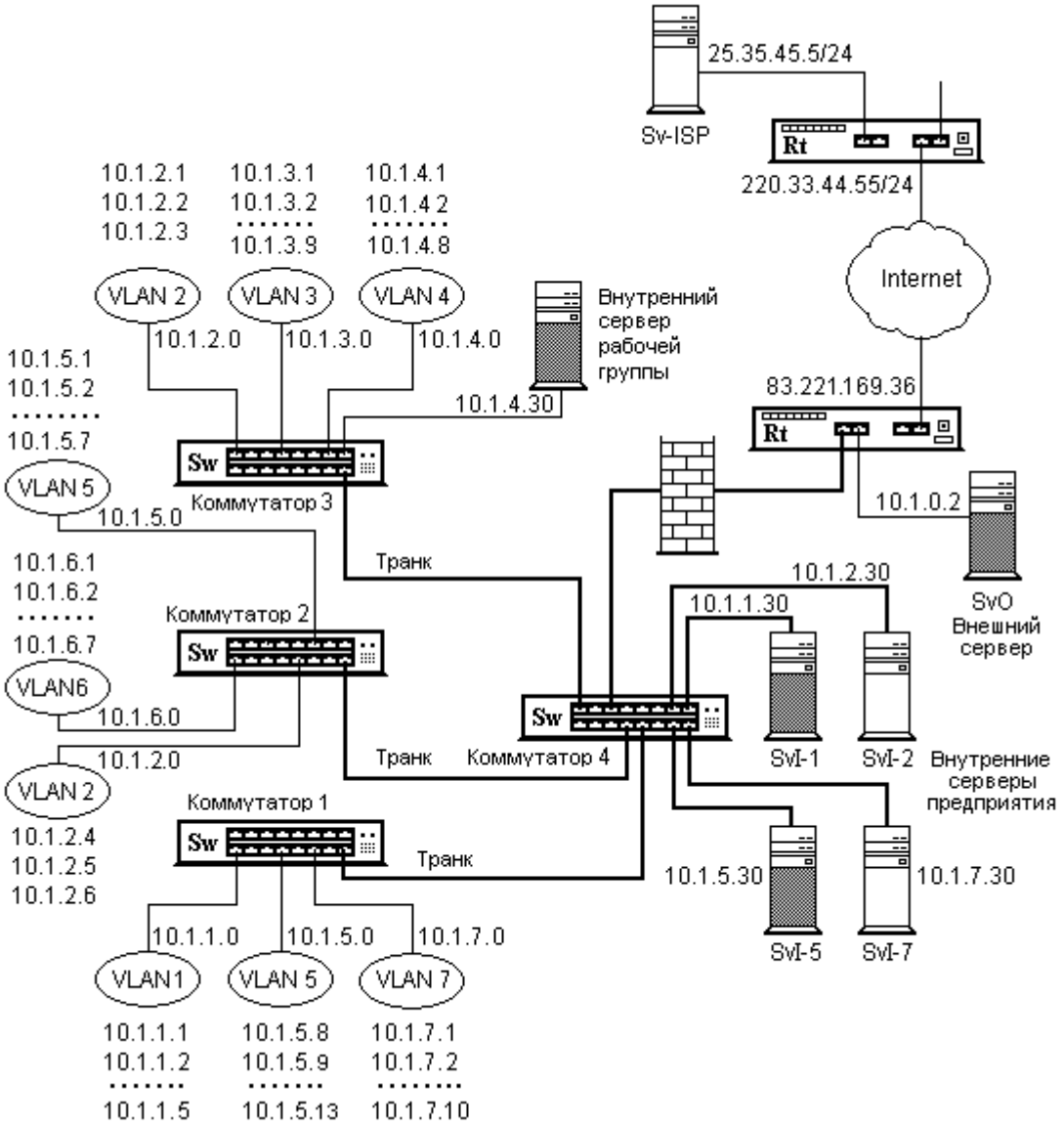


Рисунок 8.7 — Логическая схема сети с IP адресами

8.8.1. Сценарии конфигурации коммутаторов

Конфигурация коммутатора 4. Конфигурацию коммутаторов начнем с корневого устройства, с которым непосредственно связаны все остальные коммутаторы сети. Пусть все коммутаторы сети — устройства типа Cisco Catalyst 2950-24, содержащие 24 интерфейса (порта) FastEthernet. К коммутатору 4 посредством магистральных каналов (транков) подключены коммутаторы 1-3, а к портам FastEthernet подсоединены четыре внутренние серверы рабочих групп и сетевой маршрутизатор. Предположим, что внутренние серверы подключаются к следующим портам коммутатора: SvI-1 – Fa0/4; SvI-2 – Fa0/5; SvI-5 – Fa0/6; SvI-7 – Fa0/7. Первый коммутатор соединяется с корневым через магистральный порт Fa0/11, второй — через магистральный порт Fa0/12, третий — через магистральный порт Fa0/13, а соединение коммутатора 4 с маршрутизатором осуществляется через магистральный порт Fa0/24.

Сценарий конфигурации данного коммутатора состоит из следующих команд.

```
!-- Вход в привилегированный режим конфигурации.
Switch>enable
Switch#
!-- Задание пароля для входа в привилегированный режим.
Switch# configure terminal
Switch(config)#enable password <Пароль привилегированного режима>
!-- Установка пароля для входа по telnet по линиям 0…4.
Switch(config)# line vty 0 4
Switch(config-line)#password <Пароль для telnet>
                                    !--
!-- Разрешение входа по telnet.
Switch(config-line)# login
Switch(config)# exit
!-- Шифрование паролей, чтобы они не показывались в открытом виде.
Switch(config)# service password-encryption
!-- Сохранение (при необходимости) текущей конфигурации.
Switch#copy running-config startup-config
!--
!-- Стирание (в случае необходимости) текущей стартовой
!-- конфигурации.
Switch#erase startup-config
!-- Вход в режим глобального конфигурирования.
Switch#configure terminal
Switch(config)#
```

```
!--
!-- Присвоение имени Cat2950-4 конфигурируемому устройству.
Switch(config)#hostname Cat2950-4
Cat2950-4(config)#
!-- Присвоение IP-адреса для управления коммутатором.
Cat2950-4(config)# interface vlan 1
Cat2950-4(config-if)# ip address 10.1.0.4  255.255.255.0
!-- Ввод команды exit, чтобы изменения были приняты.
Cat2950-4(config-if)# exit
Cat2950-4(config)#
!--
!-- Создание виртуальных сетей.
!-- Переход в привилегированный режим.
Cat2950-4(config)# exit
Cat2950-4#
!-- Вход в базу данных VLAN для конфигурации виртуальных сетей.
Cat2950-4# vlan database

!-- Для облегчения задач администрирования сети применим VTP.
!-- Объявление домена, на который распространяется действие  VTP.
Cat2950-4(vlan)# vtp domain Victoria
!-- Задание коммутатору режима "Сервер".
Cat2950-4(vlan)# vtp server
!-- Если коммутатор уже находится в режиме "сервер" и нужно, чтобы
!-- он оставался в этом режиме, эту команду можно опустить.
!-- Создание на коммутаторе-сервере всех VLAN, имеющихся в данной
!-- сети
!-- Первая виртуальная сеть уже имеется по умолчанию. Первоначально
!-- в нее входят все (Fa0/0…Fa0/24) интерфейсы коммутатора.

!-- Создание второй виртуальной сети.
Cat2950-4(vlan)#vlan 2

!-- Аналогично задаются остальные сети.
!-- ..................
Cat2950-4(vlan)#vlan 7
Cat2950-4(vlan)#exit
Cat2950-4#
!--
!-- Задание имен сетям (при желании).
Cat2950-4# conf t
Cat2950-4(config)#vlan 2 name buchgalteria
!-- ..................................
!--
```

!-- Включение в VLAN 1 порта fa0/4 (сервера первой рабочей группы).
```
Cat2950-4(config)# interface fa0/4
```
!--
!-- Задание порту режима коммутации (работы на канальном уровне).
```
Cat2950-4(config-if)# switchport mode access
```

!-- Включение в VLAN 2 порта fa0/5 (сервера второй рабочей группы) и
!-- задание порту режима коммутации (работы на канальном уровне).
```
Cat2950-4(config)# interface fa0/4
Cat2950-4(config-if)# switchport access vlan 2
```

!-- Аналогично включаются серверы 5-й и 7-й рабочих групп в соответствующие
!-- виртуальные сети VLAN 5 и VLAN 7.

!-- Ввод команды exit для сохранения изменений.
```
Cat2950-4(config-if)# exit
Cat2950-4(config)#
```

!-- Перевод портов FastEthernet 0/11, 0/12, 0/13 и 0/24 на коммутаторе 4 в
!-- режим trunk. Конфигурация порта 0/11.
```
Cat2950-4(config)#interface FastEthernet0/11
```

!-- Задание режима инкапсуляции по протоколу 802.1Q
```
Cat2950-4(config-if)#switchport trunk encapsulation dot1q
```

!-- Задание магистрального режима
```
Cat2950-4(config-if)#switchport mode trunk
```

!-- Разрешение передачи кадров для всех VLAN по магистрали
```
Cat2950-4(config-if)#switchport trunk allowed vlan all
Cat2950-4(config-if)#exit
!--   - - - - - - - - - - - - - - - - - - - - - - - -
Cat2950-4(config)#interface FastEthernet0/24
Cat2950-4(config-if)#switchport trunk encapsulation dot1q
Cat2950-4(config-if)#switchport mode trunk
Cat2950-4(config-if)#switchport trunk allowed vlan all
Cat2950-4(config-if)#exit
Cat2950-4(config)#
```

!-- Контроль созданных VLAN и принадлежности портов
```
Cat2950-4(config)# exit
Cat2950-4# show vlan
```

Затем следует определить IP-адреса, которые нужно назначить на VLAN интерфейс, чтобы маршрутизатор был способен выполнять маршрутизацию между VLAN. Когда маршрутизатор принимает пакет, предназначенный для другой сети (VLAN), он просматривает свою таблицу маршрутизации чтобы определить, куда переслать пакет. В результате пакет передается на нужный VLAN интерфейс. Последний в свою очередь посылает пакет на тот порт, к которому подсоединен целевая рабочая станция. В качестве адреса для всех VLAN выберем адрес соответствующей виртуальной сети с номером в поле хоста равным 100.

```
!-- Конфигурируем VLAN интерфейсы IP-адресами, определенными в
!-- предыдущем пункте.
 !--
Cat2950-4#configure terminal
Cat2950-4(config)#interface vlan 2
Cat2950-4(config-if)#ip address 10.1.2.100 255.255.255.0
Cat2950-4(config-if)#no shutdown
Cat2950-4(config)#interface vlan 5
Cat2950-4(config-if)#ip address 10.1.5.100 255.255.255.0
Cat2950-4(config-if)#no shutdown
```

Этот процесс нужно повторить для всех VLAN, которые используются в маршрутизации.

Конфигурация коммутатора 1. К коммутатору 1 подключаются компьютеры трех виртуальных сетей: VLAN 1, VLAN 5 и VLAN 7. Подключение осуществляется через интерфейсы FastEthernet (fa), работающим в режиме доступа на канальном уровне. Виртуальной сети VLAN 1 выделим интерфейсы fa0/1…fa0/5, сети VLAN 5 — интерфейсы fa0/6…fa0/11, а сети VLAN 7 — fa0/12…fa0/21. Интерфейс fa0/24 настраивается на магистральный (транковый) режим.

Сценарий конфигурации первого коммутатора состоит из следующих команд.

```
!--
!-- Вход в привилегированный режим конфигурации.
Switch>enable
Switch#
!-- Задание пароля для входа в привилегированный режим.
Switch# configure terminal
Switch(config)# enable password <Пароль привилегированного режима>
!-- Установка пароля для входа по telnet.
Switch(config)# line vty 0 4
Switch(config-line)#password <Пароль для telnet>
!-- Разрешение входа по telnet.
```

```
Switch(config-line)# login
Switch(config)# exit
```
!-- Шифрование паролей чтобы они не показывались в открытом виде.
```
Switch(config)# service password-encryption
```
!-- Сохранение (при необходимости) текущей конфигурации.
```
Switch#copy running-config startup-config
```
!-- Вход в режим глобального конфигурирования.
```
Switch#configure terminal
Switch(config)#
```
!-- Присвоение имени Cat2950-1 конфигурируемому устройству.
```
Switch(config)#hostname Cat2950-1
Cat2950-1(config)#
```
!--
!-- Задание режима работы с VTP протоколом.
!-- Переход в привилегированный режим.
```
Cat2950-1(config)# exit
Cat2950-1#
```
!-- Вход в базу данных VLAN.
```
Cat2950-1# vlan database
```
!-- Включение коммутатора в домен, на который распространяется
!-- действие VTP протокола.
```
Cat2950(vlan)# vtp domain Victoria
```
!-- Задание коммутатору режима "Клиент".
```
Cat2950-1(vlan)# vtp client
Cat2950-1(vlan)#exit
```
!-- Контроль статуса коммутатора.
```
Cat2950-1#show vtp status
```
!-- Конфигурация магистрального интерфейса.
```
Cat2950-1#conf t
Cat2950-1(config)#int fa0/24
Cat2950-1(config-if)#switchport trunk encapsulation dot1q
Cat2950-1(config-if)#switchport mode trunk
Cat2950-1(config-if)#switchport trunk allowed vlan 1-7
Cat2950-1(config-if)#exit
Cat2950-1(config)#exit
```
!-- Проверка того, что информация о виртуальных сетях, созданных на сервере,
!-- распространилась на коммутатор-клиент.
```
Cat2950-1#schow vlan
```
!-- Включение в VLAN 5 группы портов с 6-го по 11-й.
```
Cat2950-1(config)# interface range FastEthernet 0/6 – 11
```
!-- Задание портам режима коммутации (работы на канальном уровне).
```
Cat2950-1(config-if)# switchport mode access
```

```
!-- Включение портов в виртуальную сеть VLAN 5.
Cat2950-1(config-if)# switchport access vlan5
!-- Включение поддержки алгоритма STP.
Cat2950-1(config-if)#spanning-tree port FastEthernet
!--
!-- Включение в VLAN 7 диапазона портов с 12-го по 21-й.
Cat2950-1(config)# interface range FastEthernet 0/12 - 21
!-- Задание портам режима коммутации.
Cat2950-1(config-if)# switchport mode access
!--
!-- Включение портов в VLAN 7.
Cat2950-1(config-if)# switchport access vlan 7
!--
!-- Сохранение настроек и переход в режим глобальной конфигурации.
Cat2950-1(config-if)#exit
!-- Перевод порта FastEthernet0/24 на коммутаторе 1 в режим trunk..
Cat2950-1(config)#interface FastEthernet0/24
Cat2950-1(config-if)#switchport mode trunk
!-- Задание режима инкапсуляции 802.1Q.
Cat2950-1(config-if)#switchport trunk encapsulation dot1q
!-- Разрешение передачи кадров для всех VLAN по магистрали.
Cat2950-1(config-if)#switchport trunk allowed vlan all
Cat2950-1(config-if)#exit
!--
```

Конфигурация коммутаторов 2 и 3. Процедура конфигурации обоих коммутаторов выполняется аналогично предыдущей. Как следует из логической схемы сети предприятия (рисунок 2.5) к коммутатору 2 подключаются компьютеры виртуальных сетей VLAN 2, 5 и 6. Интерфейс fa0/24 конфигурируется в режиме магистрального.

К коммутатору 3 подключаются компьютеры виртуальных сетей VLAN 2, 3 и 4. Кроме этого, в состав VLAN 4 входит внутренний сервер рабочей группы. Интерфейс fa0/24 конфигурируются в режиме магистрального.

В пояснительной записке необходимо привести полные тексты сценариев конфигурации всех телекоммуникационных устройств.

Правильность создания и конфигурации коммутаторов осуществляется путем задания следующих команд:

```
show vlan;
show vtp status;
show interface;
show running-config
```

8.8.2. Сценарий конфигурации маршрутизатора сети

Для проектируемой сети выбран маршрутизатор типа Cisco 2621 с IOS 12.4. В данном маршрутизаторе имеется два последовательных внешних интерфейса (WAN) Serial0/0 и Serial0/1, один из которых используем для подключения к Интернет-провайдеру, а также два внутренних порта FastEthernet 0/1 и 0/2. К внутренним портам подключаются корневой коммутатор 4 локальной сети и внешний сервер предприятия SvO.

!-- Перевод маршрутизатора в привилегированный режим EXEC.

```
Router> enable
Router#
```

!-- Вход в режим глобального конфигурирования.

```
Router#configure terminal
Router(config)#
```

!-- Установка пароля входа через виртуальный терминал.

```
Router(config)#line console 0
Router(config)#password [наш пароль]
```

!-- Вход в режим консоли.

```
Router(config)#login
Router(config)#exit
Router#wr mem
```

!-- Присвоение имени Cisco2621 конфигурируемому маршрутизатору.

```
Router(config)#hostname Cisco2621
Cisco2621(config)#
```

!-- Установка пароля входа через Telnet.

!-- Задание числа разрешенных сессий равное 5-ти (с 0-й по 4-ю).

```
Cisco2621(config)#line vty 0 4
Cisco2621(config)#password [наш пароль]
Cisco2621(config)#login
```

!-- Разрешение функционирования SNMP, для возможности получения
!-- статистики.

```
Cisco2621(config)#snmp-server community community_name RO
```

!-- Установка выданного провайдером глобального IP-адреса.

```
Cisco2621(config)#interface Serial0/1
Cisco2621(config-if)#ip address 83.221.169.36  255.255.255.0
```

!-- Установка IP-адреса интерфейса маршрутизатора в локальной сети

```
!-- (он же шлюз по умолчанию).
Cisco2621(config)# interface FastEthernet0/0
Cisco2621(config-if)# ip address 10.1.0.254  255.255.255.0
!-- Конфигурация внутреннего интерфейса FastEthernet0/0, к которому
!-- подключена вся сеть организации
Cisco2621(config)#interface FastEthernet0/0
Cisco2621(config-if)# no ip address
!--
!-- Включение интерфейса.
Cisco2621(config-if)#no shutdown
!--
!-- Сохранение конфигурации.

Cisco2621(config-if)#exit
!--
!-- Создание подинтерфейса и настройка магистрали.
Cisco2621(config)#interface FastEthernet0/0.1
!--
!-- Задание режима инкапсуляции 802.1Q.

Cisco2621(config-subif)#encapsulation dot1Q 1 native
!--
!-- Присвоение подинтерфейсу fa0/0.1  IP адреса.

Cisco2621(config-subif)#ip address 10.1.1.20  255.255.255.0
Cisco2621(config-subif)# no shutdown
Cisco2621(config-subif)#exit
!--
!-- Выполнение аналогичных операции для настройки магистралей
!-- на подинтерфейсах fa0/0.2…fa0/0.7.
Cisco2621(config)#int fastEthernet 0/0.2
Cisco2621(config-subif)#encapsulation dot1Q 2
Cisco2621(config-subif)#ip address 10.1.2.20  255.255.255.0
Cisco2621(config-subif)# no shutdown
Cisco2621(config-subif)#exit
!-- . . . . . .
Cisco2621(config)#int fastEthernet 0/0.7
Cisco2621(config-subif)#encapsulation dot1Q 7
Cisco2621(config-subif)#ip address 10.1.7.20 255.255.255.0
Cisco2621(config-subif)# no shutdown
Cisco2621(config-subif)#exit
!--
!-- Контроль состояния интерфейсов
```

```
Cisco2621#show int
!--
!-- Конфигурация интерфейса для подключения внешнего сервера
!-- Задание адреса интерфейсу внешнего сервера
Cisco2621#conf t
Cisco2621(config)#int fa0/1
Cisco2621(config-if)#ip address 10.1.0.254  255.255.255.0
!--
!-- Включение интерфейса
Cisco2621(config-if)#no shutdown
Cisco2621(config-if)#exit
Cisco2621(config)#exit
Cisco2621#
!--
!-- Конфигурация внешнего последовательного интерфейса
Cisco2621#conf t
Cisco2621(config)#int s0
!--
!-- Задание глобального IP-адреса и включение интерфейса
Cisco2621(config-if)#ip address 83.221.169.36 255.255.255.0
Cisco2621(config-if)#no shutdown
Cisco2621(config-if)#exit
Cisco2621(config)#exit
!--
!-- Задание тактовой частоты устройству с кабельным окончанием DCE
Cisco2621#conf t
Cisco2621(config)#int s0
Cisco2621(config-if)#clock rate 1000000
Cisco2621(config-if)#end
Cisco2621#
```

8.8.3. Конфигурирование списков доступа

Предположим, что политикой доступа в сети данной организации определено, что пользователям сети запрещается доступ к компьютерам рабочей группы дирекции организации (директор, главный инженер, главный бухгалтер и др.), кроме персонала группы технической поддержки (администратор сети, инженеры). Согласно распределению адресов между рабочими группами, компьютеры рабочей группы дирекции входят в виртуальную сеть с адресом 10.1.2.0/24, а виртуальная сеть рабочей группы технической поддержки имеет адрес 10.1.1.0/24.

Кроме этого, политикой безопасности установлено, что к внешнему серверу организации имеет право доступа клиенты всех рабочих групп, за исключением седьмой.

Реализация данной политики доступа осуществляется путем конфигурации на маршрутизаторе списков доступа.

```
!-- Запрет доступа к компьютерам группы управления (сеть 10.1.2.0),
!-- кроме персонала группы технической поддержки (сеть 10.1.1.0)
!--
!-- Задание расширенного списка доступа
Cisco2621#conf t
!--
!-- Разрешение доступа с виртуальной сети группы поддержки
Cisco2621(config)#access-list 102 permit ip 10.1.1.0 0.0.0.255 10.1.2.0 0.0.0.255
!--
!-- Неявный запрет для всех остальных пользователей
!--
!-- Привязка списка доступа к подинтерфейсу vlan 2
Cisco2621(config)#int fa0/0.2
Cisco2621(config-subif)#ip access-group 102 out
Cisco2621(config-subif)#exit
!--
!-- Запрет доступа к внешнему серверу пользователей 7-й рабочей группы
!-- (10.1.7.0), всем остальным пользователям сети организации доступ разрешен
!--
Cisco2621(config)#access-list 101 permit tcp any any
Cisco2621(config)#int fa0/1
Cisco2621(config-if)#ip access-group 101 out
Cisco2621(config-if)#exit
Cisco2621(config)#int fa0/1
Cisco2621(config-if)#no ip access-group 101 out
Cisco2621(config-if)#no access-list 101 permit tcp any any
Cisco2621(config)#no access-list 101 deny tcp 10.1.7.0 0.0.0.255 10.1.0.2 0.0.0.0
Cisco2621(config)#exit

!-- Контроль созданного списка доступа
Cisco2621#show access-list
```

Пусть пользоваться Интернетом разрешается сотрудникам, которые находятся в сетях 10.1.5.0 и 10.1.7.0, только в рабочие дни во время перерыва на обед, начало действия данного правила — с 1 июня 2015 г, окончание —

не определено. При этом разрешается прохождение только TCP-пакетов, содержащие данные протокола HTTP.

Сотрудникам сети 10.1.2.0 выход в Интернет разрешается в рабочие дни с 7:00 до 22:00 и в выходные дни с 9:00 до 15:00.

В сети 10.1.6.0 установлен сервер с адресом 10.1.6.30, доступ к которому разрешен только для пользователей этой сети по рабочим дням с 8:00 до 17:00. Данное правило должно вступить в действие сразу и закончиться к концу года.

Для защиты от атак типа DDoS предусмотреть закрытие любого TCP-сеанса, если он не установлен в течение 30 с.

Сценарий конфигурации маршрутизатора для указанных условий имеет следующий вид.

```
Cisco2621#conf t
Cisco2621(config)#ip access-list 101 permit tcp any any eq 80 time-range
allow-http
!-- Разрешение прохождения TCP пакетов, содержащих данные
!-- протокола HTTP, во всех направлениях.
Cisco2621(config)#interface FastEthernet0/0
  ip access-group 101 in
  time-range allow-http
  absolute start 00:01 1 June 2015
  periodic weekdays 13:00 to 14:00

!-- Назначение списка доступа интерфейсу FastEthernet0/0. Приведем пример
конфигурации такого списка доступа:

interface FastEthernet0/0
  ip access-group 102 in
  time-range http-ok
  absolute end 24:00 31 December 2015
  periodic weekdays 08:00 to 17:00
!
ip access-list 102 permit tcp any host 140.11.12.10 eq 80 time-range http-
ok
!-- Закрытие любого TCP-сеанса, не установленного в течение 30 секунд
!-- для защиты от flood-атаки SYN с отказом в обслуживании.
ip tcp synwait-time 30
```

8.8.4. Конфигурирование процедур трансляции адресов

Выбранный маршрутизатор типа Cisco2621 содержит два порта для подключения локальных сетей (FastEthernet0/0 и FastEthernet0/1) и один последовательный порт s0 для подключения к глобальной сети провайдера

Интернет-услуг. Пусть данной организации выделен один глобальный (публичный) IP-адрес (83.221.169.36/24) для внешнего сервера, а также группа глобальных IP-адресов в диапазоне 83.221.169.37 – 83.221.169.40. Для преобразования частного адреса внешнего сервера в глобальный адрес маршрутизатор должен выполнять статическую трансляцию внутреннего адреса 10.1.0.30 сервера во внешний глобальный адрес 83.221.169.36/24. Предположим, что на маршрутизаторе используется протокол маршрутизации RIP.

```
!-- Задание протокола маршрутизации
!--
Cisco2621#conf t
Cisco2621(config)#Cisco2621 rip
!--
!-- Указания адреса смежной сети
Cisco2621(config-Cisco2621)#network 83.221.169.0
Cisco2621(config-if)#exit
Cisco2621(config)#exit
!--
Cisco2621> enable
Cisco2621# configure terminal
Cisco2621 (config)# interface fastethernet 0/0
!--
!-- Указание на внутренний интерфейс
Cisco2621 (config-if)# ip nat inside
Cisco2621 (config-if)# exit
Cisco2621 (config)# interface serial0
!--
!-- Задание последовательного порта в качестве внешнего интерфейса
Cisco2621 (config-if)# ip nat outside
Cisco2621 (config-if)# exit
!--
!--  Задание соответствия локального адреса и глобального
Cisco2621 (config)# ip nat inside source static 10.1.0.2  83.221.169.36
Cisco2621 (config)# exit
!--
!-- Проверка правильности трансляции адреса осуществляется командой
Cisco2621#show ip nat translations
!--
!--
!-- Конфигурация процедуры динамического преобразования адресов
!--
Cisco2621#conf t
!--
!--Задание пула адресов
```

```
Cisco2621(config)#ip nat pool 7 83.221.169.37 83.221.169.40 netmask
255.255.255.0
!--
!-- Указание на преобразование адресов из списка 17 в пул адресов 7
Cisco2621(config)#ip nat inside source list 17 pool 7
!-- Создание списка доступа с номером 17, определяющим компьютеры,
!-- для которых разрешается выполнять трансляцию для внутренних адресов
Cisco2621(config)#access-list 17 permit 10.1.0.0 0.0.255.255
!--
!-- Задание последовательного порта в качестве внешнего интерфейса
Cisco2621(config)#int s0
Cisco2621(config-if)#ip nat outside
Cisco2621(config-if)#exit
!--
!-- Указание на внутренний интерфейс
Cisco2621(config)#int fa0/0
Cisco2621(config-if)#ip nat inside
Cisco2621(config)#exit
!--
!-- Проверка правильности восприятия команд маршрутизатором
Cisco2621#show ip nat tr
Cisco2621 #Show access-list
```

Для сохранения созданной конфигурации маршрутизатора необходимо применить команду

```
Cisco2621# copy running-config startup-config
```

9. Компьютерное моделирование функционирования сети

9.1. Цели, задачи и особенности моделирования сети

Целью моделирования является проверка функционирования спроектированной компьютерной сети предприятия в соответствии с техническим заданиев и корректности разработанных сценариев конфигурирования телекоммуникационного оборудования.

В процессе достижения поставленной цели должны быть решены следующие задачи:

- создания топологии спроектированной сети или ее фрагмента;
- назначение портов телекоммуникационного оборудования для подключения рабочих станций и серверов;
- соединение рабочих станций и серверов сети с портами соответствующего телекоммуникационного оборудования, а также телекоммуникационного оборудования между собой;
- создание виртуальных локальных сетей (Vlan) рабочих групп;
- задание IP-адресов и сетевых масок рабочим станциям и серверам;
- конфигурация коммутаторов и маршрутизатора;
- проверка доступности рабочих станций сети и степени изолированности виртуальных сетей;
- коррекция схемы сети и сценариев конфигурации (в случае необходимости) по результатам проверки функционирования спроектированной сети.

Особенность моделирования состоит в том, что в курсовом проекте, в случае громозкости схемы спроектированной сети, по согласованию с руководителем проекта, осуществляется моделирование не всей сети, а ее базового фрагмента, в котором содержатся все принципиальные составные части спроектированной сети. Моделирование сети осуществляется в среде сетевого эмулятора Packet Tracer 6.0 или среде Boson версии 7.0 и выше [7]. Для моделирования также возможно использование эмуляторов других типов, в частности OPNET или NetCracker Professional, .

В процессе моделирования вначале составляется упрощенная схема исследуемой сети. В создаваемую схему включаются те типы коммуникационных устройств, которые входят в спецификацию спроектированной сети. В случае отсутствия данного типа устройств в базе данных используемого эмулятора, по согласованию с руководителем проекта, разрешается включать в моделируемую схему коммуникационные устройства, которые по своим свойствам близки к отсутствующим образцам.

После создания топологии сети выполняется конфигурация интерфейсов коммуникационных устройств, формируются виртуальные сети, задаются сетевые адреса, инициируется процедура трансляции адресов и конфигурируются списки доступа. Затем выполняется тестирование сети путем пингования рабочих станций, серверов, просмотра и анализа трасс маршрутизации. Конфигурация сети осуществляется на основе параметров, полученных в процессе выполнения этапов ее проектирования, освещенных в подразделах 9.3-9.7 данного пособия.

Ниже рассматривается пример моделирования компьютерной сети, топология и параметры которой изображены на рисунке 9.1. Для упрощения процедуры моделирования схема сети, исходная схема упрощается, в частности, уменьшается количество виртуальных сетей и количество рабочих станций в них (рисунок 9.2).

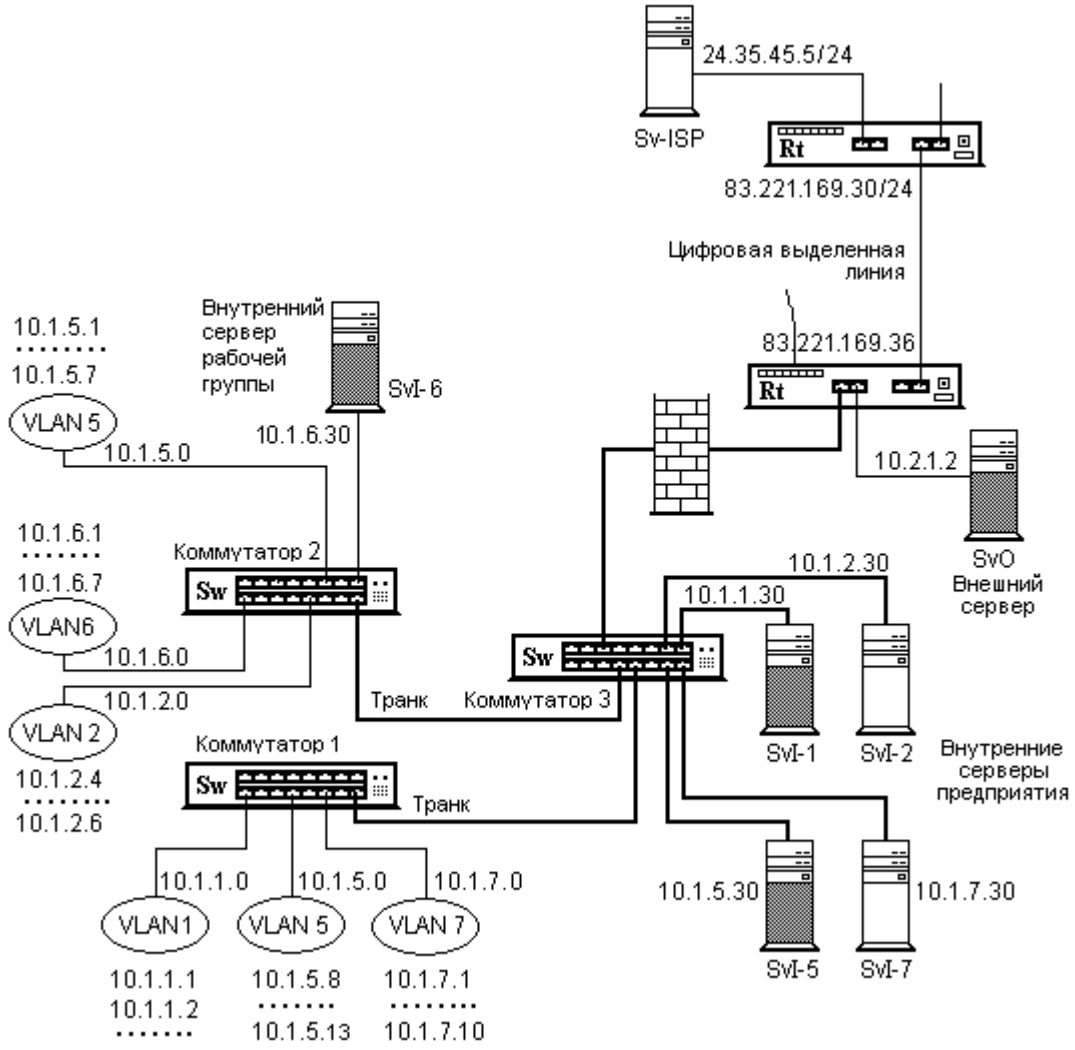


Рисунок 9.1 — Моделируемый фрагмент сети

Такое упрощение позволяет оценить работоспособность сети в целом, соответствие ее параметров техническому заданию и корректность конфигу-

рации устройств, так как отсутствующие элементы имеют аналогичные связи между компонентами сети и сценарии конфигурации с моделируемыми фрагментами сети.

Данный фрагмент включает компьютеры пяти подсетей рабочих групп, каждая из которых представляет собой виртуальную локальную сеть (соответственно VLAN1, VLAN2, VLAN5, VLAN6 и VLAN7), логически отделенную от подсетей других рабочих групп. Кроме рабочих станций в сети имеется сервер рабочей группы, входящий в пятую подсеть и внешний сервер предприятия.

9.2. Создание топологии сети в системе Packet Tracer

Для создания топологии моделируемой сети запускается Network Designer и в меню File выбирается New. При этом открывается новое рабочее окно дизайнера сети. Топология сети создается путем выбора из списка оборудования “Devices and Connectors” маршрутизатора соответствующего типа, нужных типов коммутаторов и рабочих станций и размещения их путем перетягивания с помощью мышки в рабочем поле окна конструктора. Затем распределются порты коммутаторов по локальным сетям и осуществляется соединение рабочих станций с соответствующими портами коммутаторов, а также коммутаторов между собой и коммутатора с маршрутизатором. Вид созданной топологии сети изображен на рисунке 9.2.

Модель сети содержит два аналогичных 12-портовых сетевых коммутатора второго уровня типа Cisco Catalyst 2950 — Sw-1 и Sw-2. Все порты коммутаторов являются 100 мегабитовыми портами типа FastEthernet. В первый коммутатор включены по две рабочих станции 1-й, 5-й и 7-й виртуальных сетей. Обозначение рабочей станции содержит две буквы PC и два цифровых символа. Первый из них отражает номер виртуальной сети, а второй — номер станции в соответствующей сети. Внутренний сервер рабочей группы обозначается символами SvI, а внешний — SvO. Ко второму коммутатору Sw-2 подсоединены две станции сети VLAN2, две станции VLAN5 и сервер рабочей группы, входящий в эту же виртуальную сеть, а также две рабочих станции VLAN7.

В состав сети входит маршрутизатор типа Cisco-2621, располагающий двумя портами FastEthernet и одним последовательным портом S0. Последовательный порт через выделенную цифровую линию соединен с последовательным портом маршрутизатора провайдера сетевых услуг аналогичного типа. К порту FastEthernet маршрутизатора внешней сети подключен сервер провайдера Sv-ISP.

После создания топологии сети она сохраняется в файле топологии с произвольным именем и расширением *.top. На схеме топологии моделиру-

емой сети, для облегчения ее понимания, отмечены номера портов, через которые выполнено подключение рабочих станций, серверов, а также осуществляется связь коммуникационного оборудования между собой.

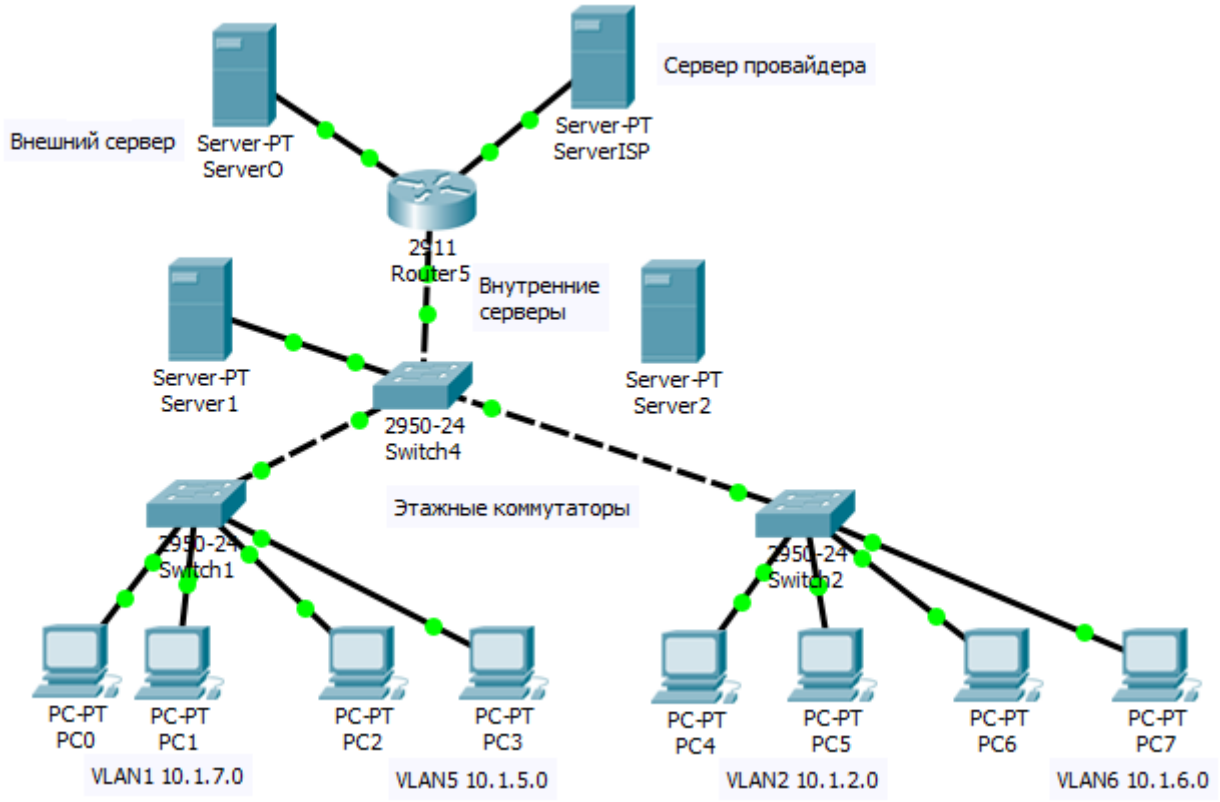


Рисунок 9.2 — Топология моделируемой компьютерной сети в окне Packet Tracer

Символы в обозначениях портов (fa0/1 и др.) отображают тип интерфейса (FastEthernet), номер модуля и номер порта в соответствующем модуле. Для обозначения последовательного порта маршрутизатора, служащего для соединения его с внешней сетью, используется символ S0.

9.3. Конфигурирование и моделирование функционирования локальной сети

Топология конфигурируемой сети изображена на рисунке 9.1. Для упрощения конфигурации и администрирования сети используем VTP режим. Конфигурация осуществляется поэтапно, начиная с создания виртуальных сетей. Для избегания ошибок периодически будет проводиться проверка созданной топологии путем использования команд show и контрольного пингования участков создаваемой сети. Конфигурацию начнем с корневого коммутатора Sw-3.

Конфигурация корневого коммутатора 3. В коммутаторе используется 4 порта в режиме доступа и три в магистральном (транковом) режиме.

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname Cat2650-3
Cat2650-3(config)#exit
Cat2650-3#vlan database
Cat2650-3(vlan)#vtp server

!-- Задание имени vtp домена
Cat2650-3(vlan)#vtp domain Victoria
Changing VTP domain from NULL to victoria
Cat2650-3(vlan)#exit
APPLY completed.
Exiting....
```

Проверка статуса коммутатора и режима работы.

```
Cat2650-3#show vtp status
```

VTP Version	: 2
Configuration Revision	: 2
Maximum VLANs supported locally	: 64
Number of existing VLANs	: 5
VTP Operating Mode	: Server
VTP Domain Name	: victoria
VTP Pruning Mode	: Disabled
VTP V2 Mode	: Disabled
VTP Traps Generation	: Disabled
MD5 digest	: 0xEE 0xB3 0xDC 0x9F 0xE2 0xE0 0x25 0xDF

Configuration last modified by 0.0.0.0 at 3-1-93 04:55:57
Local updater ID is 0.0.0.0 (no valid interface found)

Из представленного сообщения видно, что коммутатор находится в статусе сервера и входит в домен victoria

```
!--
!-- Создание VLAN-сетей на коммутаторе, которые имеются в
!--  спроектированной сети, с учетом того, что сеть VLAN1 существует
!--  по умолчанию и ей принадлежат все порты

Cat2650-3#vlan database
Cat2650-3(vlan)#vlan 2
VLAN 2 added:
```

```
    Name:VLAN0002
Cat2650-3(vlan)#vlan 5
VLAN 5 added:
    Name:VLAN0005
Cat2650-3(vlan)#vlan 6
VLAN 6 added:
    Name:VLAN0006
Cat2650-3(vlan)#vlan 7
VLAN 7 added:
    Name:VLAN0007
Cat2650-3(vlan)#exit
APPLY completed.
Exiting....
!--
```

!-- Контроль созданных виртуальных сетей

```
Cat2650-3#show vlan
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12
2	VLAN0002	active	
5	VLAN0005	active	
6	VLAN0006	active	
7	VLAN0007	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1
1	enet	100001	1500	-	-	-	-	-	0
7	enet	100007	1500	-	-	-	-	-	0
5	enet	100005	1500	-	-	-	-	-	0
2	enet	100002	1500	-	-	-	-	-	0
6	enet	100006	1500	-	-	-	-	-	0
1002	fddi	101002	1500	-	-	-	-	-	0
1003	tr	101003	1500	-	-	-	-	-	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0
1005	trnet	101005	1500	-	-	-	ibm	-	0

!-- Задание режимов и назначение портов коммутатора для VLAN

```
Cat2650-3#conf t
```

! -- Задание портов доступа

```
Cat2650-3(config)#int fa0/2
Cat2650-3(config-if)#switchport access vlan 2
```

```
Cat2650-3(config-if)#exit
Cat2650-3(config)#int fa0/5
Cat2650-3(config-if)#switchport access vlan 5
Cat2650-3(config-if)#exit
Cat2650-3(config)#int fa0/7
Cat2650-3(config-if)#switchport access vlan 7
Cat2650-3(config-if)#exit
```

!-- Проверка задания портов доступа виртуальным сетям

```
Cat2650-3#show vlan
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1,Fa0/3,Fa0/4,Fa0/6,Fa0/8, Fa0/9, Fa0/10, Fa0/11,Fa0/12
2	VLAN0002	active	Fa0/2
5	VLAN0005	active	Fa0/5
6	VLAN0006	active	
7	VLAN0007	active	Fa0/7
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1
1	enet	100001	1500	-	-	-	-	-	0
2	enet	100002	1500	-	-	-	-	-	0
5	enet	100005	1500	-	-	-	-	-	0
6	enet	100006	1500	-	-	-	-	-	0
7	enet	100007	1500	-	-	-	-	-	0
1002	fddi	101002	1500	-	-	-	-	-	0

Проверка показывает, что все виртуальные сети созданы, порты доступа по виртуальным сетям распределены верно.

!-- Задание магистральных портов

```
Cat2650-3#conf t
Cat2650-3(config)#int fa0/10
Cat2650-3(config-if)#switchport mode trunk
Cat2650-3(config-if)#exit

Cat2650-3(config)#int fa0/11
Cat2650-3(config-if)#switchport mode trunk
Cat2650-3(config-if)#exit
Cat2650-3(config)#int fa0/12
Cat2650-3(config-if)#switchport mode trunk
Cat2650-3(config-if)#exit
Cat2650-3(config)#exit
```

!-- Контроль состояния магистральных портов

```
Cat2650-3#show int trunk
```

Port	**Mode**	**Encapsulation**	**Status**	**Native vlan**
Fa0/10	on	802.1q	trunking	1
Port	Vlans allowed on trunk			
Fa0/10	1-4094			
Port	Vlans allowed and active in management domain			
Fa0/10	2,5,6,7			
Port	Vlans in spanning tree forwarding state and not pruned			
Fa0/10	2,5,6,7			

Port	**Mode**	**Encapsulation**	**Status**	**Native vlan**
Fa0/11	on	802.1q	trunking	1
Port	Vlans allowed on trunk			
Fa0/11	1-4094			
Port	Vlans allowed and active in management domain			
Fa0/11	2,5,6,7			
Port	Vlans in spanning tree forwarding state and not pruned			
Fa0/11	2,5,6,7			

Port	**Mode**	**Encapsulation**	**Status**	**Native vlan**
Fa0/12	on	802.1q	trunking	1
Port	Vlans allowed on trunk			
Fa0/12	1-4094			
Port	Vlans allowed and active in management domain			
Fa0/12	2,5,6,7			
Port	Vlans in spanning tree forwarding state and not pruned			
Fa0/12	2,5,6,7			

Из этого сообщения следует, что порты Fa0/10 - Fa0/12 находятся в транковом (магистральном) режиме и во включенном состоянии. Поддерживается протокол инкапсуляции 802.1q.

Конфигурация коммутатора 1

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname Cat2950-1
Cat2950-1(config)#exit
Cat2950-1#vlan database
Cat2950-1(vlan)#vtp client
Cat2950-1(vlan)#vtp domain Victoria
Changing VTP domain from NULL to victoria
Cat2950-1(vlan)#exit
```

```
APPLY completed.
Exiting....

Cat2950-1#show vtp status
```

VTP Version	:	2
Configuration Revision	:	2
Maximum VLANs supported locally	:	64
Number of existing VLANs	:	9
VTP Operating Mode	:	Client
VTP Domain Name	:	victoria
VTP Pruning Mode	:	Disabled
VTP V2 Mode	:	Disabled
VTP Traps Generation	:	Disabled
MD5 digest	:	0xEE 0xB3 0xDC 0x9F 0xE2 0xE0 0x25 0xDF

Configuration last modified by 0.0.0.0 at 3-1-93 04:55:57
Local updater ID is 0.0.0.0 (no valid interface found)

Из этого сообщения можно убедиться, что коммутатор переключился в клиентский режим и принадлежит домену victoria.

Продолжаем конфигурацию магистральных портов и портов доступа коммутатора. По окончании конфигурации осуществляем проверку правильности заданных предписаний.

```
Cat2950-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Cat2950-1(config)#int fa0/12
Cat2950-1(config-if)#switchport mode trunk
Cat2950-1(config-if)#exit
Cat2950-1(config)#int fa0/5
Cat2950-1(config-if)#switchport access vlan 5
Cat2950-1(config-if)#int fa0/6
Cat2950-1(config-if)#switchport access vlan 5
Cat2950-1(config-if)#exit
Cat2950-1(config)#int range fa0/7-8
Cat2950-1(config-if-range)#switchport access vlan 7
Cat2950-1(config-if-range)#end
Cat2950-1#show vlan
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/9, Fa0/10, Fa0/11, Fa0/12
2	VLAN0002	active	
5	VLAN0005	active	Fa0/5, Fa0/6
6	VLAN0006	active	
7	VLAN0007	active	Fa0/7, Fa0/8

1002	fddi-default	active
1003	token-ring-default	active
1004	fddinet-default	active
1005	trnet-default	active

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1
1	enet	100001	1500	-	-	-	-	-	0
2	enet	100002	1500	-	-	-	-	-	0
5	enet	100005	1500	-	-	-	-	-	0
6	enet	100006	1500	-	-	-	-	-	0
7	enet	100007	1500	-	-	-	-	-	0
1002	fddi	101002	1500	-	-	-	-	-	0
1003	tr	101003	1500	-	-	-	-	-	0

Контроль созданных виртуальных сетей показал, что все порты распределены по VLAN верно.

Конфигурация коммутатора 2. Конфигурация данного коммутатора выполняется аналогчно вышеизложенной процедуре.

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#hostname Cat2950-2
Cat2950-2(config)#exit
Cat2950-2#vlan database
Cat2950-2(vlan)#vtp client
Cat2950-2(vlan)#vtp domain Victoria
Changing VTP domain from NULL to victoria
Cat2950-2(vlan)#exit
APPLY completed.
Exiting....
Cat2950-2#show vtp status

Cat2950-2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Cat2950-2(config)#int fa0/12
Cat2950-2(config-if)#switchport mode trunk
Cat2950-2(config-if)#exit ^Z
%SYS-5-CONFIG_I: Configured from console by console

Cat2950-2#show vlan
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10,

			Fa0/11, Fa0/12
2	VLAN0002	active	
5	VLAN0005	active	
6	VLAN0006	active	
7	VLAN0007	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

Из таблицы видно, что в процессе реализации протокола VTP на коммутаторе активированы все виртуальные сети, объявленные на сервере.

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1
1	enet	100001	1500	-	-	-	-	-	0
5	enet	100005	1500	-	-	-	-	-	0
2	enet	100002	1500	-	-	-	-	-	0
6	enet	100006	1500	-	-	-	-	-	0
7	enet	100007	1500	-	-	-	-	-	0
1002	fddi	101002	1500	-	-	-	-	-	0
1003	tr	101003	1500	-	-	-	-	-	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0
1005	trnet	101005	1500	-	-	-	ibm	-	0

```
Cat2950-2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Cat2950-2(config)#int range fa0/2-3
Cat2950-2(config-if-range)#switchport access vlan 2
Cat2950-2(config-if-range)#exit
Cat2950-2(config)#int fa0/5
Cat2950-2(config-if)#switchport access vlan 5
Cat2950-2(config-if)#exit
Cat2950-2(config)#int range fa0/6-8
Cat2950-2(config-if-range)#switchport access vlan 6
Cat2950-2(config-if-range)#end
Cat2950-2#show vlan
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/4, Fa0/9, Fa0/10, Fa0/11, Fa0/12
2	VLAN0002	active	Fa0/2, Fa0/3
5	VLAN0005	active	Fa0/5
6	VLAN0006	active	Fa0/6, Fa0/7, Fa0/8
7	VLAN0007	active	
1002	fddi-default	active	
1003	token-ring-default	active	

```
1004    fddinet-default          active
1005    trnet-default            active
```

Контроль созданных виртуальных сетей показал, что все порты распределены по VLAN верно.

Конфигурация маршрутизатора локальной сети Rt-2621.

```
Router>
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Rt-2621
Rt-2621(config)#int fa0/0

!-- Включение интерфейса
Rt-2621(config-if)#no shutdown
%LINK-3-UPDOWN:Interface FastEthernet0/0,changed state to up

!– Конфигурация подинтерфейсов с заданием вида инкапсуляции и IP адресов
!– с целью обеспечения возможности взаимодействия между виртуальными
!– сетями на третьем уровне.
Rt-2621(config-if)#exit
Rt-2621(config)#int fa0/0.2
Rt-2621(config-subif)#encapsulation dot1q 2
Rt-2621(config-subif)#ip address 10.1.2.254 255.255.255.0
Rt-2621(config-subif)#exit
Rt-2621(config)#int fa0/0.5
Rt-2621(config-subif)#encapsulation dot1q 5
Rt-2621(config-subif)#ip address 10.1.5.254 255.255.255.0
Rt-2621(config-subif)#exit
Rt-2621(config)#int fa0/0.6
Rt-2621(config-subif)#encapsulation dot1q 6
Rt-2621(config-subif)#ip address 10.1.6.254 255.255.255.0
Rt-2621(config-subif)#exit
Rt-2621(config)#int fa0/0.7
Rt-2621(config-subif)#encapsulation dot1q 7
Rt-2621(config-subif)#ip address 10.1.7.254 255.255.255.0
Rt-2621(config-subif)#exit
Rt-2621(config)#exit

!-- Контроль состояния интерфейсов
Rt-2621#show int

!-- Задание адреса интерфейсу внешнего сервера
```

```
Rt-2621#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Rt-2621(config)#int fa0/1
Rt-2621(config-if)#ip address 10.1.0.254  255.255.255.0
Rt-2621(config-if)#no shutdown
%LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
Rt-2621(config-if)#exit
Rt-2621(config)#exit
Rt-2621#
```

!-- Конфигурация внешнего последовательного интерфейса

```
Rt-2621#conf t
Enter configuration commands, one per line.  End with
CNTL/Z.
Rt-2621(config)#int s0
```

!-- Задание публичного IP адреса и включение интерфейса

```
Rt-2621(config-if)#ip address 83.221.169.36 255.255.255.0
Rt-2621(config-if)#no shutdown
%LINK-3-UPDOWN: Interface Serial0, changed state to up
%LINK-3-UPDOWN: Interface Serial0, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0,
changed state to down
Rt-2621(config-if)#exit
Rt-2621(config)#exit
```

!-- Интерфейс переключился в состояние down потому, что не указана тактовая
!-- частота в звене данных DTE-DCE. Нужно определить, какая из сторон !--
является терминальной частью (DTE), а какая коммуникационной
!-- (DCE)? Для этого применяется команда

```
Rt-2621#show controllers s0
HD unit 0, idb = 0x1AE828, driver structure at 0x1B4BA0
buffer size 1524  HD unit 0,V.35 DTE cable
Rt-ISP#show contr s0
HD unit 0, idb = 0x1AE828, driver structure at 0x1B4BA0
buffer size 1524  HD unit 0,V.35 DCE cable
```

!– При установлении соединения точка-точка одно из устройств (DCE) должно
!– задавать тактовую частоту. Узнать допустимые значения этой частоты
!-- можно путем задания команды `clock rate ?`

```
Rt-ISP#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Rt-ISP(config)#int s0
```

```
Rt-ISP(config-if)#clock rate ?
500000
148000
1200
2400
4800
9600
1000000
. . . . .
1300000
2000000
4000000
```

!-- Задание тактовой частоты устройству с кабельным окончанием DCE

```
Rt-ISP(config-if)#clock rate 1000000
Rt-ISP(config-if)#end
Rt-ISP#
Rt-2621#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Rt-2621(config)#int fa0/1
Rt-2621(config-if)#ip  nat  inside  source  static  10.1.0.2
83.221.169.36
Rt-2621(config-if)#exit
```

!-- Задание процедуры трансляции адресов

```
Rt-2621(config)#int s0
Rt-2621(config-if)#ip nat outside
Rt-2621(config-if)#exit
Rt-2621(config)#exit
```

!-- Контроль таблицы трансляции адреса

```
Rt-2621#show ip nat translation
```

Pro	Inside global	Inside local	Outside local	Outside global
---	83.221.169.36	10.1.0.2	---	---

Проверка трансляции свидетельствует, что преобразование адресов осуществляется верно.

Конфигурация маршрутизатора Интернет-провайдера

```
Rt-ISP#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Rt-ISP(config)#router rip
Rt-ISP(config-router)#network 25.35.45.0
```

```
Rt-ISP(config-router)#network 83.221.169.0
Rt-ISP(config-router)#exit

Rt-2621#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Rt-2621(config)#router rip
Rt-2621(config-router)#network 83.221.169.0
Rt-2621(config-if)#exit
Rt-2621(config)#exit

Rt-2621#ping 83.221.169.30
```

Конфигурация списков доступа на машрутизаторе Rt-2621

```
Rt-2621(config)#ip nat inside source list1 int fa0/0 overload ?
Rt-2621(config)#ip nat inside source list 1 interface s0 overload ?
Rt-2621(config)#int s0
Rt-2621(config-if)#ip nat outside
Rt-2621(config-if)#exit
Rt-2621(config)#int fa0/0
Rt-2621(config-if)#ip nat inside
Rt-2621(config-if)#exit
Rt-2621(config)#access-list 1 permit 10.1.1.0 0.0.0.255
Rt-2621(config)#exit
!
```

!-- Проверяем созданные vlan и связанные с ними порты коммутатора

```
Sw-1#show vlan
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/9, Fa0/10, Fa0/11, Fa0/12
2	VLAN0002	active	
5	VLAN0005	active	Fa0/5, Fa0/6
6	VLAN0006	active	
7	VLAN0007	active	Fa0/7, Fa0/8
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1
1	enet	100001	1500	-	-	-	-	-	0
7	enet	100007	1500	-	-	-	-	-	0
5	enet	100005	1500	-	-	-	-	-	0
2	enet	100002	1500	-	-	-	-	-	0

6	enet	100006	1500	-	-	-	-	-	0
1002	fddi	101002	1500	-	-	-	-	-	0
1003	tr	101003	1500	-	-	-	-	-	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0
1005	trnet	101005	1500	-	-	-	ibm	-	0

Открываем в эмуляторе окно eStations и выбираем рабочую станцию PC1-1. Присвоим IP–адрес и сетевую маску станции, а также адрес шлюза по умолчанию.

```
Press Enter to begin
C:>
C:>ipconfig /ip 10.1.1.1 255.255.255.0
C:>ipconfig /dg 10.1.1.11
!
! Просмотр созданной конфигурации
!
C:>ipconfig
    Ethernet adapter Local Area Connection:
        IP Address. . . . . . . . . : 10.1.1.1
        Subnet Mask . . . . . . . . : 255.255.255.0
        Default Gateway…. . . . . . : 10.1.1.11
```

Аналогичным образом конфигурируем все рабочие станции, включенные в данный коммутатор.

Проверим возможность связи рабочих станций внутри виртуальных сетей, а также логическую изоляцию виртуальных сетей. Для этого воспользуемся процедурой пингования рабочих станций. Пропингуем с PC1-2 рабочие станции PC1-1, PC5-5 и PC7-2. В среде эмулятора это выглядит следующим образом:

```
C:>ping 10.1.1.1
Pinging 10.1.1.1 with 32 bytes of data:

Reply from 10.1.1.1: bytes=32 time=60ms TTL=241
Reply from 10.1.1.1: bytes=32 time=60ms TTL=241
Reply from 10.1.1.1: bytes=32 time=60ms TTL=241
Reply from 10.1.1.1: bytes=32 time=60ms TTL=241
Reply from 10.1.1.1: bytes=32 time=60ms TTL=241

Ping statistics for 10.1.1.1: Packets: Sent =5,
Received =5, Lost =0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 50 ms, Maximum = 60 ms, Average = 55 ms

C:>ping 10.1.5.5
Pinging 10.1.5.5 with 32 bytes of data:

Request timed out.
```

```
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 10.1.5.5:
Packets: Sent = 5, Received = 0, Lost = 5 (100% loss),
Approximate round trip times in milli-seconds:
Minimum = 0 ms, Maximum = 0 ms, Average = 0 ms

C:>ping 10.1.7.2
Pinging 10.1.7.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.1.7.2:
Packets: Sent = 5, Received = 0, Lost = 5 (100% loss),
Approximate round trip times in milli-seconds:
     Minimum = 0 ms, Maximum = 0 ms, Average = 0 ms.
```

Аналогичные действия выполняем для всех рабочих станций виртуальных сетей, включенных в коммутатор.

На основании проведенных исследований можно сделать вывод, что связь между компьютерами внутри виртуальных сетей существует, а передать пакеты в станции других vlan не возможно, так как они логически изолированы друг от друга.

Если же тестовые пакеты проходят в другие vlan, то необходимо еще раз проверить правильность назначения портов в виртуальные сети и, при наличии ошибки, скорректировать конфигурацию. Далее выполняем конфигурацию маршрутизатора.

Выполним конфигурацию маршрутизатора для обеспечения взаимодействия на сетевом уровне между виртуальными сетями

```
Router>
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int fa0/0
Router(config-if)#no shutdown
%LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
Router(config-if)#exit
!--
Router(config)#int fa0/0.1
```

```
Router(config-subif)#encapsulation dot1q 1
Router(config-subif)#ip address 10.1.1.11 255.255.255.0
Router(config-subif)#int fa0/0.5
Router(config-subif)#encapsulation dot1q 5
Router(config-subif)#ip address 10.1.5.11 255.255.255.0
Router(config-subif)#exit
Router(config)#int fa0/0.7
Router(config-subif)#encapsulation dot1q 7
Router(config-subif)#ip address 10.1.7.11 255.255.255.0
Router(config)#int fa0/0.2
Router(config-subif)#encapsulation dot1q 2
Router(config-subif)#ip address 10.1.2.11 255.255.255.0
Router(config-subif)#exit
Router(config)#exit
!
!-- Проконтролируем состояние интерфейсов и подинтерфейсов
!
Router#show ip int
Serial0 is administratively down, line protocol is down
Internet protocol processing disabled
FastEthernet0/0 is up, line protocol is up
Internet protocol processing disabled

FastEthernet0/0.1 is up, line protocol is up
  Internet address is 10.1.1.11/24
  Broadcast address is 255.255.255.0
  MTU 1500 bytes
:
:
FastEthernet0/0.7 is up, line protocol is up
  Internet address is 10.1.7.11/24
  Broadcast address is 255.255.255.0
  MTU 1500 bytes
```

Проверим возможность передачи пакетов между виртуальными сетями и связь с внешним сервером SvO, в частности, связь рабочей станции PC5-5 с внешним сервером SvO и PC7-1.

```
     Ethernet adapter Local Area Connection:
        IP Address. . . . . . . . . . . : 10.1.5.5
        Subnet Mask . . . . . . . . . . .: 255.255.255.0
        Default Gateway . . . . . . . . : 10.1.5.11

C:>ping 10.1.0.12
Pinging 10.1.0.12 with 32 bytes of data:

Reply from 10.1.0.12: bytes=32 time=60ms TTL=241
```

```
Reply from 10.1.0.12: bytes=32 time=60ms TTL=241
Reply from 10.1.0.12: bytes=32 time=60ms TTL=241
Reply from 10.1.0.12: bytes=32 time=60ms TTL=241
Reply from 10.1.0.12: bytes=32 time=60ms TTL=241

Ping statistics for 10.1.0.12:  Packets: Sent = 5,
Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 50 ms, Maximum = 60 ms, Average = 55 ms

C:>ping 10.1.7.2
Pinging 10.1.7.2 with 32 bytes of data:

Reply from 10.1.7.2: bytes=32 time=60ms TTL=241
Reply from 10.1.7.2: bytes=32 time=60ms TTL=241
Reply from 10.1.7.2: bytes=32 time=60ms TTL=241
Reply from 10.1.7.2: bytes=32 time=60ms TTL=241
Reply from 10.1.7.2: bytes=32 time=60ms TTL=241

Ping statistics for 10.1.7.2:  Packets: Sent = 5,
Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 50 ms, Maximum = 60 ms, Average = 55 ms
```

Как видно из результатов эксперимента, подключение виртуальных сетей к маршрутизатору позволяет осуществлять обмен между хостами различных виртуальных сетей.

Аналогичным образом выполняется конфигурация коммутатора Sw-2 и проверка правильности задания параметров конфигурации. В пояснительной записки необходимо привести тексты сценариев конфигурации всех устройств, входящих в состав моделируемой сети.

9.4. Тестирование сети и коррекция схемы по результатам моделирования

Проверим функционирование спроектированной сети в целом. Для этого выполним процедуру пингования с рабочих станций, включенных в виртуальные сети, относящихся ко второму коммутатору. Проведем пингование с первой рабочей станции PC6-1 шестой vlan.

```
Ethernet adapter Local Area Connection:
   IP Address. . . . . . . . . . . : 10.1.6.1
   Subnet Mask . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . : 10.1.6.11
```

!-- Пингование станции собственной vlan.

```
C:>ping 10.1.6.2
Pinging 10.1.6.2 with 32 bytes of data:

Reply from 10.1.6.2: bytes=32 time=60ms TTL=241
Reply from 10.1.6.2: bytes=32 time=60ms TTL=241
Reply from 10.1.6.2: bytes=32 time=60ms TTL=241
Reply from 10.1.6.2: bytes=32 time=60ms TTL=241
Reply from 10.1.6.2: bytes=32 time=60ms TTL=241

Ping statistics for 10.1.6.2: Packets: Sent = 5,
Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 50 ms, Maximum = 60 ms, Average = 55 ms
```

! -- Пингование интерфейса шлюза по умолчанию.

```
C:>ping 10.1.6.11
Pinging 10.1.6.11 with 32 bytes of data:
Reply from 10.1.6.11: bytes=32 time=60ms TTL=241
Reply from 10.1.6.11: bytes=32 time=60ms TTL=241
Reply from 10.1.6.11: bytes=32 time=60ms TTL=241
Reply from 10.1.6.11: bytes=32 time=60ms TTL=241
Reply from 10.1.6.11: bytes=32 time=60ms TTL=241

Ping statistics for 10.1.6.11:  Packets: Sent = 5,
Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 50 ms, Maximum = 60 ms, Average = 55 ms
```

!-- Пингование внешнего сервера предприятия

```
C:>ping 10.1.0.12
Pinging 10.1.0.12 with 32 bytes of data:

Reply from 10.1.0.12: bytes=32 time=60ms TTL=241
Reply from 10.1.0.12: bytes=32 time=60ms TTL=241
Reply from 10.1.0.12: bytes=32 time=60ms TTL=241
Reply from 10.1.0.12: bytes=32 time=60ms TTL=241
Reply from 10.1.0.12: bytes=32 time=60ms TTL=241
```

Пингование шлюза по умолчанию и сервера предприятия показало, что эти устройства достижимы. Следовательно, схема сети составлена корректно, а конфигурация устройств выполнена верно.

Аналогичное тестирование следует провести со всех рабочих станций и серверов. После проведения тестирования всех возможных интерфейсов спроектированной сети можно сделать вывод, что сеть функционирует кор-

ректно, либо необходимо провести коррекцию конфигурации или подключения рабочих станций к коммутаторам.

Конфигурация списков доступа.

```
    Router#
    Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
    Router(config)#access-list 10 permit 10.1.1.0 0.0.0.255
    Router(config)#access-list 10 deny 10.1.0.0 0.0.255.255
    Router(config)#int fa0/0.2
    Router(config-subif)#ip access-group 10 out
    Router(config-subif)#exit
    Router(config)#^Z
    %SYS-5-CONFIG_I: Configured from console by console

    Router#show access-list 10
    Standard IP access list 10
        10 permit 10.1.1.0 0.0.0.255 (0 matches)
        10 deny   10.1.0.0 0.0.255.255 (20 matches)
```

Проверка доступа к сети 10.1.2.0. Пингование выполняется с рабочей станции PC5-1 с IP-адресом 10.1.5.1

```
    C:>ping 10.1.5.5
    Pinging 10.1.5.5 with 32 bytes of data:

    Reply from 10.1.5.5: bytes=32 time=60ms TTL=241
    Reply from 10.1.5.5: bytes=32 time=60ms TTL=241
    Reply from 10.1.5.5: bytes=32 time=60ms TTL=241
    Reply from 10.1.5.5: bytes=32 time=60ms TTL=241
    Reply from 10.1.5.5: bytes=32 time=60ms TTL=241

    Ping statistics for 10.1.5.5:   Packets: Sent = 5,
    Received = 5, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
    Minimum = 50 ms, Maximum = 60 ms, Average = 55 ms

    C:>ping 10.1.1.1
    Pinging 10.1.1.1 with 32 bytes of data:

    Reply from 10.1.1.1: bytes=32 time=60ms TTL=241
    Reply from 10.1.1.1: bytes=32 time=60ms TTL=241
    Reply from 10.1.1.1: bytes=32 time=60ms TTL=241
    Reply from 10.1.1.1: bytes=32 time=60ms TTL=241
    Reply from 10.1.1.1: bytes=32 time=60ms TTL=241

    Ping statistics for 10.1.1.1:   Packets: Sent = 5,
```

```
Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 50 ms, Maximum = 60 ms, Average = 55 ms

C:>ping 10.1.2.1
Pinging 10.1.2.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.1.2.1:
Packets: Sent = 5, Received = 0, Lost = 5 (100% loss),
Approximate round trip times in milli-seconds:
Minimum = 0 ms, Maximum = 0 ms, Average = 0 ms
```

Тестирование спроектированной сети прошло успешно.

Заключение

В заключительной части записки отмечается, что параметры спроектированной сети полностью соответствуют техническому заданию, а результаты компьютерного моделирования функционирования сети подтверждают ее работоспособность. Отмечается также, что спроектированная сеть рассчитана на такое-то количество рабочих мест, содержит такое-то современное телекоммуникационное оборудование, которое позволит эксплуатировать сеть в течение 10 лет без существенной модернизации аппаратной части.

СПИСОК РЕКОМЕНДОВАНОЙ ЛИТЕРАТУРЫ

1. Амато В. Основы организации сетей Cisco. Том 1: Пер. с англ./ В.Амато. — М.: Изд-во "Вильямс", 2004. — 512 с.
2. Амато В. Основы организации сетей Cisco. Том 2. : Пер. с англ. / В.Амато. — М.: Изд-во "Вильямс", 2004. — 464 с.
3. Баскаков И. Построение коммутируемых компьютерных сетей / И. Баскаков, А. Пролетарский, Е. Смирнова, Р. Федотов. Национальный Открытый Университет "ИНТУИТ". ://http://www.intuit.ru/studies/ courses/ 3591/833 /info.
4. Боллапрагада В. Структура операционной системы Cisco IOS: Пер. с англ. / В. Боллапрагада, К.Мэрфи, Р.Уайт: Пер. с англ. — М.: Изд-во "Вильямс", 2002. — 208 с.
5. Бондаренко М.Ф. Проектирование и диагностика компьютерных систем и сетей: Учебное пособие / М.Ф.Бондаренко, Г.Ф.Кривуля, В.Г.Рябцев, С.А.Фрадков, В.И. Хаханов. – К.: НМЦ ВО, 2000. – 306 с.
6. Васин Н.Н. Основы сетевых технологий на базе коммутаторов и маршрутизаторов: Учебное пособие / Н.Н. Васин. — М.: БИНОМ, Лаборатория знаний, 2011. — 270 с.
7. Григорьев В.М. Лабораторный практикум по сетям Cisco с использованием Boson / В. М.Григорьев. — Днепропетровск: 2009. — 142 с.
8. Гук М. Аппаратные средства локальных сетей. Энциклопедия. — СПб.: Издательство Питер, 2000. — 576 с.
9. Димарцио Д. Ф. Маршрутизаторы Cisco. Пособие для самостоятельного изучения: Пер. с англ. / Д.Ф. Димарцио. — СПб: Изд-во Символ Плюс, 2003. — 512 с.
10. Кларк К. Принципы коммутации в локальных сетях Cisco: Пер. с англ. / К.Кларк, К. Гамильтон. — М.: Изд-во "Вильямс", 2003. — 976 с.
11. Коммутаторы локальных сетей D-Link: Учебное пособие. — М.: ИТ-Планета, 2006. — 156 с.
12. Кульгин М.В. Компьютерные сети. Практика построения. Для профессионалов / М.В. Кульгин. — СПб.: Изд-во "Питер", 2003. — 368.
13. Леинванд А. Конфигурирование маршрутизаторов Cisco: Пер. с англ. / А. Леинванд, Б. Пински. — М.: Изд-во "Вильямс", 2001. — 560 с.
14. Мамаев М. Технология защиты информации в Интернете. Специальный справочник / М.Мамаев, С.Петренко. — СПб.: Изд-во "Питер", 2002. — 848 с.
15. Обзор продуктов и решений компании Cisco Systems (издание VIII) www.**cisco**.com/web/RU/downloads/**Obzor_produkt**ov_VIII.pdf
16. Одом У. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2, 2-е изд.: Пер. с англ. / У. Одом. — Изд-во "Вильямс", 2011. — 736 с.

17. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. / В.Г.Олифер, Н.А.Олифер. – СПб: Изд-во "Питер", 2010. — 944 с.
18. Пакет К. Создание сетей удаленного доступа Cisco: Пер. с англ. / Л.Пакет. — Изд-во "Вильямс", 2003. — 672 с.
19. Петренко С.А., Курбатов В. А. Политики безопасности компании при работе в Интернет — М.: Изд-во ДМК-Пресс, 2011. — 400 с.
20. Программа сетевой академии Cisco CCNA 1 и 2. Вспомогательное руководство: Пер. с англ. – М.: Изд-во "Вильямс", 2005. — 1168 с.
21. Ретана А. Принципы проектирования корпоративных IP-сетей: Пер. с англ. / А. Ретана, Д. Слайс, Р. Уайт. — М.: Изд-во "Вильямс", 2002. — 368 с.
22. Семенов А.Б. Проектирование и расчет структурированных кабельных систем и их компонентов / А.Б. Семенов. — М.: ДМК Пресс, 2003. — 416+16 с.
23. Семенов Ю.А. Телекоммуникационные технологии ГНЦ ИТЭФ. http://www.book.iter.ru
24. Смирнов, И.Г. Структурированные кабельные системы / И.Г. Смирнов. — М.: Издательство: ЭКО-ТРЕНДЗ, 1998. — 178 с.
25. Столлингс В. Современные компьютерные сети: Пер. с англ. / В.Столлингс. — СПб.: Изд-во "Питер", 2003. — 783 с.
26. Столлингс В. Основы защиты сетей. Приложения и стандарты: Пер. с англ. / В.Столлингс. — М.: Изд-во "Вильямс", 2002. — 432 с.
27. Таненбаум Э. Компьютерные сети: Пер. с англ. 5-е изд. / Э.Таненбаум, Д. Уэзеролл. — СПб.: Изд-во "Питер", 2012. — 960 с.
28. Телекоммуникационные системы и сети: Учебное пособие. В 3-х томах. Том 3. — Мультисервисные сети / В.В. Величко, Е.А. Субботин, В.П. Шувалов, А.Ф. Ярославцев / Под ред. профессора В.П. Шувалова — М.: Горячая линия-Телеком, 2005. — 592 с.
29. Техническая характеристика коммутаторов семейства Catalyst фирмы Cisco [http://www.bkc.com.ua/product.asp?cid=1276].
30. Хабракен Дж. Как работать с маршрутизаторами Cisco: Пер. с англ. / Дж. Хабракен. — М.: Изд-во ДМК Пресс, 2005. — 320 с.
31. Хелеби С. Принципы маршрутизации в Internet: Пер. с англ. / С.Хелеби, Д.Мак-Ферсон: Пер. с англ. — М.: Изд-во "Вильямс", 2001. — 448 с.
32. Хьюкаби Д. Руководство Cisco по конфигурированию коммутаторов Catalyst: Пер. с англ. / Д.Хьюкаби, С. Мак-Квери. — М.: Изд-во "Вильямс", 2004. — 560 с.
33. Чернега В.С. Компьютерные сети /В.Чернега, Б.Платтнер. — Севастополь: Изд-во СевНТУ, 2006. — 500 с.

34. Чернега В.С. Расчет и проектирование технических средств обмена и передачи информации / В.С. Чернега, В.А. Василенко, В.Н. Бондарев — М.: Высшая школа, 1990. — 224 с.
35. Чернега В. Безпровідні локальні компютерні мережі: навчальний посібник для технічних університетів / В. Чернега, Б.Платтнер. — К.: Кондор-Видаництво, 2013. — 238 с.
36. Catalyst 2950 and Catalyst 2955 Switch Command Reference. — San Jose: Cisco Systems Inc., 2008. – 674 P.
37. Catalyst 3550 Multilayer Switch Command Reference. — San Jose: Cisco Systems Inc., 2004. — 670 P.
38. Quinn-Andry T. Netzwerk-Design / Terry Quinn-Andry, Kitty Haller. – Munchen: Markt&Technik Buch- und Software Verlag, 1998. — 397 S.
39. Установка и настройка коммутаторов Cisco Catalyst серий 2900XL и 3500 [http://www.network.xsp.ru].
40. ГОСТ 21.614-88. Изображения условные графические электрооборудования и проводок на планах. М.: 1988. – 31 с.
41. Стандарт ANSI/TIA/EIA-569-A (Февраль 1998). Стандарт телекоммуникационных трасс и пространств коммерческих зданий. http://www.ivtechno.ru/files/TIA-EIA-569-A.pdf
42. Стандарт ISO/IEC 11801:2009. Информационные технологии. Прокладка кабелей по схеме общего назначения в помещениях пользователей телекоммуникационных систем. http://iiti.it/home/index.php/ Download-document/6-Generic-cabling-for-customer-premises.html.
43. Стандарт ANSI/TIA/EIA-606 администрирования телекоммуникационных инфраструктур коммерческих зданий http://www.rfcmd.ru/sphider/docs/INT/ANSI_TIA_EIA-606.htm
44. Структурированные кабельные системы. Открытый стандарт OSSIRIUS SCS 702 v3.1. от 2010-01-01. http://1labi.com/content/view/33/33/#17

Приложение А1 - Таблица вариантов задания на курсовой проект

Номер варианта соответствует номеру студента в списке группы

Исходные данные на проектирование	Варианты								
	1	2	3	4	5	6	7	8	9
Расстояния между зданиями, км	-	-	-	-	-	-	-	-	-
Внутренних/внешних серверов в сети	2/1	4/1	4/2	3/2	2/2	4/1	5/2	2/3	4/3
Место подключения серверов: узел этажа (Э), здания (З), серверная ферма (СФ)	Э	Э	Э	Э	Э	З	З	З	СФ
Реализация сети: свич/роутер	С	Р	С	С	С	Р	С	Р	С
Деление на подсети: Да/Нет	Нет	Да	Нет	Нет	Нет	Да	Нет	Да	Нет
Деление на VLAN	Да	Нет	Да	Да	Да	Нет	Да	Нет	Да
Адрес шлюза по умолчанию: Приложение Б									
Вид связи с IP: Frame Relay (FR); ATM (A); ВОЛС(В); FastEthernet (FA)	FA	A	FR	B	B	FA	A	FR	B
Способ адресации: Класс/Бесклас	Б	Б	Б	Б	Б	Б	Б	Б	К
Возможность расширения: Да/Нет	Да	Да	Да	Да	Да	Да	Да	Да	Да
Наличие резервирования	Н	Н	Да	Н	Н	Да	Н	Н	Н
Количество каналов, соединяющих узлы этажа с узлом здания (1-16)	2	1	2	2	1	3	1	1	2
Допустимая отказоустойчивость,<= сек	600	1200	200	2000	600	600	600	1200	2000
Наличие DMZ: Да/Нет	Нет	нет	Да	Нет	Нет	Да	Нет	Нет	Да
Виды политики безопасности:									
удаленного доступа	+	+	+		+	+	+		+
взаимодействия с Интернет	+	+	+	+	+	+	+	+	+
правила предоставления доступа	+			+		+		+	+
выбора и использования паролей	+	+		+			+		+
инструкция по защите от вирусов		+			+			+	

Продолжение таблицы А1

Параметры сети	Варианты							
	10	11	12	13	14	15	16	17
Расстояния между зданиями, км	-	-	-	-	-	-	-	-
Внутренних/внешних серверов в сети	4/1	6/3	2/3	4/2	3/1	3/2	6/4	5/2
Место подключения серверов: узел этажа (Э), здания (З), серверная ферма (СФ)	СФ	Э	Э	Э	Э	Э	Э	З
Реализация сети: свич/роутер	С	С	Р	С	Р	С	Р	С
Деление на подсети: Да/Нет	Нет	Нет	Да	Нет	Да	Нет	Да	Нет
Деление на VLAN	Да	Да	Нет	Да	Нет	Да	Нет	Да
Адрес шлюза по умолчанию: Приложение Б								
Вид связи с IP: Frame Relay (FR); ATM (A); ВОЛС(В); FastEthernet (FA)	FA	A	FR	B	B	FA	A	FR
Способ адресации: Класс/Бесклас	Б	К	Б	К	К	Б	К	Б
Возможность расширения: Да/Нет	Да	Да	Да	Да	Да	Да	Да	Да
Наличие резервирования	Н	Н	Н	Н	Н	Н	Д	Д
Количество каналов, соединяющих узлы этажа с узлом здания (1-16)	2	1	2	2	1	3	1	1
Допустимая отказоустойчивость, сек	2000	600	200	600	1000	1200	240	2000
Наличие DMZ: Да/Нет	Да	Да	Да	Нет	Да	Нет	Да	Да
Виды политики безопасности:								
удаленного доступа	+	+	+		+	+	+	
взаимодействия с Интернет	+	+	+	+	+	+	+	+
правила предоставления доступа	+			+		+		+
выбора и использования паролей	+	+		+			+	
инструкция по защите от вирусов		+			+			+

Продолжение таблицы А1

Параметры сети	Варианты							
	18	19	20	21	22	23	24	25
Расстояния между зданиями, км Тип ЛС: Медь-ТР; ВОЛС (ОЛ)	-	-	0.5 ТР	1,2 ОЛ	2.2 ОЛ	10 ОЛ	8 ОЛ	0,4 ТР
Внутренних/внешних серверов в сети	2/2	4/3	3/4	4/2	6/2	3/1	4/1	3/2
Место подключения серверов: узел этажа (Э), здания (З), серверная ферма (СФ)	З	З	З	СФ	СФ	З	З	З
Реализация сети: свич/роутер	С	Р	С	С	С	Р	С	Р
Деление на подсети: Да/Нет	Нет	Да	Нет	Нет	Нет	Да	Нет	Да
Деление на VLAN	Да	Нет	Да	Да	Да	Нет	Да	Нет
Адрес шлюза по умолчанию: Приложение Б								
Вид связи с IP: Frame Relay (FR); ATM (A); ВОЛС(В); Ethernet (E)	В	А	FR	В	В	Е	А	FR
Способ адресации: Класс/Бесклас	К	Б	Б	Б	Б	К	Б	К
Возможность расширения: Да/Нет	Да	Да	Да	Нет	Нет	Нет	Нет	Нет
Наличие резервирования	Д	Д	Д	Н	Н	Н	Н	Н
Количество каналов, соединяющих узлы этажа с узлом здания (1-16)	2	2	1	2	2	1	3	1
Допустимая отказоустойчивость, сек	2400	600	600	40	60	200	100	200
Наличие DMZ: Да/Нет	Да	Да	Нет	Да	Нет	Да	Нет	Да
Виды политики безопасности:								
удаленного доступа	+	+	+	+		+	+	+
взаимодействия с Интернет	+	+	+	+	+	+	+	+
правила предоставления доступа	+	+			+		+	
выбора и использования паролей	+	+	+		+			+
инструкция по защите от вирусов			+			+		

Приложение А2 - Варианты чертежей зданий (Приложение А4)

Вар-т	Кол-во зданий	Кол-во этажей/ зданий	Чертеж 1-го здания					Чертеж 2-го здания		
			Этажи					Этажи		
			1	2	3	4	5	1	2	3
1	1	1/1	Д.1							
2	1	1/1	Д.2							
3	1	1/1	Д.3							
4	1	2/1	Д.1	Д.2						
5	1	2/1	Д.2	Д.3						
6	1	2/1	Д.3	Д.4						
7	1	2/1	Д.4	Д.5						
8	1	3/1	Д.1	Д.3	Д.2					
9	1	3/1	Д.1	Д.4	Д.5					
10	1	3/1	Д.2	Д.3	Д.4					
11	1	3/1	Д.3	Д.2	Д.5					
12	1	3/1	Д.1	Д.4	Д.2					
13	1	4/1	Д.1	Д.2	Д.3	Д.4				
14	1	4/1	Д.2	Д.3	Д.4	Д.5				
15	1	4/1	Д.3	Д.4	Д.5	Д.1				
16	1	4/1	Д.1	Д.5	Д.3	Д.4				
17	1	4/1	Д.4	Д.2	Д.1	Д.3				
18	1	4/1	Д.2	Д.5	Д.3	Д.4				
19	1	5/1	Д.1	Д.2	Д.3	Д.4	Д.5			
20	2	1/2	Д.2					Д.3		
21	2	1/2	Д.3					Д.5		
22	2	1/2	Д.4					Д.3		
23	2	2/2	Д.2	Д.3				Д.1	Д.4	
24	2	2/2	Д.3	Д.4				Д.2	Д.5	
25	2	2/2	Д.1	Д.3				Д.5	Д.4	
26	2	2/2	Д.5	Д.1				Д.4	Д.2	

Приложение А3 – Варианты адресов шлюзов по умолчанию (IP-адреса)

Вариант	IP-адрес
1	78.25.34.238
2	89.208.181.222
3	78.234.108.44
4	125.222.126.88
5	22.78.123.80
6	80.238.104.44
7	196.243.106.8
8	224.32.132.80
9	89.208.180.43
10	208.98.234.100
11	200.106.32.111
12	140.235.100.91
13	222.2.140.100
14	79.120.90.91
15	83.221.165.30
16	30.83.222.160
17	56.187.91.20
18	86.200.43.145
19	59.180.81.94
20	209.34.55.68
21	90.91.92.93
22	23.87.63.120
23	230.180.81.96
24	156.67.82.20
25	120.20.32.160
26	21.91.25.100

Приложения А4. — Варианты поэтажных чертежей здания, занимаемого организацией

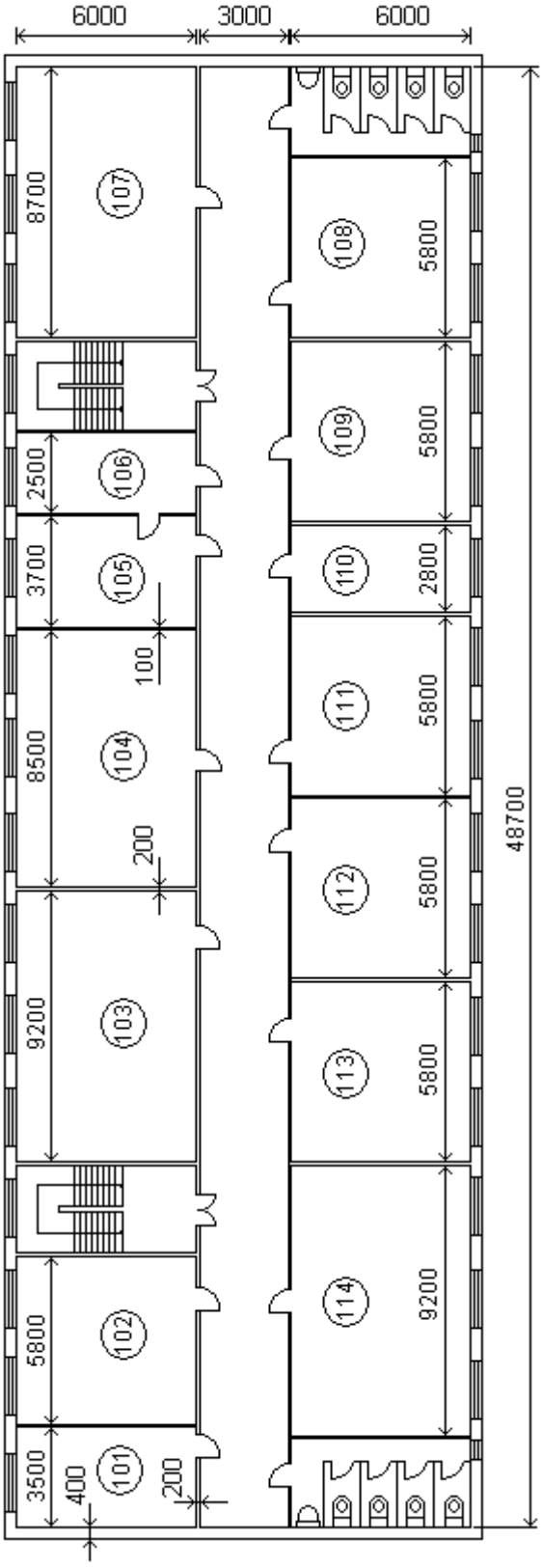


Рисунок В1 – Чертеж этажа здания В1

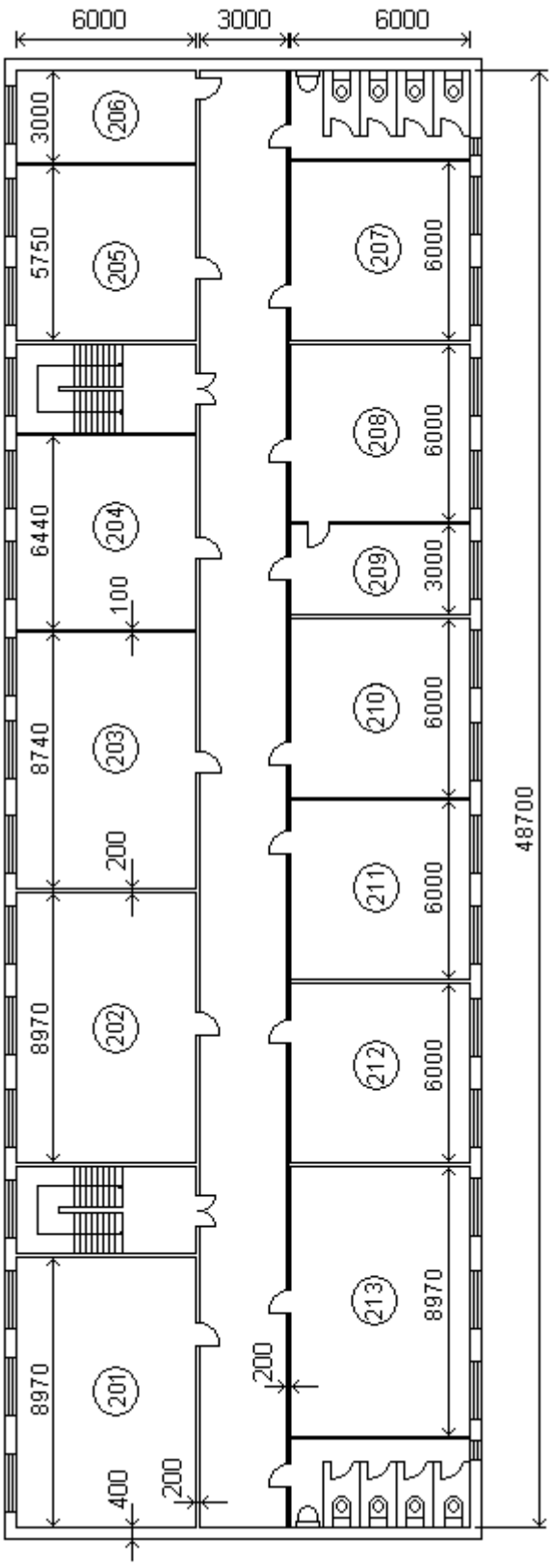


Рисунок В2 – Чертеж этажа здания В2

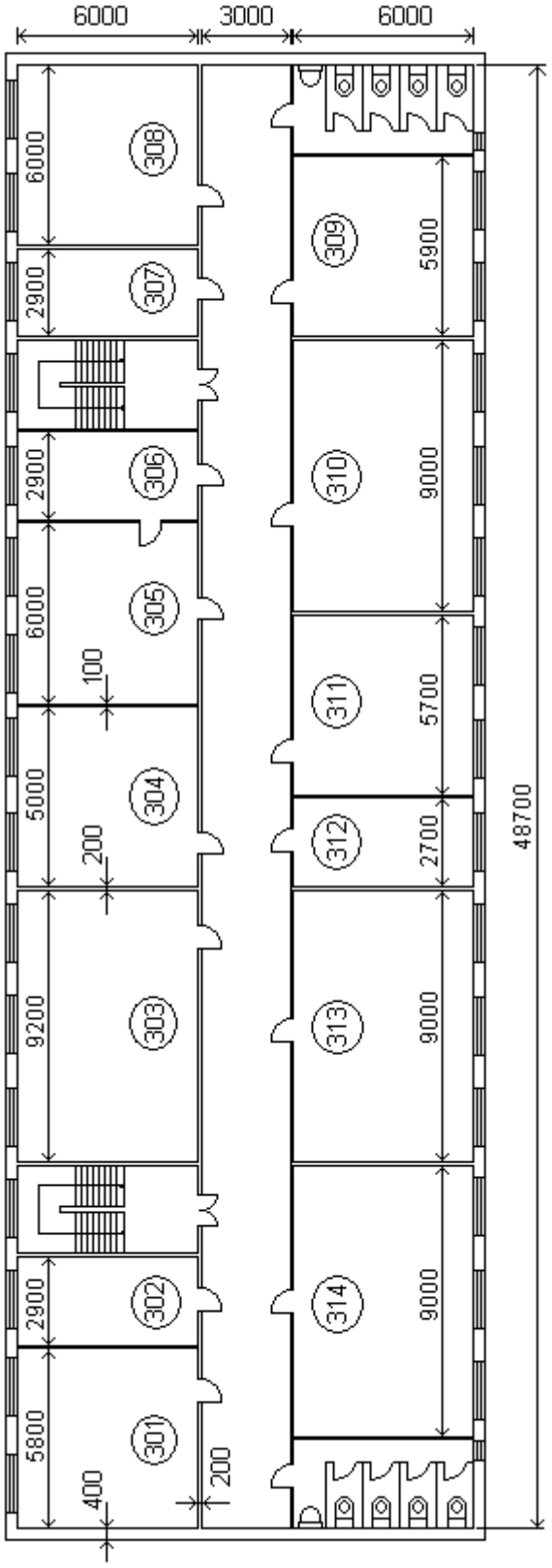


Рисунок В3 – Чертеж этажа здания В3

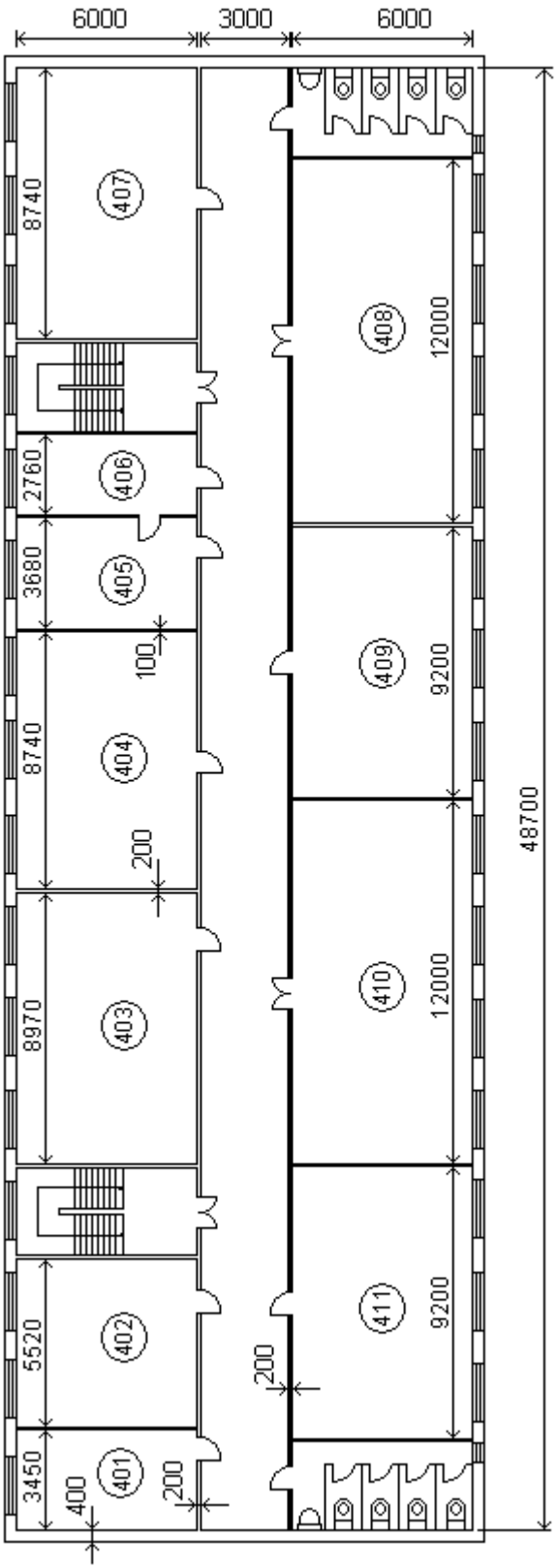


Рисунок В4 – Чертеж этажа здания В4

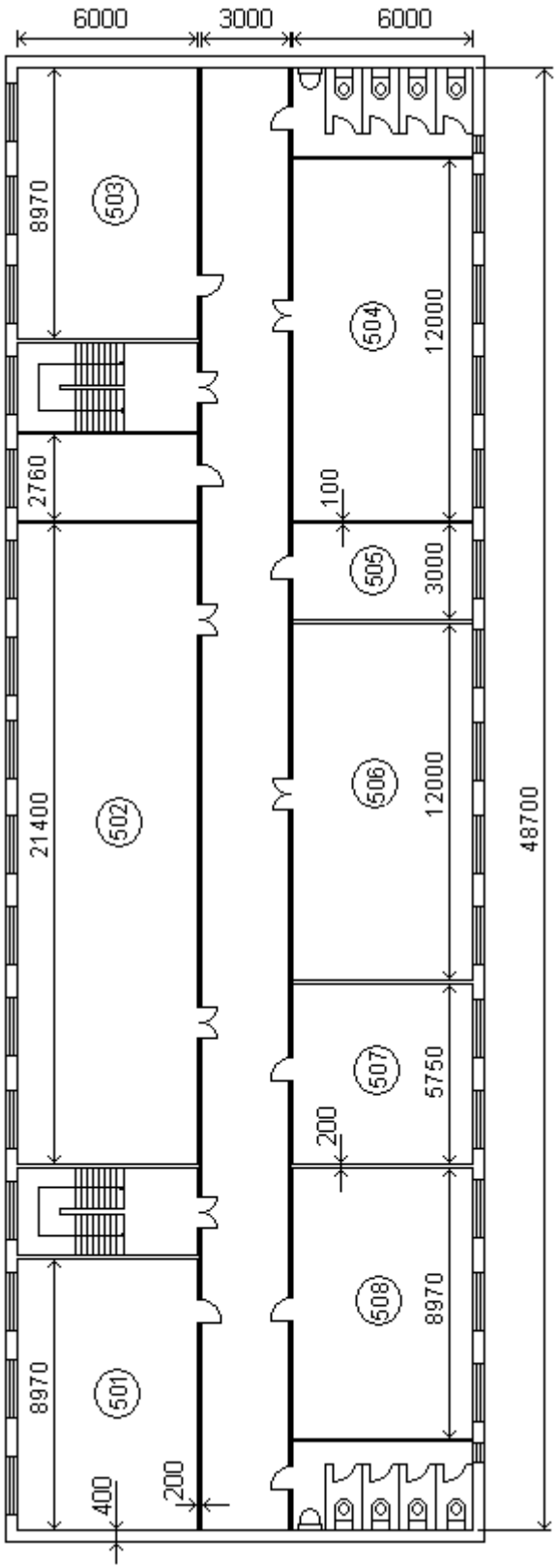


Рисунок В5 – Чертеж этажа здания В5

Приложение А5. Пример выполнения таблицы соединений

Обозначение кабеля	Откуда идет	Куда поступает	Данные кабеля	Примечание
КГ303-1-1	303 — ТР-1-1	312 — ПП-01-01	UTP-5e 4PR - 27 м	
КГ303-1-2	303 — ТР-1-2	312 — ПП-02-01	UTP-5e 4PR - 27 м	
КГ303-2-1	303 — ТР-2-1	312 — ПП-01-03	UTP-5e 4PR - 30 м	
КГ303-2-2	303 — ТР-2-2	312 — ПП-02-01	UTP-5e 4PR - 30 м	
ПК303-1	303 — КК-1	303 — ТР-1-1	UTP-5e RJ45 - 2 м	
ПК312-1	312 — ПП-02-01	312 — СК-02-12	UTP-5e RJ45 - 1 м	
ПК312-8	312 — СК-03-06	312 — М-01-02	UTP-5e RJ45 - 1 м	

					СевГУ 09.03.02.04 ТС
Изм	Лист	№ докум.	Подп.	Дата	
Разработ.		Иванов		5.5.18	Компьютерная сеть предприятия "Омега-1". Таблица соединений
Проверил		Дрозин		7.5.18	
Н.Контр.		Волкова		7.5.18	
Утвердил		Шумейко		8.5.18	

Лит	Лист	Листов
Т	1	4

Курсовой проект
Кафедра ИС
группа ИС-41о

Приложение А6. Цепи и контакты разъемов интерфейса V.35

Контакты разъема		Описание цепей	Обозначение	Источник
M34	DB-25			
A	1	Заземление корпуса (шасси)	Ground	Общий
P	2	Передача данных - A	TD-A	DTE
R	3	Прием данных - A	RD-A	DCE
C	4	Запрос передачи	RTS	DTE
D	5	Готовность к передаче	CTS	DCE
E	6	Готовность данных	DSR	DCE
B	7	Сигнальное заземление	SG	Общий
F	8	Детектирование несущей	CD	DCE
X	9	Синхронизация приема - B	RC-B	DCE
	10	Не используется		
W	11	Внешняя синхронизация передачи - B	XTC-B	DTE
AA	12	Синхронизация передачи - B	TC-B	DTE
	13	Не используется		
S	14	Передача данных - B	TD-B	DTE
Y	15	Синхронизация передачи - A	TC-A	DCE
T	16	Прием данных - B	RD-B	DCE
V	17	Синхронизация приема - A	RC-A	DCE
L	18	Локальный шлейф	LL	DTE
	19	Не используется		
H	20	Готовностьтерминала	DTR	DTE
N	21	Удаленный шлейф	RL	DTE
	22	Не используется		
	23	Не используется		
U	24	Внешняя синхронизация передачи - A	XTC-A	DTE
M	25	Режим тестирования	TM	DCE

Приложение А7. Данные для выбора сечения кабеля для открытой электропроводки

Сечение кабеля, мм²	Закрытая проводка					
	Медный провод			Алюминиевый провод		
	Ток, А	Мощность, кВт		Ток, А	Мощность, кВт	
		220 В	380 В		220 В	380 В
0, 5	-	-	-	-	-	-
0, 75	-	-	-	-	-	-
1, 0	14	3, 0	5, 3	-	-	-
1, 5	15	3, 3	5, 7	-	-	-
2, 0	19	4, 1	7, 2	14	3, 0	5, 3
2, 5	21	4, 6	7, 9	16	3, 5	6, 0
4, 0	27	5, 9	10	21	4, 6	7, 9
6, 0	34	7, 4	12	26	5, 7	9, 8
10	50	11	19	38	8, 3	14
16	80	17	30	55	12	20
25	100	22	38	65	14	24
35	135	29	51	75	16	28

Данные для выбора сечения кабеля для закрытой электропроводки

Сечение кабеля, мм²	Открытая проводка					
	Медный провод			Алюминиевый провод		
	Ток, А	Мощность, кВт		Ток, А	Мощность, кВт	
		220 В	380 В		220 В	380 В
0, 5	11	2, 4	-	-	-	-
0, 75	15	3, 3	-	-	-	-
1, 0	17	3, 7	6, 4	-	-	-
1, 5	23	5, 0	8, 7	-	-	-
2, 0	26	5, 7	9, 8	21	4, 6	7, 9
2, 5	30	6, 6	11	24	5, 2	9, 1
4, 0	41	9, 0	15	32	7, 0	12
6, 0	50	11	19	39	8, 5	14
10	80	17	30	60	13	22
16	100	22	38	75	16	28
25	140	30	53	105	23	39
35	170	37	64	130	28	49