Учреждение образования
«Гомельский государственный университет
имени Франциска Скорины»

Факультет физики и информационных технологий
Кафедра автоматизированных систем обработки информации

СОГЛАСОВАНО
Заведующий кафедрой
автоматизированных систем
обработки информации
А.В.Воруев
__ _____ 2023 г.

СОГЛАСОВАНО
Декан
факультета физики и
информационных технологий
Д.Л.Коваленко
__ _____ 2023 г.

ЭЛЕКТРОННЫЙ УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

АППАРАТНО-ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ СЕТЕЙ

для специальности
1-53 01 02 Автоматизированные системы обработки информации

составители: заведующий кафедрой АСОИ, к.т.н., доцент, Воруев А.В.
старший преподаватель Кулинченко В.Н.
старший преподаватель Кучеров А.И.

Рассмотрено и утверждено
на заседании кафедры АСОИ
__14 марта___ 2023 г., протокол № _8_

Рассмотрено и утверждено
на заседании научно-методического
совета университета
_____ 2023 г., протокол № ___

Гомель 2023

1 ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Электронный учебно-методический комплекс (ЭУМК) по дисциплине «Аппаратно-программное обеспечение сетей» представляет собой комплекс систематизированных учебных, методических и вспомогательных материалов, предназначенных для использования в образовательном процессе специальности 1-45 80 01 Системы и сети инфокоммуникаций.

ЭУМК разработан в соответствии со следующими нормативными документами:

1. Положением об учебно-методическом комплексе на уровне высшего образования, утвержденном постановлением Министерства образования Республики Беларусь от 26.07.2011 №167.

2. Учебная программа составлена на основе образовательного стандарта ОСВО 1-53 01 02-2021 г. и учебного плана ГГУ имени Ф.Скорины регистрационный № I 53-1-21/УП, дата утверждения 31.05.2021.

3. Учебной программой по учебной дисциплине «Аппаратно-программное обеспечение сетей» для специальности 1-53 01 02 Автоматизированные системы обработки информации, утвержденной 17.05.2022, регистрационный номер УД-2022-94/уч.

Целью дисциплины «Аппаратно-программное обеспечение сетей» является обеспечение приобретения теоретических знаний и практических навыков при подготовке специалистов в области аппаратно-программных средств современных сетевых технологий.

ЭУМК направлен на всестороннюю подготовку обучающихся теоретическим основам и практическим навыками по решению новых инженерных задач, возникающих при освоении и внедрении в сетевых стандартов и методов организации вычислительного процесса в сетевых структурах. Организация изучения дисциплины на основе ЭУМК предполагает продуктивную образовательную деятельность, позволяющую сформировать социально-личностные и профессиональные компетенции будущих специалистов.

ЭУМК способствует успешному осуществлению учебной деятельности, дает возможность планировать и осуществлять самостоятельную управляемую работу, обеспечивает рациональное распределение учебного времени по темам учебной дисциплины и совершенствование методики проведения занятий.

ЭУМК состоит из теоретического, практического и вспомогательного разделов. Теоретический раздел содержит тексты лекций. Практический раздел содержит методические рекомендации к лабораторным работам, тестовые задания и вопросы для самоконтроля. Вспомогательный раздел содержит учебную программу и список литературы.

Теоретический раздел содержит лекционный материал по всем темам учебной программы, включая и темы, вынесенные на самостоятельное изучение. В разделе так же содержатся рекомендации по организации и выполнению управляемой самостоятельной работы по трем уровням сложности.

Практический раздел включает в себя темы лабораторных занятий и задания с краткими методическими указаниями по выполнению лабораторных работ. В разделе так же приводятся некоторый набор тестовых заданий и к каждой теми указаны вопросы для самоконтроля.

Вспомогательный раздел содержит необходимые элементы учебно-программной документации по дисциплине с указанием рекомендуемой литературы (основной, дополнительной, вспомогательной).

Все разделы ЭУМК в полной мере соответствуют содержанию учебной программы и объему учебного плана.

Дисциплина компонента учреждения высшего образования «Аппаратно-программное обеспечение сетей» изучается студентами 2 курса дневной, заочной и дистанционной форм обучения специальности 1-53 01 02 - «Автоматизированные системы обработки информации».

Дневная форма обучения: всего часов по плану – 240 (6 зач. ед.); аудиторное количество часов – 124, из них: лекции – 64, лабораторные занятия – 60.

Форма отчётности – экзамены в 3,4 семестре.

Заочная форма обучения: всего часов по плану – 240 (6 зач. ед.), аудиторное количество часов – 30, из них: лекции – 16, лабораторные занятия – 14.

Форма отчётности – контрольные работы и экзамены в 4,5 семестрах.

Заочная сокращенная дистанционная форма обучения: всего часов по плану – 240 (6 зач. ед.), аудиторное количество часов – 20, из них: лекции – 10, лабораторные занятия – 10.

Форма отчётности – контрольные работы и экзамены в 4,5 семестрах.

2 ТЕКСТЫ ЛЕКЦИЙ

1 Организация вычислительного процесса в сетевой среде

1.1 Концепция цифровой сети

Впервые компьютерные сети появились почти одновременно с самими компьютерами. Это было связано с тем, что ресурс компьютерного времени был чрезвычайно дорогим и важно было разделить его стоимость между несколькими пользователями. Пользователи получили возможность параллельно подготавливать свои данные, которые затем могли обрабатываться последовательно или параллельно (в виде пакетов) блоками вычислительной системы.

Так появились принципы совместного использования ресурсов и терминальные системы. Эти системы широко использовались до 80-х годов 20 века, а некоторые образцы - почти до начала 21 века. Возрождение компьютерных сетей было вызвано практической необходимостью обмена данными между пользователями персональных вычислительных систем.

С этой точки зрения для компьютерных сетей подходит следующее определение: сеть - это система независимых компьютеров, соединенных друг с другом с целью обмена данными, периферийными устройствами и другими сетевыми ресурсами.

По прогнозам, общее число пользователей цифровых сетей во всем мире вырастет с 3,9 миллиарда в 2018 году до 5,3 миллиарда к 2023 году при среднем показателе 6 процентов. Что касается численности населения, то это составляет 51 процент мирового населения в 2018 году и 66 процентов мирового населения к 2023 году (рисунок 1.1).

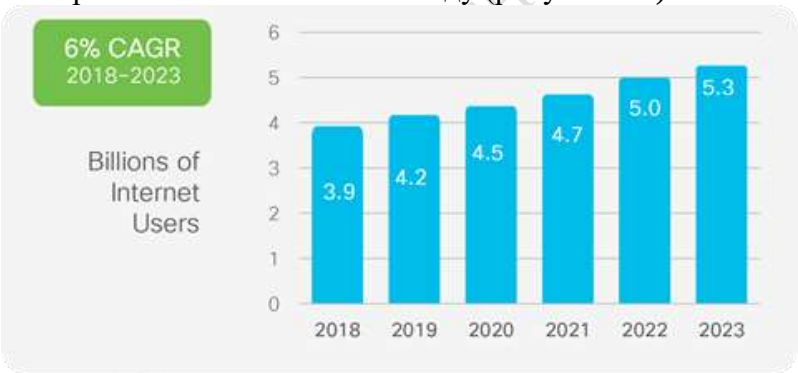


Рисунок 1.1 - Глобальный рост числа пользователей Интернета

Первоначально все сети можно было разделить на два класса:

- сети обмена данными или информационные сети;
- сети обработки данных или компьютерные сети.

Информационные сети включали системы для передачи сигналов, сообщений, данных и других видов информации. Распределенные и унифицированные вычислительные системы относились к сетям обработки данных. Но, поскольку распределенная обработка требует использования механизмов обмена информацией, эта грань постепенно стирается, и на данный момент все компьютерные сети являются как информационными, так и вычислительными. Поэтому часто используется более общий термин "цифровые сети".

Цифровые сети можно рассматривать с разных точек зрения:

- для запущенной программы сеть представляет собой сложную систему маршрутов для передачи данных и ресурсов для их обработки;
- для пользователя компьютерная сеть - это инструмент для доступа к сетевым ресурсам;
- для менеджера сеть - это средство управления производственными процессами;
- для сетевого дизайнера это набор стандартов и требований, которые необходимо соблюдать во время реализации проекта.

Современная цифровая сеть обладает следующими свойствами:

- отличное сочетание "производительность - удобство использования - стоимость" вычислительных ресурсов;
- обмен данными и устройствами;
- онлайн-доступ к обширной корпоративной информации;
- использование внешних данных;
- интеграция информационных систем.

Однако существуют также проблемы, связанные с внедрением сетей. Например, сложное программирование для распределенных систем, обеспечение совместимости программного обеспечения, обеспечение надежности передачи информации, обеспечение безопасности. Область использования компьютерных сетей сегодня постоянно расширяется, она включает в себя науку, образование, бизнес, развлечения.

Производительность сети часто измеряется скоростью передачи данных, которая может быть реализована в ее среде. Этот подход основан на том факте, что разные типы сетевых сервисов предъявляют разные требования к пропускной способности сети (рисунок 1.2).

Сочетание нескольких видов услуг в рамках единой сетевой структуры предъявляет дополнительные требования к используемому оборудованию и вспомогательным программным системам.

Таким образом, современные сети представляют собой сложные аппаратные и программные системы.

Во всем мире количество устройств и подключений растет быстрее (в среднем на 10 процентов), чем численность населения (в среднем на 1,0 процента) и пользователей Интернета (в среднем на 6 процентов). Эта тенденция ускоряет увеличение среднего числа устройств и подключений на домохозяйство и на душу населения.

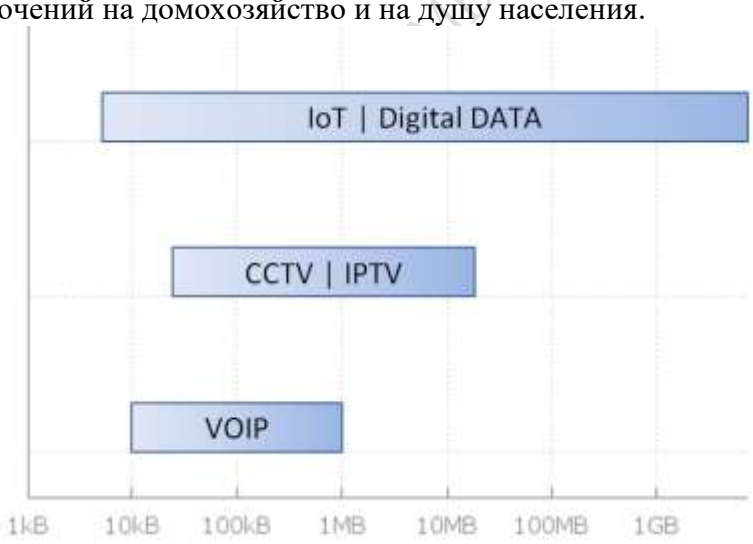


Рисунок 1.2 - Уровень требований к сетевым службам для пропускной способности сети

Растущее число приложений D2D, таких как интеллектуальные счетчики, видеонаблюдение, мониторинг здравоохранения, транспортировка и отслеживание посылок или активов, в значительной степени способствуют росту устройств и подключений. К 2023 году соединения D2D составят половину или 50 процентов от общего числа устройств и подключений.

Соединения D2D станут самой быстрорастущей категорией устройств и подключений, увеличившись почти в 2,4 раза за прогнозируемый период (средний показатель 19 процентов) до 14,7 миллиарда подключений к 2023 году. Смартфоны будут расти на втором месте по темпам роста - в среднем на 7 процентов (увеличившись в 1,4 раза). Подключенные телевизоры (которые включают телевизоры с плоским экраном, телевизионные приставки, цифровые медиа-адаптеры [DMA], проигрыватели дисков Blu-ray и игровые консоли) будут

расти следующими самыми быстрыми темпами (в среднем чуть менее 6 процентов), до 3,2 миллиарда к 2023 году. ПК продолжат снижаться (снижение на 2,3 процента) в течение прогнозируемого периода. Однако в течение прогнозируемого периода и к концу 2023 года компьютеров будет больше, чем планшетов (1,2 миллиарда ПК против 840 миллионов планшетов).

К 2023 году доля потребителей в общем объеме устройств, включая как стационарные, так и мобильные устройства, составит 74 процента, а бизнес претендует на оставшиеся 26 процентов. Доля потребителей будет расти несколько более медленными темпами, составив 9,1 процента в среднем по сравнению с бизнес-сегментом, который вырастет на 12,0 процента в среднем (рисунок 1.3).

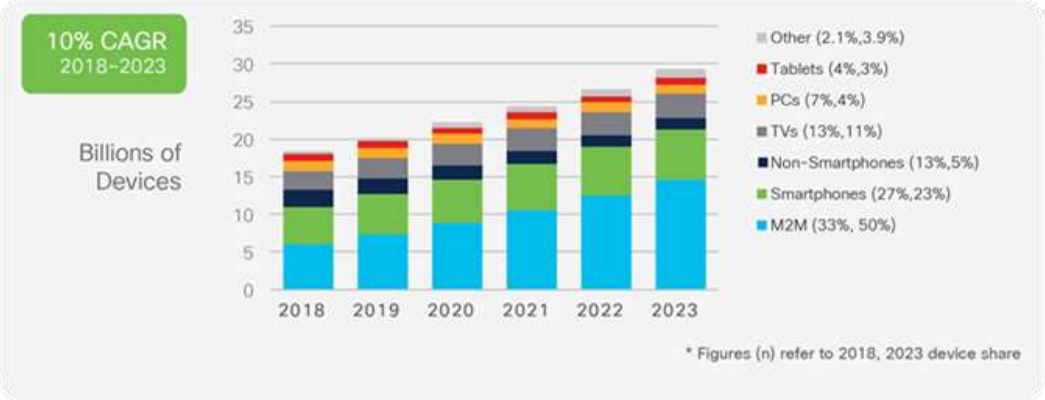


Рисунок 1.3 - Глобальный рост числа устройств и подключений

1.2. Виртуализация сетевых узлов и сегментов сети

Исторически корпоративные серверы состояли из серверной операционной системы (ОС), такой как Windows Server или Linux Server, установленной на определенном оборудовании. Вся оперативная память сервера, вычислительная мощность и место на жестком диске были выделены для предоставляемых услуг (например, веб-сервисов, служб электронной почты и т.д.).

Основная проблема с этой конфигурацией заключается в том, что при сбое компонента служба, предоставляемая этим сервером, становится недоступной. Это известно как единственная точка отказа. Та же проблема относится и к сетевым устройствам, которые ретранслируют трафик.

Другая проблема заключалась в том, что выделенные серверы использовались недостаточно часто. Выделенные серверы часто простаивали в течение длительных периодов времени, ожидая, пока не возникнет необходимость в предоставлении конкретной услуги, которую они предоставляют. Эти серверы тратили впустую энергию и занимали больше места, чем требовал объем их обслуживания. Это известно как разрастание сервера.

Виртуализация сетевых узлов использует преимущества незанятых ресурсов и объединяет количество необходимых серверов и сетевых устройств. Это также позволяет нескольким операционным системам существовать на одной аппаратной платформе. Кроме того, становится возможным сбалансировать нагрузку.

Например, предположим, что Server1 на рисунке 1.4 испытывает нехватку ресурсов. Чтобы предоставить больше доступных ресурсов, консоль управления перемещает экземпляр Windows в гипервизор на сервере 2.

Нет никакой концептуальной разницы между запуском сетевого узла и запуском виртуальной машины. Сетевые подключения могут быть виртуализированы на уровне программных связей между операционными средами на уровне гипервизора.

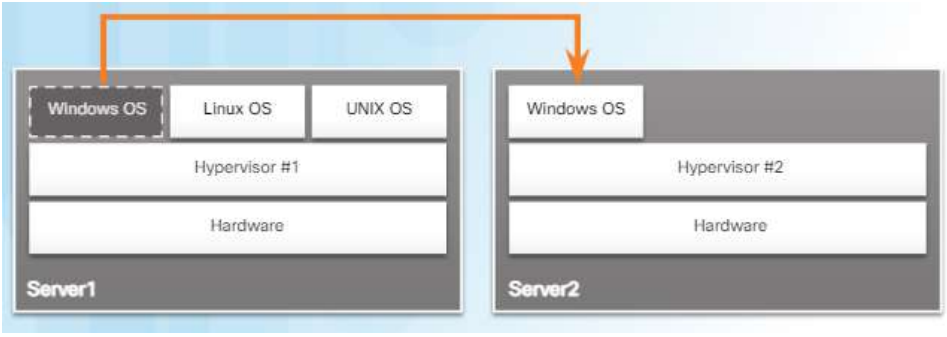


Рисунок 1.4 - Перемещение виртуального сервера Windows

1.3 Организация вычислительного процесса в сетевой структуре

Вычислительные процессы в цифровых сетях можно разделить на три класса: централизованные, децентрализованные и распределенные. Основное различие между централизованной и децентрализованной моделью заключается в распределении функций между сторонами. На рисунке 1.5 показаны некоторые возможные варианты архитектур программных систем с "тонкими клиентами" разного уровня "толщины".

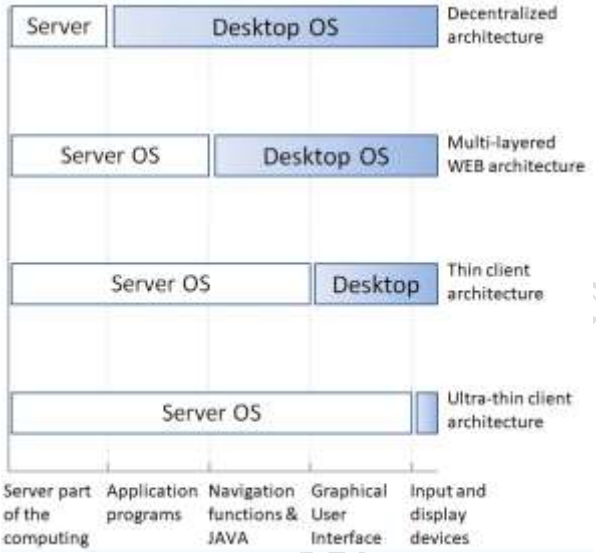


Рисунок 1.5 - Четыре уровня толщины "тонкого клиента"

Многоуровневая веб-архитектура, тонкий клиент и ультратонкий клиент являются примерами модели централизованного обслуживания. Ультратонкий клиент (терминал) может отображать только растровое изображение и передавать информацию с устройств ввода на сервер. Оконная система реализована с использованием ресурсов сервера, к которому подключены терминалы. Эта архитектура создает большую нагрузку на серверный процессор, что ограничивает количество одновременных клиентов. Чтобы снизить нагрузку на сервер, запросы от терминалов группируются и обрабатываются параллельно. Тонкие клиенты - это устройства, способные поддерживать оконную систему (например, X-Window). В этом случае объем информации, передаваемой клиенту, значительно сокращается по сравнению с предыдущей архитектурой. На следующем уровне расположены Java-станции, которые сочетают в себе интерфейс веб-браузера с возможностью загрузки и запуска Java-апплетов и автономных Java-приложений. Это добавляет к функциям ввода-вывода возможность загружать программы по сети и выполнять их локально (на клиенте). Перераспределение клиентских функций в любой из рассмотренных архитектур увеличивает сетевой трафик и нагрузку на ресурсы сервера. Решение этой проблемы было найдено в использовании специализированных устройств для типичных сетевых сервисов и подходе этих устройств к клиентам (рисунок 1.6). Современное сетевое оборудование может быть использовано для выполнения функций обработки программных систем.

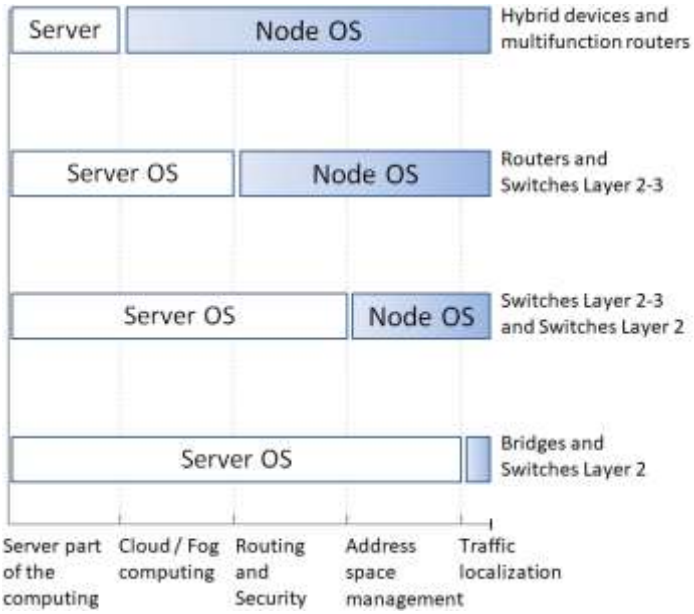


Рисунок 1.6 - Четыре уровня перераспределения функций сервера

Количество протокольных и прикладных функций, которые можно портировать на сетевые устройства, во многом зависит от поддержки встроенных операционных системам выбранных устройств требуемых протоколов и сетевых сервисов, а также количества свободных ресурсов (ЦП, ОЗУ и др.). Эта модель перераспределения ресурсов относится к технологии туманных вычислений.

Туманные вычисления - это децентрализованная вычислительная инфраструктура, в которой данные, вычисления, хранилище и приложения расположены где-то между источником данных и облаком. Как и пограничные вычисления, туманные вычисления приближают преимущества и возможности облака к месту создания данных и их обработки.

1.4 Структура сетевой среды туманных вычислений

Туманные вычисления являются частью инфраструктуры распределенных вычислений для модели сети IoT, которая определяет изолированный сегмент, расположенный ближе к периметру сети относительно устройства IoT. Это позволяет устройствам получать доступ к данным, запускать приложения и принимать немедленные решения. Данные не нужно отправлять через сетевые подключения в режиме онлайн. Предусмотрена возможность их промежуточного накопления и первичной переработки. Устройства IoT способны работать при потере сетевых соединений, что повышает отказоустойчивость. Конфиденциальные данные хранятся в границах, где они необходимы, что повышает уровень безопасности (рисунок 1.7).

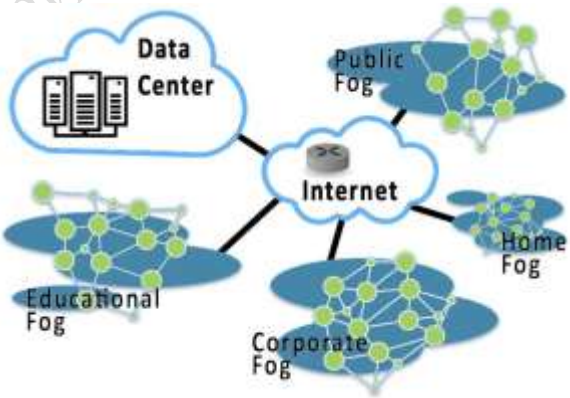


Рисунок 1.7 - Сетевая модель туманных вычислений

Для обеспечения работоспособности системы необходимо использовать компоненты платформы поддержки приложений, которые реализуют инфраструктуру для размещения приложений, первичных банков данных и обеспечения мобильности приложений между облачными средами и средами туманных вычислений.

Устройства, обеспечивающие как кабельное, так и беспроводное подключение к сетевой среде устройств IoT, являются естественными посредниками.

Операционная система такого сетевого устройства должна обладать высоким уровнем универсальности, поскольку ее вычислительная мощность обеспечивает замену функциональности, вынесенной за пределы IoT-устройств. Например, Cisco IOx - это программное решение Cisco для своих устройств, которое сочетает в себе функции Cisco IOS и Linux, что позволяет маршрутизаторам размещать приложения рядом с объектами, которыми эти приложения управляют и которые необходимо отслеживать, анализировать и оптимизировать (рисунок 1.8).

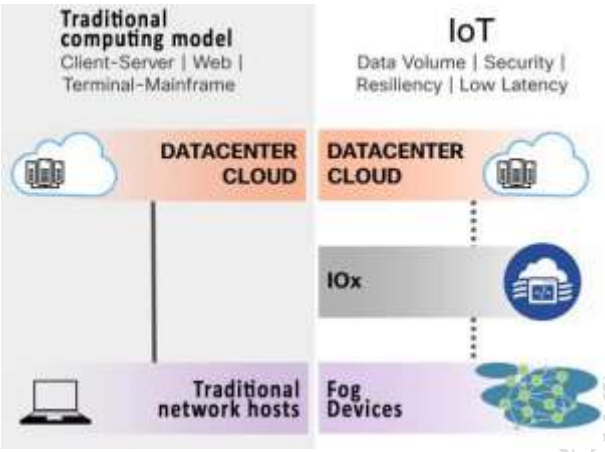


Рисунок 1.8 - Изменение границ действий запросов в туманных вычислениях IoT

Количество протокольных и прикладных функций, которые можно портировать на сетевые устройства, во многом зависит от поддержки встроенными операционными системами выбранных устройств требуемых протоколов и сетевых сервисов, а также количества свободных ресурсов (ЦП, ОЗУ и др.).

1.5 Программно определяемая сетевая архитектура

Предполагается, что при решении практических задач количество IoT-устройств и объем их трафика превышают ресурсные возможности каналов связи на пути: сетевой периметр - облачный сервер. При этом количество этих устройств динамически изменяется как в большую, так и в меньшую сторону в зависимости от потребностей решаемой задачи. Следовательно, настройки устройств сетевого подключения должны динамически изменяться, что позволяет объединять подмножества IoT-устройств в единый сегмент сети или удалять их из этого сегмента. Чтобы сеть обладала этими свойствами, используется программно-определяемая сетевая архитектура.

Программно-определяемая сеть - это сеть передачи данных, в которой уровень управления сетью отделен от устройств передачи данных и реализуется программным обеспечением. Формально это один из способов виртуализации вычислительных ресурсов, позволяющий более гибко решать вопрос ограничения доступа к физической среде передачи данных.

Централизованное управление несколькими сетевыми устройствами снижает вероятность ошибки при назначении доступа и сокращает время обслуживания сети в случае изменения политик безопасности или протоколов связи. Архитектура SDN разграничивает целевой и управляющий потоки данных, возникающие на уровне передачи данных, уровне управления и уровне приложений (рисунок 1.9).

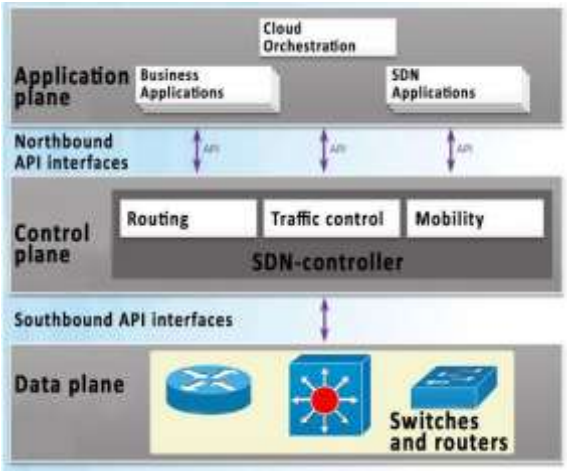


Рисунок 1.9 - Трехуровневая модель архитектуры SDN

Локализация трафика в плоскости данных позволяет высвободить ресурсную мощность ЦП сетевого устройства для организации централизованного управления, согласования режимов совместной работы или решения смежных задач, что и является целью плоскости управления.

Точка принятия решения об авторизации доступа терминального оборудования к физическому интерфейсу и присвоении характеристик организуемому каналу связи фактически передается на сторону сервера или ближайшего программного контроллера. Например, таким контроллером может стать Cloud-Fog Middleware.

Промежуточное ПО Cloud-Fog развернуто в облаке и выступает в качестве промежуточного ПО между облаком и туманностью, то есть набором узлов управления туманом. Он обрабатывает задачи выделения ресурсов, задачи размещения запросов и передает задачи в конкретную туманность для выполнения. Запросы с задачами, обрабатываемыми в облаке, являются независимыми от задержки задачами, запрашиваемыми из соседних туманностей. Эти задачи могут быть ресурсоемкими (например, анализ больших данных или обработка изображений) и, следовательно, должны выполняться в облаке с практически бесконечными ресурсами.

1.6 Определение границ облачной среды

Иерархическая архитектура службы приложений позволяет комбинировать аппаратные решения, программные интерфейсы обслуживания клиентов (приложения) и программно реализованные (виртуализированные) сетевые службы для повышения эффективности обслуживания конечного оборудования.

Архитектура, состоящая из контроллера туманности (Плоскость управления, уровень 1) и многоуровневых узлов тумана (Плоскость управления, уровни 2, 3 и 4), показана на рисунке 1.10. Уровни работают вместе, чтобы обеспечить миграцию услуг для перераспределения трафика с поддержкой QoE. В такой архитектуре мы рассматриваем полностью подключенный и полностью туманный сценарий, где узлы тумана иерархически организованы для предоставления видеоуслуг конечным пользователям.

В примере используются широко распространенные локальные узлы тумана. Это мобильные устройства (Плоскость управления, уровень 4), где такой туманный узел передает видеоконтент по беспроводной сети от устройства к устройству (Интерфейс D2D) для мобильных устройств с высокими и схожими требованиями к трафику друг с другом для создания сети D2D.

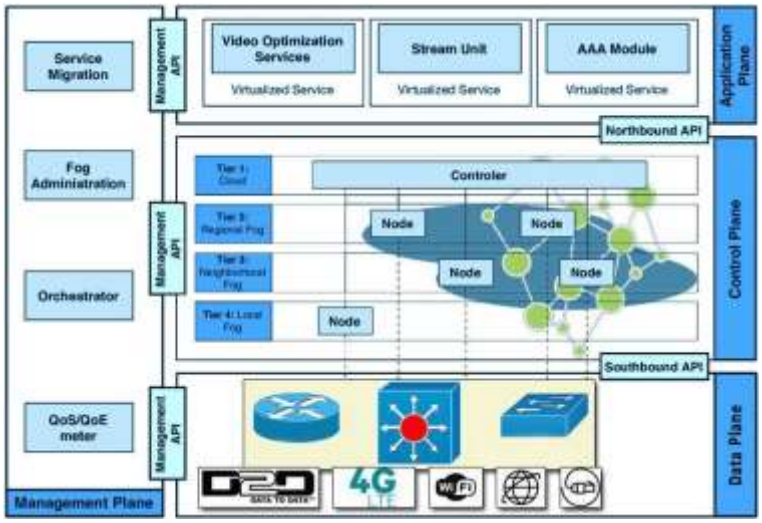


Рисунок 1.10 - Многоуровневая архитектура туманных вычислений

Соседний узел тумана, например, базовая станция или точка доступа (Плоскость управления, уровень 3), поддерживает от нескольких десятков до нескольких сотен локальных узлов тумана. Над ними должен располагаться региональный туманный узел, например, блок основной полосы частот или Интернет-провайдер (Плоскость управления, уровень 2), который управляет координацией по всему городу. Облако или подключение к нему (Control Plane, уровень 1) является вершиной такой многоуровневой архитектуры.

2 Модели описания сетевого взаимодействия

2.1 Классификация сетевых архитектур

Общий рынок сетевых структур весьма разнообразен. Для их описания применяются группы и комбинации критериев (признаков) классификации. Среди наиболее крупных групп можно выделить: Глобальные признаки классификации. Технические признаки классификации. Признаки классификации на основе пользовательских данных.

Например, в качестве комбинированного классификатора, учитывающего размер сети, функциональные возможности и подчиненность управляющей организации, сети делят на PAN, LAN, MAN, WAN. В рамках расширения данного классификатора применяются понятия *частные сети (Private Network, PN), домашние сети (Home Network, HN), сети масштаба кампуса (Campus Area Network, CAN), беспроводныее сети (Wireless LAN, WLAN), корпоративные сети (Enterprise Wide Networks, EWN) и глобальные сети (Global Area Network, GAN).* Пример соотношения некоторых из этих сетей показаны на рисунке 2.1.

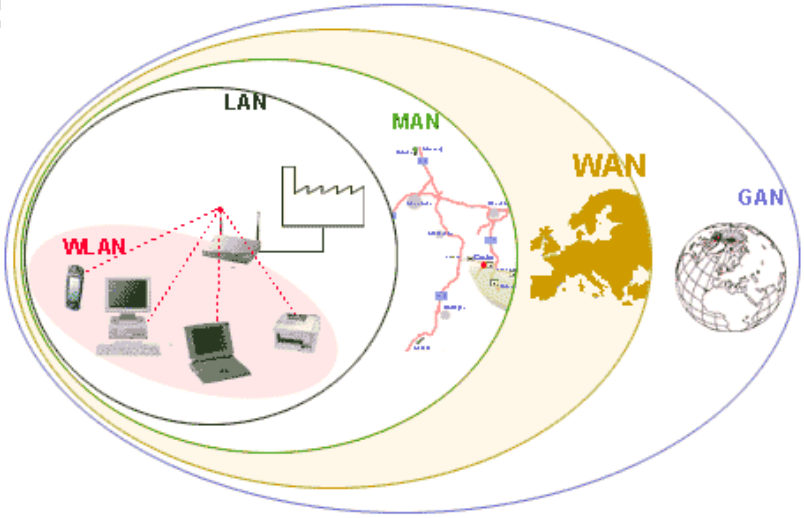


Рисунок 2.1 – Пример классификатора сети по размеру и функционалу

Личная или Персональная вычислительная сеть (*Personal Area Network, PAN*) – это структура, объединяющая вычислительные системы и гаджеты, сосредоточенные на весьма ограниченной территории. Обычно радиус удаления не превышает 10 м. В общем случае персональная сеть представляет собой коммуникационную систему, ориентированную на реализацию сервисов для одного или небольшой группы пользователей.

Персональные сети (рисунок 2.2) могут быть беспроводными (WPAN) или сконструированы с помощью кабелей. USB и FireWire часто соединяют проводную PAN, в то время как WPAN обычно используют WiFi, Bluetooth (piconets) или инфракрасные соединения (IrDa).

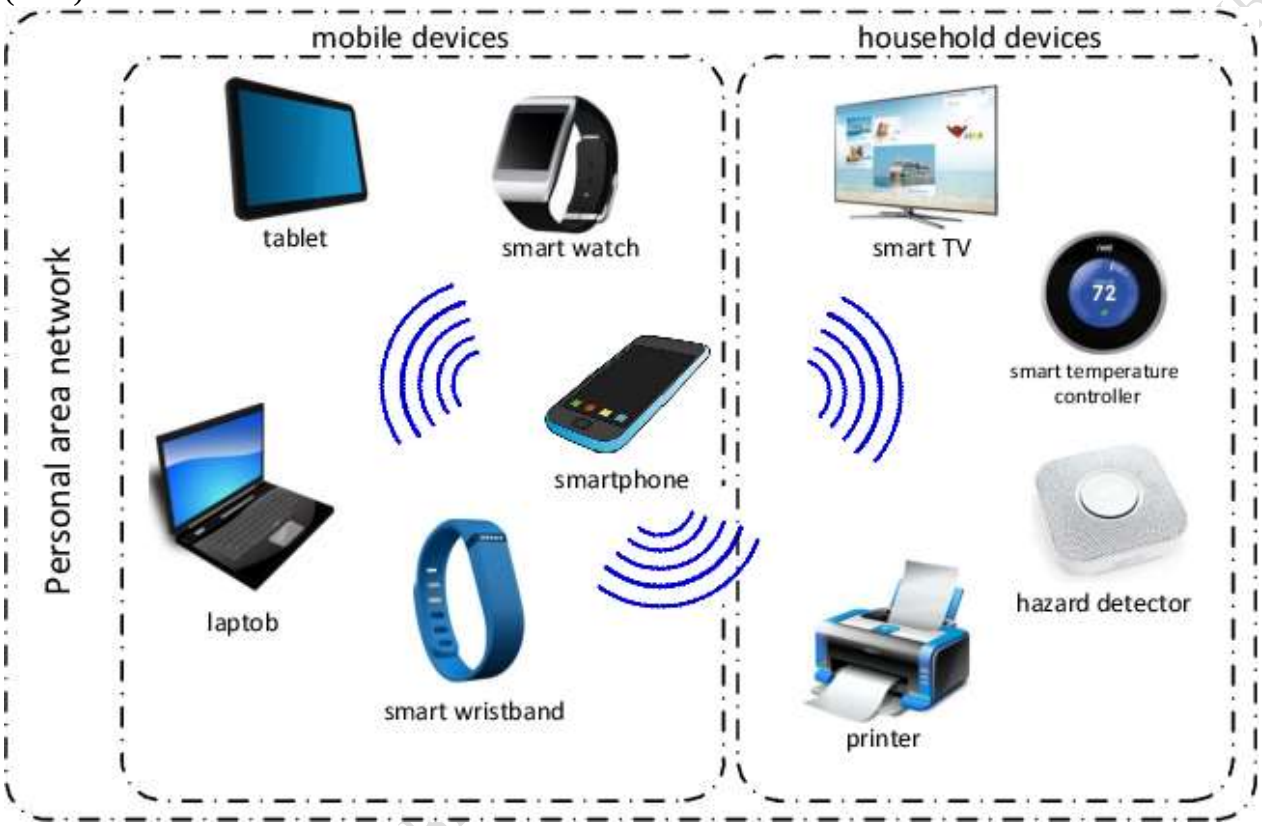


Рисунок 2.2 – Пример постоения Personal Area Network

Как правило, персональные сети не проектируются заранее. Состав устройств сети может динамически расширятся и сжиматься в зависимости от возможности обеспечивать стабильную связь ее участников.

Локальная вычислительная сеть (*Local Area Network, LAN, ЛВС*) – это структура, объединяющая вычислительные системы и их автономные части, сосредоточенные на небольшой территории. Обычно радиус удаления не превышает 1–2 км, хотя в отдельных случаях локальная сеть может иметь и более протяженные размеры. В общем случае локальная сеть представляет собой коммуникационную систему, принадлежащую одной организации.

Функциональное назначение сети, или спектр решаемых ею задач, узко направлено. Например, использование файлов, хранящихся на дисках других компьютеров сети, совместное использование устройств печати, модемов, факсов, доступ к единым базам данных, внутренняя электронная почта и др.

Локальная сеть может применяться для управления производственным процессом конкретного предприятия. Причем эти задачи могут начинаться с обычного документооборота и заканчиваться удаленным управлением любыми технологическими процессами.

Более сложные задачи предъявляют высокие требования к надежности процесса передачи информации. Например, такая функция, как распределенная обработка данных, требует наличия механизма установления однозначной последовательности выполняемых действий, т. е. необходимо решение задачи синхронизации в распределенной системе, что далеко не просто.

Однако, большинство локальных сетей ориентированы на решение простых пользовательских задач. В таких случаях каждая рабочая станция или узел сети, как правило, автономно обладает необходимыми ресурсами для решения поставленных перед нею задач, а ресурсы локальной сети необходимы для получения задания и отправки результатов, хранения больших объемов данных, совместного использования дорогостоящих устройств. Классическая схема локальной сети приведена на рисунке 2.3.

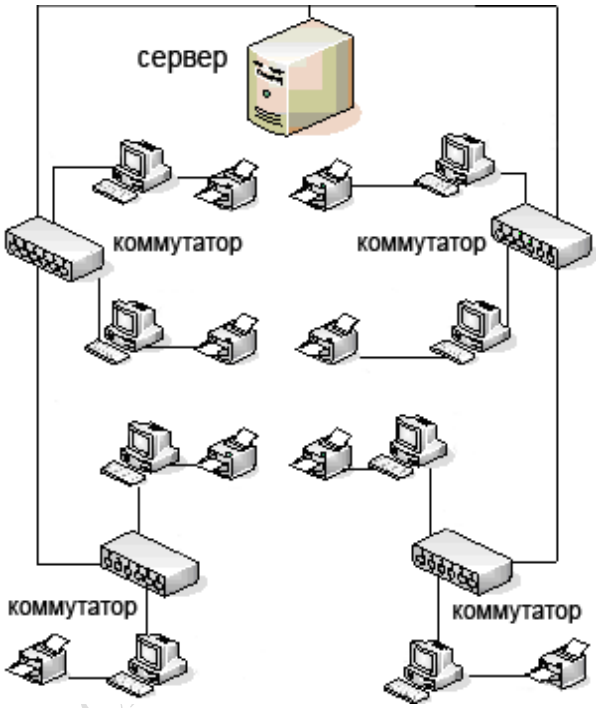


Рисунок 2.3 – Пример схемы локальной вычислительной сети

Примерный жизненный цикл локальной сети можно разбить на шесть этапов (таблица 1.1), каждый из которых включает в себя набор инженерных задач. Этапы 3–5 этого цикла должны регулярно повторяться. В противном случае либо сеть перестанет соответствовать современным стандартам, либо начнется процесс ее саморазрушения.

Местная, региональная, муниципальная или городская сеть (*Metropolitan Area Network, MAN*) – это структура, объединяющая вычислительные системы, рассредоточенные по территории одного региона, включающего в себя общие объекты или субъекты управления.

Такие крупные системы практически невозможно разработать и внедрить одному собственнику, тем более, что их окупаемость достаточно невелика. Сети MAN решают задачи управления хозяйством и организации услуг. К их числу можно отнести: расписание движения общественного транспорта, управление рынком вакансий, функцию информирования населения, Internet–магазины и т. п.

Современная сеть MAN охватывает территорию диаметром около 40–50 км, обладает двумя или более маршрутами доставки сообщения между узлами сети, применяет широкий спектр современного коммуникационного оборудования.

Таблица 1.1 – Примерный жизненный цикл локальной сети

№	Этап	Содержание работ по этапу
1	Разработка проекта	− предпроектное обследование объекта; − составление, оформление и согласование технического задания; − выбор необходимой конфигурации серверов и рабочих мест для использования их в составе информационной системы компьютерной сети; − выбор необходимого сетевого оборудования; − подготовка полного проекта сети в соответствии с требованиями заказчика.
2	Монтаж	− выполнение проекта, монтаж структурированной кабельной системы; − установка и настройка активного сетевого оборудования; − установка и настройка сетевого программного обеспечения на серверы и рабочие места; − установка систем защиты информации от несанкционированного доступа.
3	Тестирование	− проведение анализа работы сети для определения «узких мест» и их устранение; − анализ информационной безопасности сети; − проверка систем защиты информации от несанкционированного доступа; − проверка работы активного сетевого оборудования.
4	Обслуживание	− построение систем резервного копирования информационных ресурсов предприятия; − формирование политики безопасности предприятия, реализация систем разграничения доступа к информационным ресурсам; − проведение обучения персонала по использованию локальной сети на рабочих местах; − гарантийное и послегарантийное обслуживание элементов сети.
5	Модернизация	− установка сетевых операционных систем нового поколения; − установка дополнительного прикладного программного обеспечения; − установка дополнительных или более новых версий систем управления и мониторинга сетей; − обновление системы защиты информации от несанкционированного доступа; − расширение возможностей использования современных технологий, в частности, системы электронного документооборота, сетевых баз данных, приема/переачи сообщений, доступа в Internet.
6	Демонтаж	− уведомление пользователей с последующим отключением их от сети; − отключение доступа к сетевым ресурсам; − демонтаж и утилизация активного оборудования; − демонтаж и утилизация элементов структурированной кабельной системы.

Можно утверждать, что чаще всего сети MAN – это пример сообщества, состоящего из более мелких сетей: локальных, частных, домашних, а также вычислительных систем отдельных пользователей. Способы их объединения могут быть различными, основываться на применении различных типов передающих сред и иметь различные источники финансирования. Тем не менее, мотив объединения всегда один – ускорение и удешевление информационного обмена и доступа к сетевым услугам.

К числу популярных пользовательских сервисов (кроме упомянутых ранее), которые можно организовать только в сетях такого масштаба, можно добавить следующие: организация оперативного документооборота между предприятиями, организациями и частными лицами; организация безналичного расчета посредством использования кредитных карт; наконец, желание пользователей получить доступ к сфере развлечения, в том числе цифровому телевидению и компьютерным играм.

Следует заметить, что качество и количество технологий, применяемых для организации связи между сетями, непрерывно растет. Одновременно меняются требования к надежности и безопасности передаваемой информации. Таким образом, сети MAN сегодняшнего дня сильно отличаются от своих предшественников.

Самым распространенным примером муниципальной сети являются системы кабельного телевидения. Они стали правопреемниками эфирных телесетей в тех местах, где качество передачи сигнала посредством радиосигнала было слишком низким.

Вначале стали появляться специализированные, разработанные прямо на объектах сетевые структуры. Затем компании-разработчики занялись продвижением своих систем на рынок, начали заключать договора с городскими органами управления и в итоге охватили целые территории. Следующим шагом стало создание телевизионных программ и даже целых каналов, предназначенных только для кабельного телевидения.

Когда Internet стал привлекать к себе массовую аудиторию, операторы кабельного телевидения поняли, что, внеся небольшие изменения в систему, можно сделать так, чтобы по тем же каналам в неиспользуемой части спектра передавались (причем в обе стороны) цифровые данные. С этого момента кабельное телевидение стало постепенно превращаться в муниципальную компьютерную сеть. В первом приближении систему MAN можно представить себе такой, как она изображена на рисунке 2.4. На этом рисунке видно, что по одним и тем же линиям передается и телевизионный, и цифровой сигналы.

Поскольку городская территория разделяется на сферы обслуживания между несколькими провайдерами – большую роль в организации согласованной работы сети MAN играют органы местного управления.

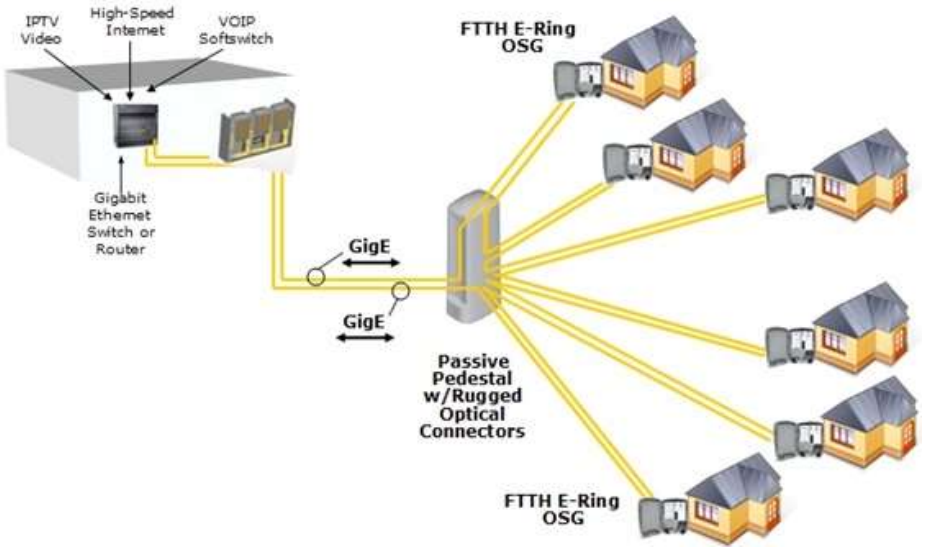


Рисунок 2.4 – Муниципальная сеть на базе оптоволоконной системы

Глобальная вычислительная сеть (*Global/World Area Network, GAN/WAN*) – охватывает максимальную территорию. Теоретически эта сеть может объединить все вычислительные системы на земном шаре для решения одной общей задачи. При этом созданные системы управления такой сетью уже сама по себе весьма сложная задача.

По этому признаку глобальные сети можно разделить на распределенные и централизованные. Централизованные лучше защищены от несанкционированных акций, распределенные же отличаются большей надежностью при передаче данных, а также большей живучестью.

Глобальные сети решают задачи управления хозяйством в наиболее крупном размере, например, расписание движения международного транспорта, предварительный заказ билетов, бронирование мест в гостиницах, Internet-магазины и т. п. (рисунок 2.5).

Свойства глобальных сетей удобнее рассматривать в сравнении их с локальными вычислительными сетями:

- *по протяженности и качеству линий связи* локальные сети, по определению, отличаются от глобальных небольшими расстояниями между узлами сети. Это в принципе делает возможным использование в локальных сетях более качественных и более дорогих линий связи;

- *по сложности методов передачи данных* в условиях низкой надежности физических каналов в глобальных сетях требуются более сложные, чем в локальных сетях методы передачи данных и соответствующее оборудование. Считается, что в глобальных сетях соединения не могут быть постоянными. Нередко используются коммутируемые соединения, да и другие виды соединений ориентированы на временный характер;

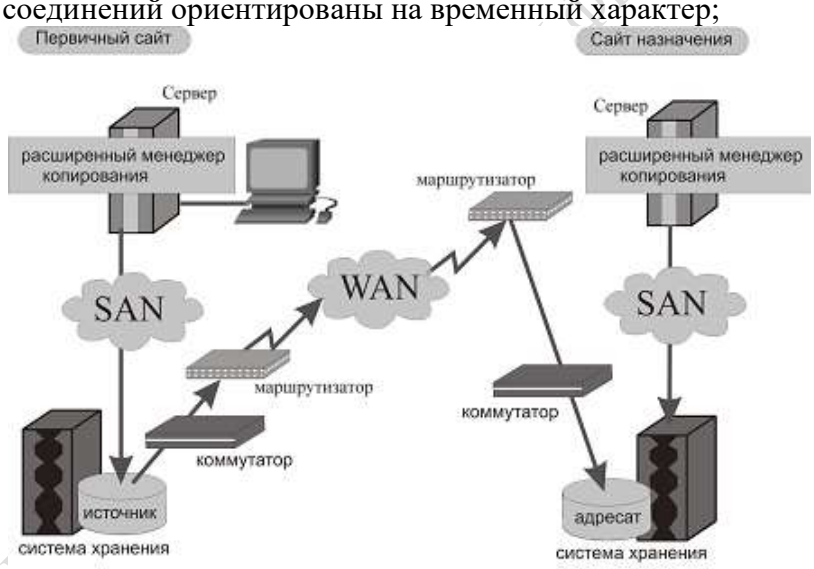


Рисунок 2.5 – Обмен данными между сетями SAN через структуру WAN

- *число информационных ресурсов* в глобальных сетях значительно больше;

- *скорость обмена данными* в локальных сетях, существенно выше, чем в глобальных;

- высокие скорости обмена данными позволяют предоставлять пользователю в локальных сетях более *широкий* спектр *услуг*.

Примеры технических признаков классификации:

− *сети на основе каналов кабельного телевидения* – доставка информации конечному пользователю производится так же, как и доставка телевизионного сигнала (рисунок 2.6). Адаптер пользователя декодирует смешанный сигнал, выделяет информационную составляющую, транслируемую как обычный телевизионный канал посредством *мультиплексирования*. Примеры технологии – сети *Community Antenna TeleVision (CATV), Gigabit Passive Optical Network (GPON)*;

− *сети на основе систем энергоснабжения* – система доставки информации по существующей инфраструктуре (рисунок 2.7). Поскольку электросеть проникает в каждую

комнату любого дома, то компьютер пользователя получает достаточный уровень мобильности. Для передачи сигнала через электросеть используется мультиплексирование OFDM;

− *сети сотовых операторов* – сотовые системы используют три различных метода мультиплексирования голосовых и информационных данных на арендуемом диапазоне радиочастот: FDMA, TDMA и CDMA;

− *хаотически возникшие пользовательские сетевые сегменты* на базе технологий локальных вычислительных сетей.

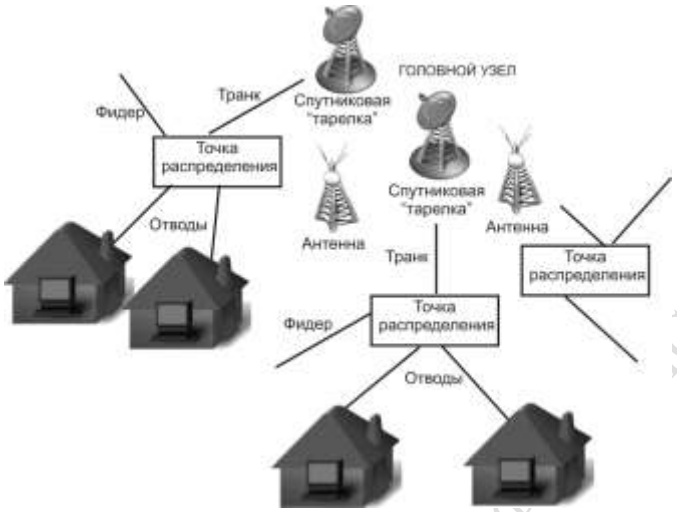


Рисунок 2.6 – Сеть каналов частной беспроводной сети

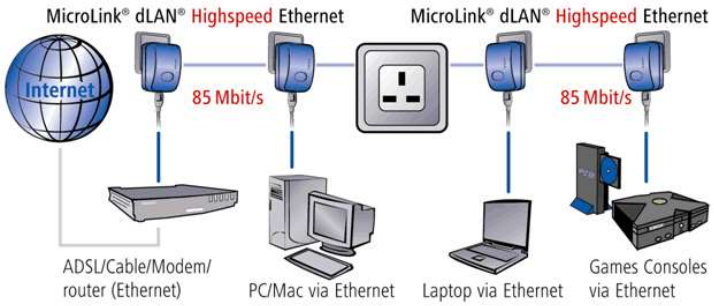


Рисунок 2.7 – Пример сети на основе системы энергоснабжения

Еще одним распространенным примером классификатора является оценка принадлежности трафика к внутрисетевому/внешнесетевому типу. Вся сеть делятся на три части (рисунок 2.8).

Внутренняя сеть (Intranet) - это частная совокупность локальных и глобальных сетей внутри организации, которая доступна только для членов организации или других лиц с надлежащими полномочиями.

Организация может использовать *внешнюю часть сети организации (Extranet)* для обеспечения защищенного доступа к сети для сотрудников, работающих в других организациях, которым необходим доступ к данным в своей сети. К этому сегменту сети часто применяют термин DMZ. В качестве оператора такой сети может выступать провайдер (ISP), которому можно передать часть функций информационной безопасности. Или, например, организация обеспечивающая сервис внешнего центра обработки данных (ЦОД, NOC).

Внешняя публичная сеть (Internet) – это публичная совокупность глобальных сетей MAN и WAN, которая доступна всем пользователям.

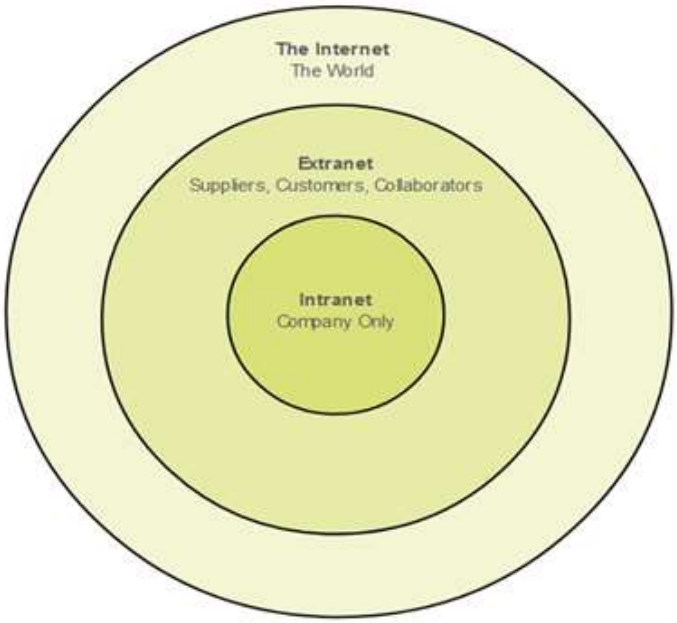


Рисунок 2.8 – Пример классификатора по типу принадлежности трафика

2.2 Формализация описания сетевого взаимодействии

Люди должны использовать установленные правила или соглашения, регулирующие разговор, при этом у носителя языка могут встречаться в речи весьма сильные отклонения, которые его собеседник сможет или не сможет распознать. Таким образом, часть информационного сообщения может быть потеряна. Такие примеры отклонений в использовании правил речи довольно часто встречаются и в письменных текстах (рисунок 2.9).

94НН03 С006Щ3НN3 ПОК43Ы8437, К4КN3
У9N8N73ЛЬНЫ3 83ЩN МОЖ37 93Л47Ь
Н4Ш Р43УМ! 8П3Ч47ЛЯЮЩN3 83ЩN!
СН4Ч4Л4 Э70 6ЫЛО 7РУ9НО, НО С3Й Ч4С
Н4 Э70Й С7РОК3 84Ш Р43УМ ЧN7437 Э70
4870М47NЧ3СКN, Н3 349УМЫ84ЯСЬ 06
Э70М.

Рисунок 2.9 – Пример нарушения правил написания текста

Набор правил при организации сеанса связи между вычислительными системами требует точного выполнения. Любое отклонение или задержка приводит к потере данных, повторной передаче и, как следствие, снижению скорости информационного обмена. Сетевое взаимодействие между устройствами можно разделить на ряд последовательных шагов. Пример такого разделения представлен на рисунке 2.10.

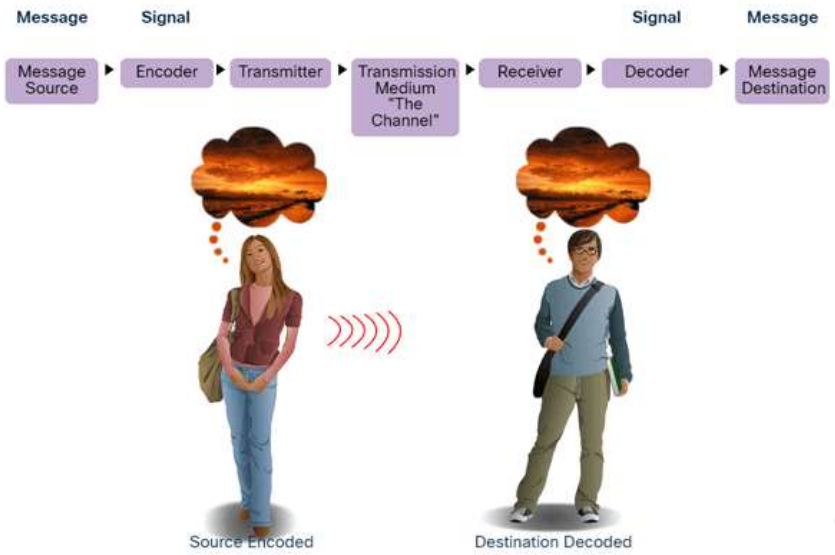


Рисунок 2.10 – Пример формального описания передачи информации

Кодирование - это процесс преобразования информации в форму, приемлемую для последующей передачи.

Декодирование - обратный процесс, в результате которого информация преобразуется в исходный вид.

Кодировка данных при обмене между узлами должна быть в формате, соответствующем каналу связи, сетевому стандарту и программному средству подключения. Сообщения, отправленные по сети, преобразуются битовые блоки. Битовые блоки кодируются в виде световых, звуковых или электрических импульсов. Конечный хост декодирует сигналы и интерпретирует их в сообщение.

2.3 Теоретические модели ISO/OSI и TCP/IP

Сетевая модель – теоретическое описание принципов работы набора сетевых протоколов, взаимодействующих друг с другом.

Применение сетевых моделей позволяет решать следующий ряд вопросов:

− обеспечение передачи информации между различными типами локальных и глобальных сетей;

− стандартизация сетевого оборудования, что позволяет устройствам одного производителя взаимодействовать с устройствами других производителей;

− сохранение капиталовложений пользователей за счет обеспечения возможности взаимодействия старого сетевого оборудования с новыми устройствами;

− разработка программного и аппаратного обеспечения, использующего общие интерфейсы для передачи как внутри сети, так и между различными сетями.

Чаще других применяется модель OSI, разработанная в 1974 году Международной организацией стандартизации ISO. Модель OSI состоит из семи уровней, расположенных один поверх другого: *физического, канального, сетевого, транспортного, сеансового, представительского, прикладного*. Передача информации начинается на прикладном уровне. Затем информация претерпевает ряд преобразований и определенных приращений на более нижних уровнях до тех пор, пока данные не достигнут физического уровня и не будут по сети переданы второму участнику соединения – приемнику.

Взаимодействие между уровнями OSI изображено на рисунке 2.11.

Рисунок 2.11 – Модель взаимодействия уровней в OSI

Модель DoD разрабатывалась вместе с протоколом TCP/IP как часть проекта ARPAnet. Это достаточно простая модель. Она содержит всего четыре уровня (рисунок 2.12).

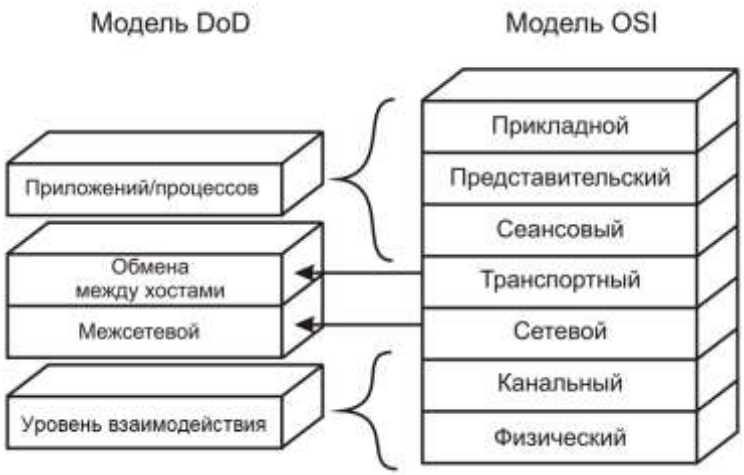


Рисунок 2.12 – Соответствие уровней модели DoD уровням модели OSI

Уровни модели DoD выполняют описанные ниже функции:

− *уровень приложений/процессов* – верхний уровень модели DoD выполняет функции трех верхних уровней модели OSI: прикладного, представления и сеансового. В источниках по TCP/IP можно встретить утверждение, что уровень приложений шифрует данные, создает точки проверки и управляет сеансом связи;

− *уровень взаимодействия* – во многих источниках, включая четырехуровневые диаграммы DoD, этот уровень называется так же, как соответствующий ему уровень модели OSI - транспортный;

− *межсетевой уровень* – этот уровень довольно точно соответствует сетевому уровню модели OSI. На межсетевом уровне выполняется маршрутизация сигнала на основе логических цифровых адресов;

− уровень сетевого интерфейса – этот уровень выполняет функции канального и транспортного уровней модели OSI.

Далее в тексте пособия будут использоваться обе эти модели при описании свойств оборудования и программных систем, участвующих в сетевом обмене.

2.4 Понятие и свойства сетевых протоколов

Протоколы (*protocols*) – это набор правил и процедур, регулирующих порядок реализации некоторой связи. В компьютерной среде протоколы – это правила и технические процедуры, позволяющие нескольким компьютерам, объединенным в сеть, общаться друг с другом.

Сетевые устройства используют согласованные протоколы для связи. Протоколы могут иметь одну или несколько функций. Иерархически организованный набор разноуровневых протоколов, достаточный для организации полноценного взаимодействия узлов в сети, называется *стеком протоколов*.

Многие стеки протоколов разрабатывались задолго до того, как стала широко использоваться модель OSI, поэтому на программном уровне они более соответствуют модели DoD (рисунок 2.13).

Модель DOD	Протокол TCP/IP			
Уровень процессов/приложений	Telnet	FTP	LDP	SNMP
	TFTP	SMTP	NFS	POP
Уровень взаимодействия	TCP		UDP	
Межсетевой уровень	ICMP	BootP	ARP	RARP
	IP			
Уровень сетевого интерфейса	Ethernet	FTTH	FDDI	другие стандарты

Рисунок 2.13 – Соответствие протоколов стека TCP/IP уровням модели DoD

Передача данных по сети разбита на ряд последовательных действий, каждому из которых соответствуют свои правила и процедуры, составляющие протокол. В обязательном порядке сохраняется очередность их выполнения: на компьютере-отправителе – в направлении сверху вниз, а на компьютере-получателе – снизу вверх.

Протоколы могут быть двух типов: низкоуровневые и высокоуровневые:

– низкоуровневые протоколы появились достаточно давно и с тех пор не претерпели никаких кардинальных изменений. За длительное время использования таких протоколов в них были найдены и устранены все возможные «дыры» и ошибки.

– что касается высокоуровневых протоколов, то они постоянно разрабатываются и совершенствуются.

Стандарты низкоуровневых протоколов как видно из рисунка 2.13 (уровень сетевого интерфейса) могут быть жестко связаны со стандартами на оборудование, для которых действуют спецификации IEEE 802. Примерами низкоуровневых протоколов (межсетевого уровня на рисунке 2.13) являются ICMP, BootP, ARP, RARP, IP, а также драйвера сетевых устройств, оболочка NDIS и другие протоколы такого же уровня из других стеков.

Многие авторы описывают протоколы опираясь не на модель DoD, а на модель ISO/OSI. В таблице 2.2 – пример такого описания.

Таблица 2.2 – Примеры функций, выполняемых протоколами

Модель OSI	**Функции**	**Примеры протоколов**
Прикладной уровень	Прикладной уровень отвечает за доступ приложений в сеть. Задачами этого уровня является копирование файлов, обмен почтовыми сообщениями и управление сетью.	FTP - протокол копирования файлов TFTP - упрощенный протокол копирования файлов Telnet - удаленный доступ в сеть SMTP - простой протокол почтового обмена CMIP - общий протокол управления информацией SNMP - простой протокол управления сетью NFS - сетевая файловая система FTAM - метод доступа для копирования файлов
Представительский уровень	Уровень представления отвечает за возможность диалога между приложениями на разных машинах. Этот уровень обеспечивает преобразование данных (кодирование, компрессия и т.п.) прикладного уровня в поток информации для транспортного уровня.	DNS LDAP NetBIOS/IP
Сеансовый уровень	Сеансовый уровень отвечает за организацию и поддержку соединений между сессиями, администрирование и безопасность сети	
Транспортный уровень	Транспортный уровень определяет протоколы обмена сообщениями и обеспечивает сквозное управление протоколом данных через сеть	TCP UDP QUIC
Сетевой уровень	Сетевой уровень отвечает за деление пользователей на группы (адресацию) и управление сетью. На этом уровне происходит маршрутизация пакетов на основе преобразования MAC-адресов в сетевые адреса. Сетевой уровень обеспечивает передачу пакетов на транспортный уровень.	IP - протокол Internet IPX - протокол межсетевого обмена X.25 (частично этот протокол реализован на канальном уровне) CLNP - сетевой протокол без организации соединений
Канальный уровень	Канальный уровень обеспечивает формирование, передачу и прием кадров данных. Этот уровень обслуживает запросы сетевого уровня и использует сервис физического уровня для приема и передачи пакетов.	HDLC для последовательных соединений Ethernet WiFi FDDI PPP
Физический уровень	Физический уровень отвечает за подключение к физической среде передачи (медь, оптика. радио). Этот уровень получает кадры данных от канального уровня и преобразует их в оптические или электрические сигналы, соответствующие значениям битов в потоке данных. Эти сигналы посылаются через среду передачи на приемный узел.	

2.5 Общие положения адресации

Адресация в сети – это процесс, состоящий из нескольких этапов преобразования адресной информации для установления однозначного соответствия адреса приемника приемнику, а адреса источника – источнику. Еще одно название – отображение или разрешение имен. Процесс делится на три этапа, соответствующие трем логическим уровням адресации: прикладному, транспортному и сетевому, что хорошо соотносится с эталонной моделью OSI.

На верхнем уровне адресации используются специальные имена, например, идентификаторы процессов, рабочих станций или символьные доменные имена. Они предназначены для конкретных процессов, программ ими управляющих, а также для пользователей. Дополнительное назначение адресов верхнего уровня – удобство работы программистов и/или пользователей при обращении к сетевым ресурсам, что помогает существенно увеличить скорость при использовании сетевых ресурсов и управлении ими.

Примером могут служить имена NetBIOS в сетях MicroSoft, которые могут включать до 16 символов. Первые 15 символов можно использовать для указания понятного имени компьютера, а шестнадцатый символ зарезервирован для указания службы компьютера, которая передает информацию. Чаще всего NetBIOS-адресация в сетях MicroSoft используется поверх протокола TCP/IP.

Адреса сетевого уровня назначаются и используются операционной системой и программами управления сетевых устройств. Здесь решаются вопросы маршрутизации, что накладывает свои требования на структуру адресных конструкций. У работающей операционной системы может быть один и более сетевых адресов. При этом, если используется несколько интерфейсных карт, то операционная система должна назначить однозначное соответствие каждого сетевого адреса конкретному порту сетевого обмена, например, сетевому адаптеру. Для этого в самой нижней части адресного стека применяются физические адреса устройств (MAC-адреса).

Передача информационных импульсов по любой среде передачи может и должна быть принята любым другим сетевым устройством, которое подключено к этой среде. Таким образом, именно MAC-адреса позволяют перенаправить пакет конкретному сетевому адаптеру или модему, или любому другому активному сетевому оборудованию.

В общем случае к адресу сетевого интерфейса и схеме его назначения можно предъявить несколько требований: адрес должен уникально идентифицировать сетевой интерфейс в сети любого масштаба; схема назначения адресов должна сводить к минимуму ручной труд администратора и вероятность дублирования адресов; желательно, чтобы адрес имел иерархическую структуру, удобную для построения больших сетей; адрес должен быть удобен для пользователей сети, то есть он должен допускать символьное представление; адрес должен быть по возможности компактным, чтобы не перегружать память коммуникационной аппаратуры.

Можно перечислить следующие примеры подходов к решению задачи распределения адресов: уникальные статические адреса; выбор из фиксированного подмножества статических адресов; статические адреса, назначаемые администратором; динамические адресные системы: централизованные; децентрализованные; случайные адресные системы.

Адреса могут использоваться для идентификации:

- отдельных интерфейсов;
- групп интерфейсов;
- сразу всех сетевых интерфейсов сети (широковещательные).

Одна из классических систем адресации сводится к тому, что при установке сети каждому абоненту присваивается индивидуальный адрес по порядку, к примеру, от 0 до 30 или от 0 до 254. Присваивание адресов производится программно или с помощью переключателей на плате адаптера. При этом требуемое количество разрядов адреса определяется из неравенства:

$2^n > N_{max}$,

где n – количество разрядов адреса, а Nmax – максимально возможное количество абонентов в сети. Например, восемь разрядов адреса достаточно для сети из 255 абонентов. Один адрес отводится для широковещательной передачи, то есть он используется для пакетов, адресованных всем абонентам одновременно. К примеру, механизм, аналогичный этому, применяется в сети ArcNet.

При описании общих положений адресации требуется обратить внимание на аппаратную систему адресация информационных потоков:

- кабельная система привязана к инфраструктуре и ее адресация статична. Подключение кабеля к настроенному сетевому интерфейсу определяет трафик, который будет доставляться. Трафик доставляется в полном объеме. Фильтрацией занимаются протоколы L2 и выше;
- порт интерфейса сетевого устройства является управляемой величиной, следовательно, динамически может изменять значение адреса в рамках предопределенного уровня свободы. По сути операционная система сетевого устройства обращается к собственной переменной, которая может быть ассоциирована с физическим сетевым интерфейсом или его виртуальной версией.

Механизмы адресации L2, L3, L4 и *«процес2процесс»* рассматриваются в соответствующих разделах пособия.

3 Среда передачи данных

3.1 Физический уровень ISO/OSI (L1)

Физический уровень (L1) описывает: все физические среды передачи данных (кабель, оптоволокно, радиоволны и др.), сетевые разъемы, компоновку сети, методы передачи и кодирования сигналов, устройства передачи, методы распознавания ошибок при передаче сигналов. Сетевые сигналы могут быть представлены в аналоговом или цифровом (дискретном) виде. Аналоговый сигнал может изменяться непрерывно и выглядит как волна с положительными и отрицательными перепадами напряжения. В дискретной форме для представления единиц и нулей используются различные способы представления сигналов. Некоторые формы представления дискретных сигналов представлены на рисунке 3.1.

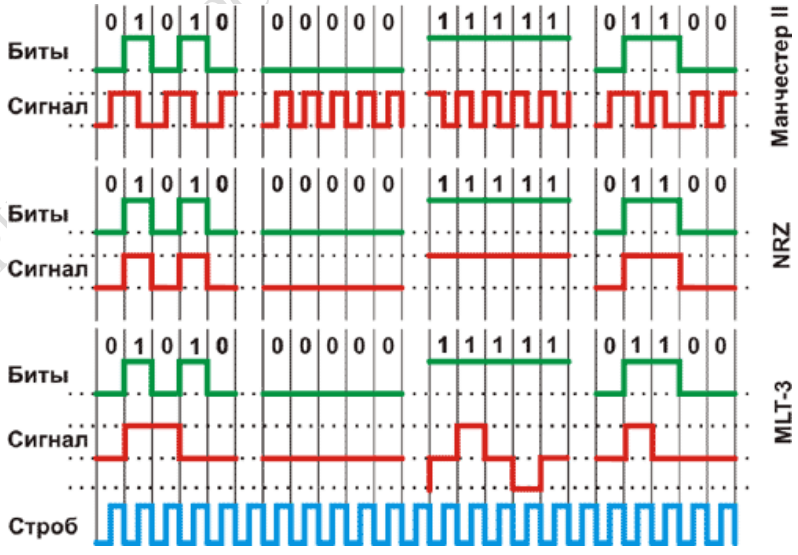


Рисунок 3.1 – Примеры цифровых сигналов

Физический уровень управляет скоростью передачи данных, анализом потока ошибок и уровнями напряжения сигнала. При отсутствии физического соединения работа протоколов уровня L2 и L3 невозможна. Характеристики соединения уровня L1 будут естественным ограничителем для канала связи.

Под средой передачи данных следует понимать набор оборудования, с помощью которого осуществляется взаимодействие между участниками соединения в рамках сеанса связи. В самом простом случае среда передачи реализована в виде кабеля (единственного или в составе группы) и/или задействуются беспроводные технологии.

Для использования кабеля в компьютерной сети должны быть однозначно описаны: тип кабельной системы и ее физические характеристики; формы и уровни информационного сигнала; способы разветвления среды передачи и подключения к ней; требования, выставляемые к сетевому оборудованию.

При использовании беспроводных технологий ограничений и требований еще больше, пколлоскольку каждая из этих сред имеет особые способы кодирования, декодирования и применения сигнала в среде.

Среда передачи может работать в одном из следующих режимов:

Симплексная передача. Однонаправленный канал, сигналы проходят по нему всегда только в одном направлении.

Полудуплексная передача. Сигналы могут передаваться в обоих направлениях по единственному каналу связи, но в каждый момент времени сигналы передаются только в одну сторону.

Дуплексная передача. Данный способ реализует полноценную двустороннюю связь по единственному каналу связи.

Многоканальная передача. Одновременная независимая передача от многих отправителей к такому же числу получателей по общей линии связи.

Свойства среды передачи определяют уровень защиты передаваемых сигналов от помех. Помехи бывают следующих типов:

Электромагнитные помехи представляют собой вторжение постороннего электромагнитного сигнала, нарушающего форму полезного сигнала. В этом случае принимающий компьютер не может правильно интерпретировать сигнал.

Радиочастотные помехи представляют собой сигналы устройств, излучающих сигналы на радиочастотах. Радиочастотным считается электромагнитное излучение на частотах от 10 КГц до 100 ГГц. Излучение от 2 до 10 ГГц называется также микроволновым.

Влияние радиочастотных помех устраняется с помощью помехозащитных фильтров, применяемых в различных типах сетей.

Перекрестные помехи. К этому типу помех относятся сигналы проводов, расположенных на расстоянии нескольких миллиметров друг от друга. Протекающий по проводу электрический ток создает электромагнитное поле, которое генерирует сигналы в другом проводе, расположенном рядом. Довольно часто, разговаривая по телефону, можно услышать приглушенные разговоры других людей. Причиной этого являются перекрестные помехи.

Перекрестные помехи значительно уменьшаются, если скрутить два провода, как это сделано в витой паре. Чем больше витков приходится на единицу длины, тем меньше влияние помех.

Затухание сигналов. Проходя по кабелю, электрические и оптические сигналы становятся все слабее. Чем больше расстояние до источника, тем слабее сигнал. Такое ослабление сигнала с расстоянием называется затуханием сигнала. Затухание является причиной того, что в спецификациях различных сетевых архитектур указывается ограничение на длину кабеля. Если это ограничение соблюдается, то эффект затухания не повлияет на нормальную работу канала связи.

Различные среды передачи данных имеют различные допуски по диапазону рабочих частот и скорости затухания сигнала (рисунок 3.1).

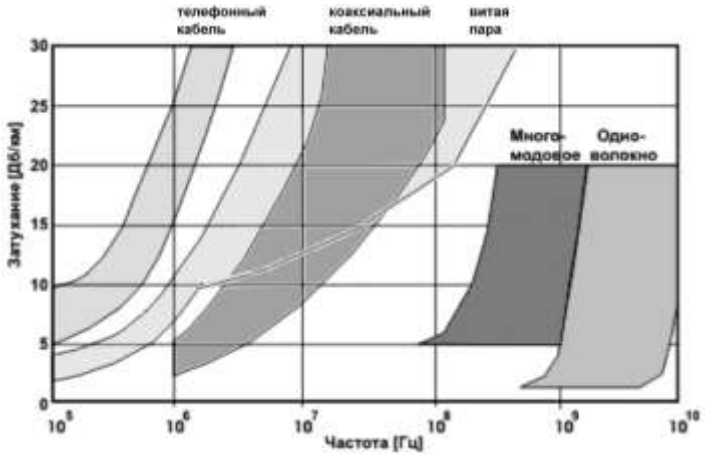


Рисунок 3.1 – Характеристики кабельных сред передачи данных

При увеличении частоты затухание увеличивается, потому что, чем выше частота сигнала, тем интенсивнее рассеивание его электромагнитной энергии в окружающее пространство. При увеличении частоты сам провод превращается из носителя сигнала в антенну, рассеивающую его энергию в пространство.

3.2 Кабельные системы

Элементы кабельных систем, начиная с типа линий, средств подключения и заканчивая интерфейсами подключаемых устройств, стандартизированы и предполагают жесткие ограничения для сетей определенноо типа. Например, сети Home Network допускается строить в рамках стандарта HDMI, сети межконтинентальных магистралей GAN предполагают использование многожильного оптоволокна с высокими частотными характеристиками и резервированием.

В рамках данного параграфа пособия преподлагается рассматривать кабельные системы для сетей масштаба LAN.

Коаксиальный кабель (COAX) применяется для передачи электрических импульсов. Он состоит из центральной медной жилы в диэлектрической оболочке, поверх которой нанесена металлическая оплетка, и вся конструкция защищена внешней защитной оболочкой (рисунок 3.1). Для обеспечения большей гибкости центральная жила может быть набрана из нескольких проводов малого сечения.

Рисунок 3.2 – Структура коаксиального кабеля

Различают два вида коаксиального кабеля: толстый (около 1 см в диаметре) и тонкий (около 5 мм в диаметре). Тонкий коаксиальный кабель применяется для монтажа во внутренних помещениях, а толстый – для магистральных линий внутри зданий и между ними (в шахтах, тоннелях и в пленумных полостях). Встречаются виды коаксиального кабеля с дополнительным внешним экраном. Он толще, дороже и сложнее при монтаже, а потому сфера его применения ограничена.

Коаксиальный кабель используется в топологии «шина», где обязательно использование оконечных терминаторов. Эффективная длина сегмента зависит от удельного сопротивления кабеля, толщины центральной жилы и типа материала, который идет на изготовление центральной жилы. Например, при удельном сопротивлении 50 Ом (Novell/Ethernet) медный коаксиальный кабель имеет эффективную длину: тонкий около 200 м, толстый около 500 м. При удельном сопротивлении 93 Ом (ArcNet) – более 610 м.

Технические ограничения коаксиального кабеля по частотным характеристикам не были причиной вытеснения его использования в современных LAN. Коаксиальный кабель все еще остается носителем цифрового и аналогового сигналов в сетях кабельного телевидения.

«Витая пара» (далее просто – витая пара), также как и коаксиальный кабель, применяется для передачи цифровых сигналов в форме электрических импульсов. В этом случае для компенсации внешних электромагнитных полей применяется метод естественной компенсации. Когда внешняя помеха искажает амплитуду сигнала на один из проводов пары, это компенсируется за счет симметричной наводки на втором проводе пары. За счет перевивания проводов пары между собой достигается эффект самокомпенсации помехи в итоговом сигнале. Чем больше число витков на единицу длины, тем эффективнее работает данный принцип. Для того чтобы соседние пары проводов не оказывали элекромагнитное влияние друг на друга пары в кабеле дополнительно перевиваются уже между собой.

Витые пары бывают следующих типов (рисунок 3.3):

- экранированная (*shielded twisted pair – STP*);
- изолированная (s*creened twisted pair – ScTP*);
- неэкранированная (*unshielded twisted pair – UTP*).

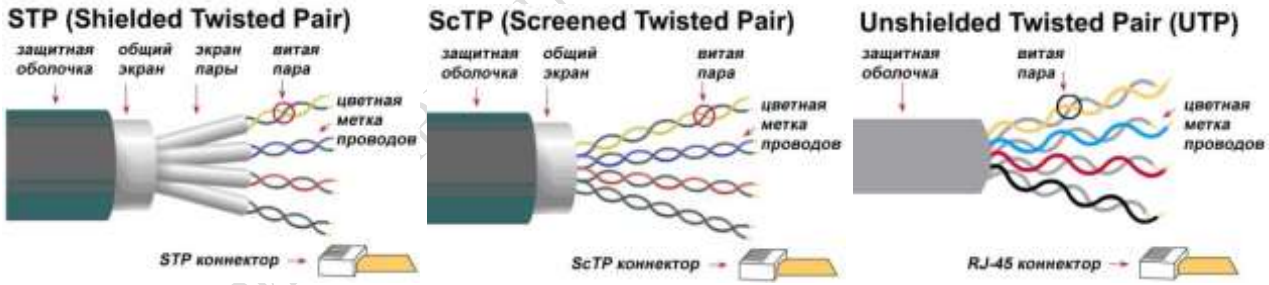


Рисунок 3.3 – Структура кабелей STP, ScTP и UTP

Экранированная витая пара (STP) и изолированная витая пара (ScTP) дороже при производстве, поэтому для проектирования сетей чаще применяется неэкранированная витая пара (UTP).

Витую пару UTP принято классифицировать по категориям. В качестве UTP категории 0 может быть использован двойной провод в жесткой оболочке, применяемый в аналоговых сетях, например, телефонных. Начиная с UTP категории 3, витая пара включает 4 попарно свитых проводника. Сравнительно недавно, одновременно с разработкой стандартов для гигабитных технологий передачи данных, производители стали предлагать кабели с улучшенными частотными свойствами, которые стали позиционироваться как кабели UTP категорий 6 и 7. Электрические характеристики этих витых пар намного превосходят аналогичные характеристики кабелей UTP старого образца (рисунок 3.4).

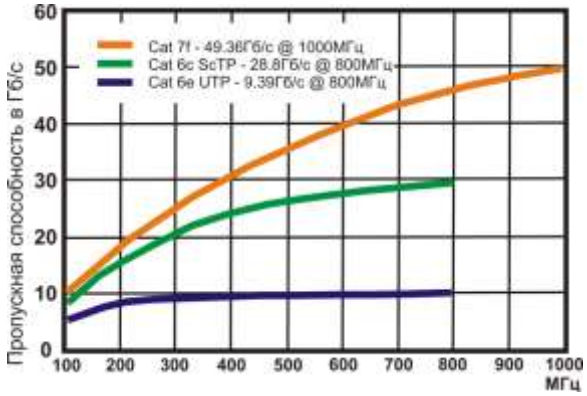


Рисунок 3.4 – Сравнение допустимых скоростей передачи данных в кабеле UTP категорий 6 и 7 при увеличении частоты сигнала

Витую пару применяют в сетях с топологиями: «*кольцо», «звезда», «ячейка».* Максимальный скоростной режим для большинства современных LAN с использованием UTP 6e ограничена 1 Гбит/с. Если интерфейсы узлов сети и ретранслирующих устройств поддерживают спецификации IEEE 802.3bz, скорость может быть повышена до 2,5 Гбит/с и 5 Гбит/с.

Для коммуникации применяется комбинация настенных розеток, в том числе pach-панели, и соединительные штекеры RJ-45 (рисунок 3.5), в устаревших системах (например, ArcNet, POTS) – RJ-11.

Рисунок 3.5 – Кабель «витая пара» с коннектором RJ-45

Для соединения настенной розетки с сетевым адаптером или pach-панели с хабом применяются кабели patch-cord (прямая расшивка). Для соединения сетевых устройств или напрямую двух сетевых интерфейсов применяются кабели cross-cord (cross-кабель).

Если частота передачи достаточно высока, то электрическая и магнитная составляющие сигнала могут распространяться в свободном пространстве (не требуется сплошной проводник). Для того чтобы сигнал распространялся в нужном направлении с наименьшими помехами и потерями, иногда используют такую среду, как *волновод*.

Виды волноводов:

− *металлический волновод* – металлический волновод представляет собой полую металлическую трубку круглого (рисунок 3.6) или прямоугольного сечения. Электромагнитные волны могут распространяться по волноводу, отражаясь от стенок.

Рисунок 3.6 – Структура строения волноводов

В результате интерференции отраженных под определенными углами волн образуются направляемые волновые структуры с синусоидальным или близким к нему распределением поля в поперечном сечении. При этом амплитуды направляемых волн описываются функциями от поперечных координат. Такие волновые структуры называются модами (от англ. *mode*). В кабеле эти моды являются мешающими, паразитными.

В волноводе же, при отсутствии центрального провода уже не может распространяться «кабельная» волна, но одна из мод может быть использована для передачи сигнала.

Металлические волноводы получили применение в качестве линий передачи сантиметровых и миллиметровых волн. При уменьшении длины волны уменьшаются поперечные размеры волновода и возрастают потери мощности волны в стенках. Поэтому для волн с длинами порядка миллиметра и короче волноводы применяются лишь на очень короткие расстояния.

Металлические волноводы применяют на частотах от 2 до 110 ГГц для соединения сверхвысокочастотных передатчиков и приемников с антеннами. В волноводы под повышенным давлением закачивается сухой воздух или чистый азот. Это делается с целью снижения влажности, поскольку в сверхвысокочастотном диапазоне она существенно увеличивает затухания. Прокладка волноводной линии при условиях, которые требуется выполнить (прямолинейность трассы и др.), оказывается очень дорогостоящей, поэтому их применение не стало массовым;

− *диэлектрический волновод* – диэлектрический волновод – это стержень из диэлектрического материала, в котором могут распространяться электромагнитные волны с малыми потерями. Для волн миллиметрового диапазона это полистирол и полиэтилен (фторопласт), малопоглощающие, так называемые неполярные диэлектрики. Электромагнитная волна может распространяться внутри стержня, отражаясь от его границ под углом полного внутреннего отражения. Как и в металлическом волноводе, при интерференции образуются направляемые волны – моды. При этом нет потерь мощности в металле, но имеют место потери в диэлектрике. Эти потери все же достаточно велики, поэтому диэлектрические волноводы получили применение для передачи сигнала на миллиметровых волнах на сравнительно короткие расстояния (метры, десятки метров).

Однако диэлектрические волноводы оказались чрезвычайно перспективными для применения в диапазоне световых волн, точнее, в диапазоне инфракрасных волн с длиной волны порядка микрометра. Они представляют собой волокна из стекла, поэтому получили название оптических волокон или волоконных *световодов*.

В современных высокоскоростных сетях используется *волоконно-оптический кабель*, по сути, являющийся диэлектрическим волноводом.

Оптоволокно используется для передачи информационного сигнала в виде оптического импульса и допускает использование одного световода для организации нескольких сеансов связи одновременно в обоих направлениях. Если это реализовано, то кабельная система называется многомодовой, если нет – одномодовой.

Во многомодовом оптоволокне есть два варианта организации одновременного двустороннего обмена несколькими участниками соединения через один световод:

− со сдвигом фаз одной длины световой волны;
− с использованием разных длин световых волн.

Пример распространения оптического сигнала в кабеле показан на рисунках 3.7 – 3.9, структура и способ соединения оптоволокна – на рисунке 3.10.

Оптоволокно состоит из одной или нескольких стеклянных или пластиковых жил (световодов), покрытых слоем стекла, которое, в свою очередь, заключено в поливинхлоридную оболочку. Для генерации световых импульсов используется один из двух источников света:

− *светодиоды* обычно используются в одномодовом режиме, интенсивность импульсов невелика;

– *полупроводниковые лазеры* генерируют интенсивный, хорошо сфокусированный световой импульс заданного цвета. Они используются в многомодовом режиме.

Важное свойство оптического волокна – долговечность. Фактически при появлении новых стандартов связи существующая кабельная система нуждается только в замене сетевых интерфейсов.

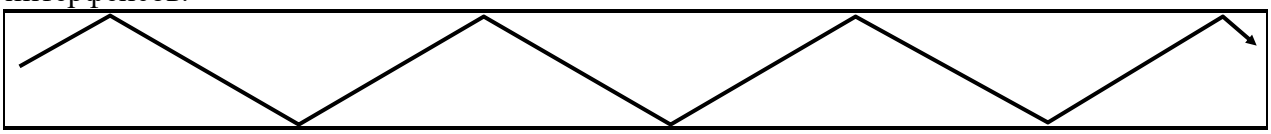


Рисунок 3.7 – Траектория световых импульсов в одномодовом оптоволоконном кабеле

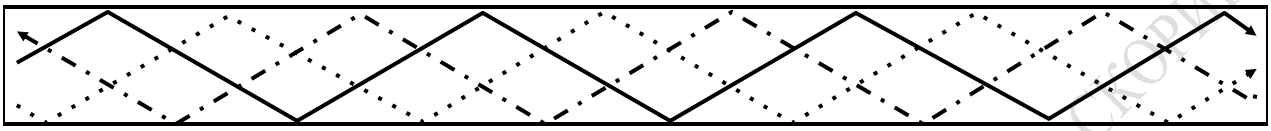


Рисунок 3.8 – Траектория световых импульсов во многомодовом оптоволоконном кабеле с использованием сдвига фаз

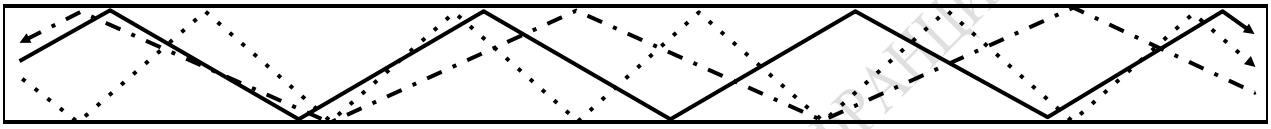


Рисунок 3.9 – Траектория световых импульсов во многомодовом оптоволоконном кабеле с использованием сдвига длины волны

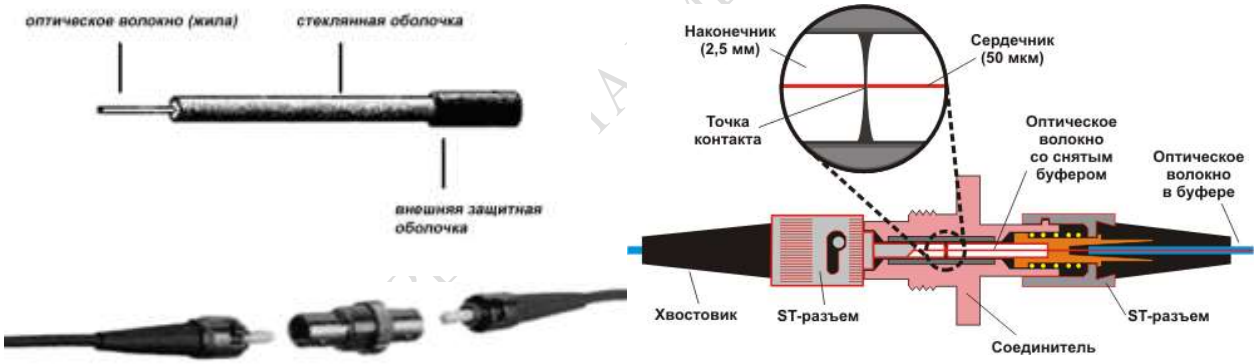


Рисунок 3.10 – Структура оптоволокна и способ его соединения

Оптоволокно применяют в топологиях: «звезда», «кольцо», «ячейка» или их комбинации. В сентябре 2012 года NTT Japan продемонстрировала систему на оптоволоконном кабеле, способную передавать 1 петабит в секунду (10^{15} бит/с) на расстояние 50 километров.

3.3 Структурированные кабельные системы

В настоящее время по мере того, как все большее количество пользователей переходят к применению открытых систем, выпускаемое активное оборудование проектируется на основе положения, что кабельная часть информационной инфраструктуры соответствует требованиям стандартов, то есть является гарантированно надежной и способной обеспечивать определенные рабочие характеристики.

К различным рискам, являющимся следствием нестандартных кабельных систем, можно отнести следующие: сетевые рабочие характеристики ниже определенных стандартами, повышенная стоимость внесения изменений в систему и неспособность системы поддерживать новые технологии. По мере распространения принципов структурированного

кабелирования стоимость устанавливаемого сетевого оборудования падает, а эффективность передачи данных растет с экспоненциальной зависимостью.

Проектирование структурированной кабельной системы (СКС) разделяется на две основные стадии: *архитектурную* и *телекоммуникационную*. Основной задачей архитектурной стадии является определение общей структуры СКС, оптимальной по комплексу технико-экономических характеристик в процессе создания и последующей эксплуатации. Телекоммуникационная стадия чаще всего начинается после окончания архитектурной, а иногда и после завершения капитальных строительно-монтажных работ. В этот период уточняется конкретная структура СКС, составляется перечень необходимого оборудования, планы его размещения и т. д.

В самом общем случае СКС включает в себя три подсистемы:

− подсистема внешних магистралей (первичная) – является основой для построения сети связи между компактно расположенными на одной территории зданиями (кампус);

− подсистема внутренних магистралей (вторичная или вертикальная) связывает между собой отдельные этажи здания и/или пространственно разнесенные помещения в пределах одного здания;

− горизонтальная (третичная) подсистема образована внутренними информационными кабелями между сетевым оборудованием и информационными розетками рабочих мест, самими информационными розетками, коммутационным оборудованием и соединительными кабелями.

Для размещения оборудования используется стандарт, включающий в себя способы коммутации, энергообеспечения и защиты оборудования от несанкционированного доступа. Одним из центральных элементов этого стандарта (как с точки зрения топологии сетей, так и с точки зрения организации энергоснабжения, коммутации и защиты) являются коммуникационные шкафы.

Коммуникационные шкафы (рисунок 3.11) в общем случае рассматриваются как конструкции, предназначенные для обслуживания горизонтальной распределительной системы. Кроме этой основной функции, они могут выполнять и дополнительные – в них допускается размещение промежуточных и главных кроссов.

Для успешного размещения оборудования в коммуникационных шкафах требуется организация высокого уровня совместимости по геометрическим параметрам крепежных элементов.

Стандартный размер коммуникационных шкафов предписывает размер ~ 465 мм по горизонтали и шаг (межосевое расстояние для крепежных отверстий) ~ 17 мм по вертикали. Габарит такого шкафа определяется как 19”. Существует и «расширенный» стандарт на 23”.

Рисунок 3.11 – Примеры коммуникационных шкафов и стоек

По высоте шкафы измеряются в юнитах (количестве единиц оборудования) «U»: 4U (280 мм), 6U (345 мм), 9U (478 мм), 12U (612 мм), 15U (746 мм), 18U (878 мм), 21U (1012 мм) и выше.

Системы энергоснабжения оборудования и источники бесперебойного питания размещаются внутри коммуникационных шкафов, так что следует учитывать этот факт при выборе размеров коммуникационного шкафа для конкретного проекта сети.

Кабельные системы являются лишь носителем (средством передачи) данных в сети. Основой сети является сетевое оборудование. Большая его часть собирается в коммуникационных стойках или шкафах, и его объединение в сеть представляет серьезную проблему, которая может быть сформулирована следующим образом: *чем больше структуризация системы, тем меньше задокументирована и систематизирована сама структура связей между оборудованием*.

Внутри коммуникационной стойки образуется хаотически переплетенный жгут проводов (рисунок 3.12), и процесс поиска нужного кабеля занимает существенное время.

Рисунок 3.12 – Пример коммутации сети для учебного класса

В качестве решения данной проблемы были разработаны системы комбинированной коммутации, применяемые для серверных решений типа «Blade». В этом случае система коммутации базируется на внутренних шинах специального серверного шасси (рисунок 3.13).

Рисунок 3.13 – Шасси HP BladeSystem c7000 (виды спереди и сзади)

Коммутационное оборудование имеет порты подключения на передней и задней (магистральной) панели, при этом последние имеют программное управление и могут быть настроены для работы в любой комбинации коммутационных каналов (рисунки 3.14, 3.15).

Рисунок 3.14 – Модуль коммутатора FC для организации SAN

Рисунок 3.15 – Модуль маршрутизатора

Серверные «лезвия» могут иметь различные физический размер, компоновку и состав оборудования. Единственное и обязательное требование – совместимость с шасси Blade-системы (рисунок 3.16).

Рисунок 3.16 – Серверное лезвие HP ProLiant

Все модули, устанавливаемые в шасси современного Blade-сервера, используют общие системы питания и охлаждения, единую коммуникационную среду и средства управления. Все элементы этой системы дублируются. Современные Blade-серверы поддерживают горячую замену всех своих модулей: вычислительных, коммуникационных, блоков питания, вентиляторов.

Использование Blade-серверов позволяет обеспечить свободный доступ к каждому вычислительному или сетевому модулю, отсутствие нагромождения кабелей значительно облегчают задачи установки и замены отдельных устройств, поддержку и эксплуатацию всей системы в целом. Blade-серверы потребляют существенно меньше электроэнергии и занимают гораздо меньше места.

3.4 Магистральные кабельные системы

В качестве крупных элементов инфраструктуры организации и поддержки информационных потоков в современных условиях используются оптоволоконные магистрали. Прокладка оптоволоконных магистралей на территории суши является хоть и дорогостоящей, но довольно простой задачей. Преимуществом такого решения является возможность организации логистики данных и начала возврата инвестиций поэтапно до завершения проекта целиком, поскольку опорные пункты связи и промежуточной маршрутизации, через которые проходит оптоволоконная магистраль обеспечивают доступ к пользовательской аудитории, которая территориально находится вокруг него.

Существенная сложность этого решения состоит в необходимости закладывать пропускную способность магистрали с учетом потенциального быстрого роста

информационного роста нагрузки на сеть как на каждой из конечных точек магистрали, так и на промежуточных ее узлах.

Можно утверждать, что прокладка оптоволоконных магистралей по суше решает местные региональные задачи и не всегда может обеспечивать целевой трафик регионов, которые географически удалены от центров маршрутизации. Дополнительным ограничением на выбор такого решения могут быть неблагоприятные геологические условия, экологические ограничения, природные катаклизмы и риск военных конфликтов, которые могут повредить инфраструктуру магистральных сетей и затруднить ее эксплуатацию, либо техническое обслуживание.

У подводных оптоволоконных магистралей присутствуют аналогичные риски: экстерриториальное размещение, фиксированная конфигурация кабельной структуры (с момента укладки до вывода из эксплуатации), потенциальное повреждение в результате организации движения судов (промышленное рыболовство, использование якорей), потенциальное преднамеренное повреждение (рисунок 3.17) и даже вред со стороны местной фауны (например, агрессивное поведение акул).

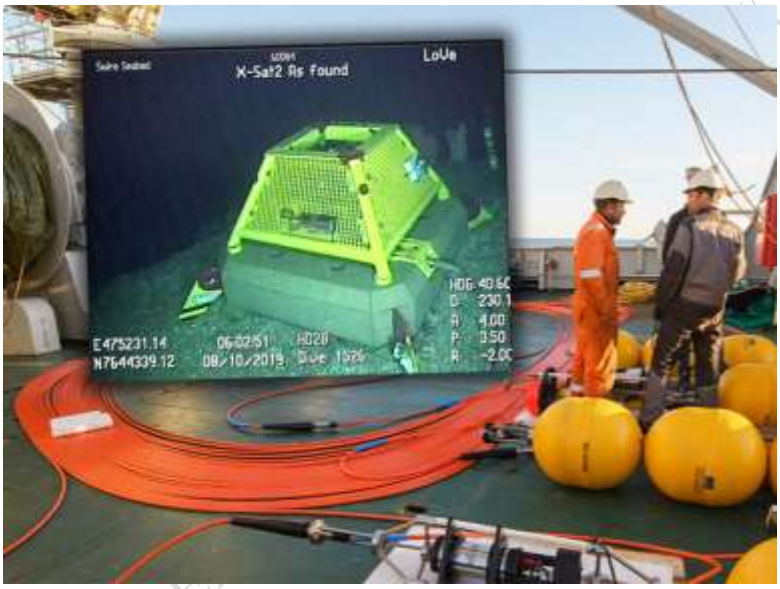


Рисунок 3.17 - Прецедент повреждения подводных кабелей морской обсерватории Лофотен-Вестеролен у побережья Северной Норвегии

Исходя из этих рисков все типы оптоволоконных магистральных кабелей должны быть защищены, а степень защиты зависит от рельефа океанского или морского дна и глубины их размещения. Решение разместить оптоволоконные магистрали на дне в прибрежной зоне в ряде случаев оказывается безальтернативным и самым экономичным способом.

Например, в 1989 году было введено в эксплуатацию кабельное соединение Scotland-Northern Ireland 1 между населенными пунктами Великобритании Donaghadee и Portpatrick через Северный пролив Между Атлантическим океаном и Ирландским морем. Длина магистрали составляет около 35 км. Скорость передачи данных на момент ввода в эксплуатацию составляла 3,36 Гбит/сек (0,00336 Tbps). Предполагалось завершить эксплуатацию данной магистрали к 2014 году, но ее использование продолжается и в 2021 году.

В том же 1989 году было создано еще три линии оптоволоконной магистрали между Бельгией и Великобританией, между Данией и Швецией и двумя островами Дании в Балтийском море. Основной задачей морских магистралей того периода была организация транзита трафика между разделенными сетями.

Недостатком организации работ такого типа магистралей является техническая сложность обслуживания и необходимость введения избыточности числа световодов для обеспечения надежности, поддержания полосы пропускания и возможности ее расширения

при увеличении нагрузки в дальнейшем. Подтвержденная возможность продления сроков эксплуатации магистралей относительно медных решений, а также потенциальная возможность увеличения скоростных характеристик используемых световод за счет модернизации оконечных интерфейсов послужила причиной быстрого роста инвестиций в данные технологии.

Еще одним удобством, которое быстро освоили на рынке, стало гарантированное качество связи на дальних дистанциях. Поскольку между точкой погружения магистрали и вывода ее на берег число отводов строго регламентировалось, поэтому «промежуточный разбор трафика» характерный для оптоволоконных магистралей на суше не мешал решению целевой задачи.

Уже в 1998 году был завершен трансатлантический проект Atlantic Crossing-1 (AC-1). Он соединил в кольцевую структуру узлы связи Sylt (Германия), Beverwijk (Нидерланды), Whitesands Bay (Великобритания), Brookhaven, NY (США). Длина магистрали составляет около 13.168 км. Скорость передачи данных на момент ввода в эксплуатацию 40 Гбит/сек (0,04 Tbps). На 2014 год скорость передачи информации была доведена до 2,35 Тбит/сек (2,35 Tbps). Предполагается завершить ее эксплуатацию к 2023 году:

- 1999 год = 0,04 Tbps
- 2002 год = 0,12 Tbps
- 2007 год = 0,635 Tbps
- 2008 год = 0,815 Tbps
- 2009 год = 1,165 Tbps
- 2010 год = 1,455 Tbps
- 2012 год = 1,76 Tbps
- 2013 год = 2,1 Tbps
- 2014 год = 2,35 Tbps

Более поздние скоростные показатели для AC-1 в открытых источниках не приводятся.

Магистраль построена согласно спецификациям стандарта Synchronous Digital Hierarchy (SDH) и включает в себя 8 каналов DWDM (Dense Wavelength Division Multiplexing) в двух оптоволоконных парах.

Расстояние между несущими частотами в DWDM-системах может составлять от 25 до 200 ГГц, в современных сетях используется сетка каналов с шагом 50 ГГц . В зависимости от типа используемого кабеля, для передачи могут быть задействованы спектральные диапазоны C (1530..1565 нм), S (1460..1530 нм) и L (1565..1625 нм). Пример плотности заполнения канала приведен на рисунке 3.18.

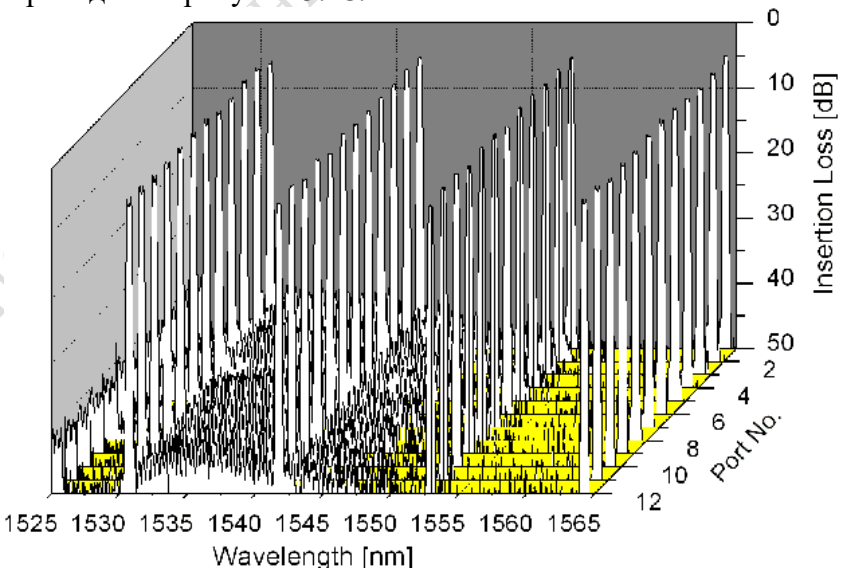


Рисунок 3.18 - Распределение каналов с шагом в 50 ГГц для 12-портовой матрицы WSS

На данный момент через Атлантический океан проходит около 20 оптоволоконных магистралей большая часть из которых введена в эксплуатацию после 2008 года. Их ресурс на модернизацию, то есть повышение информационной емкости - очень велик.

С этого момента имеет смысл ввести классификацию подводных оптоволоконных магистралей по принципу географического охвата и государственной принадлежности узлов связи, которые подключаются к магистрали непосредственно, либо в качестве «точки отвода от магистрали».

1. Национальная оптоволоконная магистраль - соединяет узлы связи на территории одного государства.

2. Региональная оптоволоконная магистраль - соединяет узлы связи на территории рядом расположенных государств одного региона.

3. Межрегиональная оптоволоконная магистраль - соединяет узлы связи на территории разных государств расположенных далеко друг от друга.

4. Интерконтинентальная оптоволоконная магистраль - соединяет узлы связи на территории государств расположенных на разных материках.

Atlantic Crossing-1 (AC-1) является примером интерконтинентальной оптоволоконной магистрали, Scotland-Northern Ireland 1 - примером национальной оптоволоконной магистрали.

3.5 Беспроводные сетевые среды

Применение беспроводных сетей удобно для мобильных устройств и автономных элементов вычислительной системы в составе группы.

Беспроводные сети имеют три варианта реализации:

− *локальные вычислительные сети* (на беспроводном принципе) – в этом случае единственная разница обычной сети от беспроводной заключается в отсутствии кабельной системы, однако, используемое соединение точка-точка, как правило, закреплено не только за помещением, но и за местоположением самого помещения. В этом случае используется бесперебойная связь. Фиксированный приемопередатчик соединяется кабелем с рабочей станцией. Прием передачи может называться точкой доступа;

− *расширенные локальные вычислительные сети* – в этом случае часть сети реализуется с помощью кабельной сети, а отдельные ее участники обладают большим уровнем мобильности. В некоторых случаях беспроводным соединением может быть радиомост между сегментами кабельной сети. Обратным примером может служить беспроводная сеть, в которой кабелем соединяется система серверов;

− *мобильные сети* – это сети мобильных компьютеров. В более общем случае – это система вычислительных комплексов, объединенная в сеть с помощью любого вида беспроводной технологии.

Техническая реализация беспроводных сетей предполагает:

− *радиосоединение:*

а) узкополосное – одна радиочастота на всех;

б) широкополосное – набор частот – наиболее проработанный и традиционный тип носителя беспроводной связи, несмотря на то, что технология дает плохой уровень защиты от электромагнитных излучений;

− *лазерное излучение* – можно использовать только в случае наличия прямой видимости приемника и передатчика между двумя зданиями. Можно обеспечить достаточно высокую скорость передачи, но надежность связи – низкая из-за того, что луч может рассеиваться или отклоняться (из-за особенностей изготовления оборудования, многие авторы объединяют с инфракрасной связью);

− *инфракрасное излучение* – здесь используется и прямой сигнал, и отраженный; из-за этого поддерживается достаточно низкая скорость распространения сигнала, но обеспечивается высокая надежность передачи;

– *микроволновое соединение* – используется как разновидность радиосоединения – на текущий момент является достаточно дешевой технологией. Недостатки – низкая скорость передачи данных и малый радиус действия;

– *использование сотовых сетей общего доступа* – наиболее удобен для реализации удаленного подключения мобильной станции пользователя к сети предприятия, осуществляющего данную услугу;

– *спутниковые системы* – самая глобальная из беспроводных систем по охвату территории. Недостатки – высокая стоимость передающего оборудования и арендная плата за трафик через спутник.

Беспроводные сети также можно поделить по размеру зоны охвата:

– *Wireless Personal-Area Network (WPAN)* – сети малой мощности и ближнего действия (до 10 м). Базируются на стандартах IEEE 802.15 и частоте 2,4 ГГц. Bluetooth и/или Zigbee;

– *Wireless LAN (WLAN)* – сети среднего размера (до 100 м). Базируются на стандарте IEEE 802.11 и частотах от 1 до 7,0 ГГц (рисунок 3.19);

– *Wireless MAN (WMAN)* – сети для обширной географической области, такой как город или район. Базируются на стандартах IEEE 802.11 и IEEE 802.15, используют определенные лицензированные частоты.

– *Wireless WAN (WWAN)* – сети обширной географической области для национальной и/или глобальной коммуникации. WMAN, как правило, используют в качестве носителя сети операторов сотовой связи или низкоорбитальные спутниковые группировки.

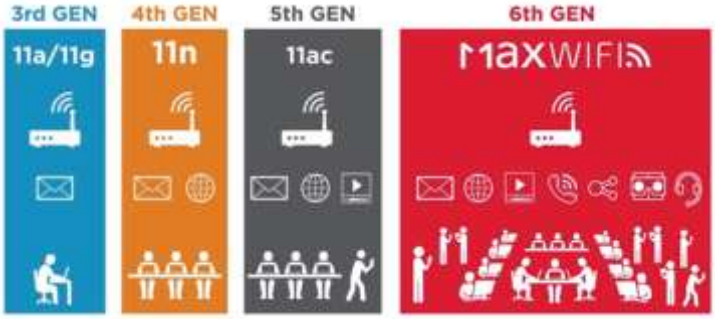


Рисунок 3.19 – Эволюция WiFi

Внедрение беспроводных технологий в вычислительный процесс предприятий и высокий уровень обеспеченности персонала мобильными устройствами привели к развитию концепции Bring Your Own Device (BYOD). Концептуально с работодателя снимается необходимость обслуживания технической и программной составляющей этих устройств, но возникает неоходимость обеспечения более высоких нормативов информационной безопасности.

Основным вектором внимания в этом случае должен стать внутрипериметральный сетевой трафик.

3.6 Сетевые устройства уровня L1

Устройства уровня L1 наиболее зависят от типа кабельной системы и особенностей ее эксплуатации. В том числе по силовой нагрузке на разъем, вероятность повреждения от вибрации, корозии и, например, оптического выгорания.

К устройствам этого типа можно отнести следующие:

– модемы (*MODEM*);
– повторители (*REPEATER*);
– трансиверы (*TRANSIEVER*) и медиаконверторы (*CONVERTOR*);
– сетевые интерфейсы устройств (*NIC*);
– концентраторы (*HUB, MAU*);
– сплитеры и мультиплексоры.

Модем (модулятор-демодулятор) служит для передачи информации на большие расстояния, недоступные локальным сетям. Передача осуществляется через выделенные или коммутируемые телефонные линии.

Скоростные параметры модемов имеют следующие характеристики:

- *cps* – скорость передачи символов, байт/с;
- *bps* – скорость передачи, бит/с;
- *baud* – количество изменений сигнала в линии за 1 секунду.

Для повышения эффективной скорости работы при ограниченной полосе линии применяют различные методы кодирования и модуляции, при которых *bps* превышает *baud*.

Синхронные модемы POTS (Plain old telephone service, DialUp) работают на скоростях до 56 Кбит/с на аналоговых линиях. Тип модема также зависил от числа функций, реализованных в нем либо только аппаратно, либо совместно с программным способом (*софт-модемы*).

DSL-модемы (*Digital Subscriber Line, цифровая линия подписки*) разработаны телефонными компаниями для предоставления услуг кабельного телевидения. Распространился асимметричный подвид стандарта – ADSL. *ADSL-модем* передаёт данные одновременно с голосом, используя обычную пару медных телефонных проводов (рисунок 3.20). Скорость передачи данных зависит от фактической длины линии (не должна превышать 5,46 км), а также от типа и состояния интерфейсов и кабелей.

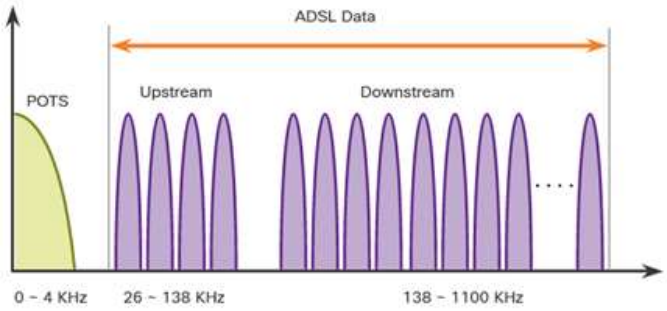


Рисунок 3.20 – Разделение частотного диапазона канала связи

Версия стандарта ADSL2+ 2005 года регламентировала скорость передачи данных 24 Мбит/с в одну сторону и 3,5 Мбит/с в противоположную одновременно.

Повторитель регенерирует форму сигналов, передаваемых в сетевой среде, за счет чего позволяет увеличивать длину сетевого сегмента. Устройство является избыточным с точки зрения современных кабельных сетевых архитектур. Эффективно применялся в топологии «шина» для коаксиальных кабельных систем. В беспроводных сетях устройства данного типа называются радиоповторитель (радиоудлинитель).

На рисунке 3.21 представлена схема расширения зоны радиопокрытия повторителем WiFi. Входной сигнал может доставляться до повторителя кабельной системой или же сигнал может приниматься по каналу WiFi на общей или независимой несущей радиочастоте.

Рисунок 3.21 – Разделение частотного диапазона канала связи

Трансивер (TRANSmitter – передатчик + receiver – приемник) – тип устройств является устаревшим подходом к универсуализации технического подключения сетевого интерфейса к кабельной системе разных типов (рисунок 3.22). Устройство предназначено для преобразования потока параллельных данных, пересылаемый по шине компьютера, в поток последовательных данных, пересылаемый по кабелю. Устройство не является автономным и должно быть совместимо с аппаратной и программной составляющей основной сети.

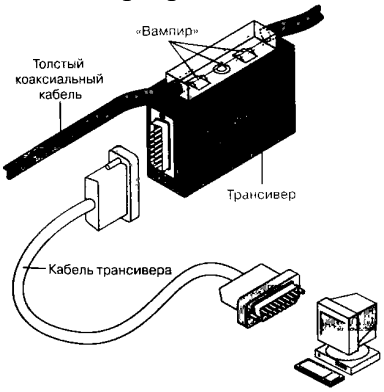


Рисунок 3.22 – Подключение трансивера к коаксиальному кабелю

Медиаконвертор – двухпортовое устройство, оба порта которого представляют средозависимые интерфейсы. Устройство может работать автономно и иметь, в ряде случаев, независимое управления от порта, чей трафик оно обслуживает. Некоторые авторы описывают медиаконверторы как упрощенную версию устройства L2 мост (bridge). Конверторы, в отличие от повторителей, могут работать в дуплексном режиме. В современных ЦОД распространены конверторы 10GBase-TX/10GBase-FX (рисунок 3.23).

Рисунок 3.23 – Медиаконвертор 10G

На рисунке 3.23 один из портов устройства является сменным шасси для размещения средозависимого сменного модуля интерфейса формата SFP+. Эти модули, если они входят в состав сетевого устройства, уже фигурируют в описании проекта сети как полноценные конверторы.

Шасси сменных средозависимых модулей, применяемые в современных сетевых устройствах:

− SFP (small form-factor pluggable) можно рассматривать как обновленную версию GBIC (Gigabit interface converter). Его объем составляет 1/2 от модуля GBIC, что значительно увеличивает плотность портов сетевых устройств. Скорость передачи данных SFP от 100 Мбит/с до 4 Гбит/с.

− SFP+ - расширенная версия SFP, поддерживающая 8 Гбит/с Fibre Channel, 10 Gigabit Ethernet и стандарт оптической транспортной сети OTU2. SFP+ также предлагает прямое подключение для соединения двух портов SFP+ без дополнительных оптических модулей, включая DAC (Direct Attach Cable) и AOC (Active Optical Cable).

− SFP28 - расширенная версия SFP+. Конверторы имеют одинаковый размер, но SFP28 поддерживает 25 Гбит/с на одном канале.

− QSFP+ (quad small form-factor pluggable) - может переносить 4 канала одновременно, и каждый канал может обрабатывать скорость передачи данных 1 Гбит/с.

− QSFP+ поддерживает четыре канала 10 Гбит/с. И эти 4 канала могут быть объединены в канал 40 Gigabit Ethernet. QSFP+ может заменить 4 стандартных SFP+ модулей, которые могут улучшить плотность портов и снизить общую стоимость системы по сравнению с традиционными SFP+ продуктами.

− QSFP28 – эффективное решение для организации высокоскорост-ных соединений, которое предназначено для ресурсоемких приложений (рисунок 3.24). Обеспечивает четыре канала высокоскоростных дифференциальных сигналов со скоростями передачи данных от 25 Гбит/с (потенциально до 40 Гбит/с) для удовлетворения требований 100 Гбит/с Ethernet (4×25 Гбит/с) и 100 Гбит/с 4X InfiniBand Enhanced Data Rate (EDR).

Рисунок 3.24 – Подключение 100G QSFP28->4x SFP28 DAC

Сетевой адаптер или сетевая карта (netcard) – это интерфейсная карта ввода-вывода информации, которая обеспечивает преобразование информационных сигналов, поступающих от системной шины компьютера в форму, пригодную для ретрансляции в соответствующей среде передачи (рисунок 3.25). Внутреннее строение сетевого адаптера и его физические интерфейсы зависят от типа топологии, среды передачи и сетевого стандарта, для работы с которыми предназначен данный сетевой адаптер.

Сетевые адаптеры или сетевые интерфейсные карты (Network Interface Card, NIC), выпускаемые многими производителями в широком ассортименте, различаются поддерживаемыми средами передачи, типом системной шины (ISA, EISA, MCA, PCI, реже VLB), архитектурой и производительностью. Для ноутбуков существовали адаптеры Ethernet в стандарте PCMCIA (PC CARD).

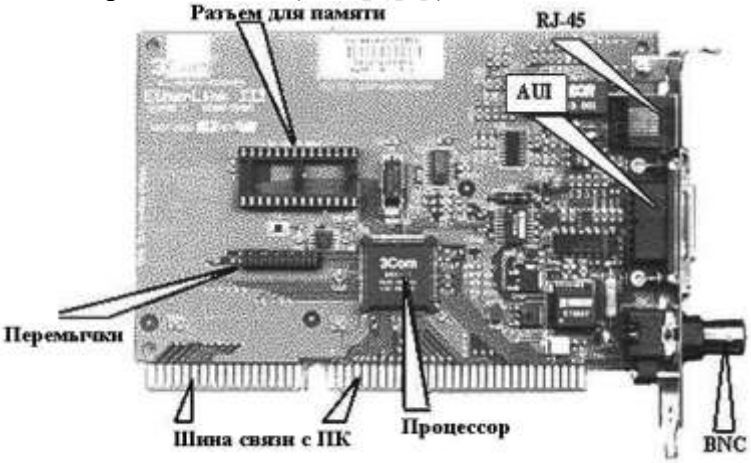


Рисунок 3.25 – Функциональные блоки сетевого адаптера Ethernet

Выпускались также адаптеры, подключаемые к RS-232 LPT-порту (Paraport), Thunderbolt или (наиболее часто) для USB. Примеры показаны на рисунке 3.26.


Рисунок 3.26 – Сетевые адаптеры для портов LPT, PCMCIA и USB

Подавляющее число современных вычислительных систем, начиная со SmartTV и заканчивая серверами blade, имеют в своем составе один или несколько встроенных сетевых интерфейсов.

На текущий момент широко распространены сетевые карты с интерфейсом 1000Base-TX на шину PCIX. Применяются также сетевые карты с оптическим интерфейсом (рисунок 3.27).

Настройка сетевого адаптера заключается в первую очередь в настройке операционной системы, которая может быть успешно осуществлена только при условии отсутствия конфликтов по оборудованию между сетевым адаптером и любым другим устройством системы.

Конфликт может быть по прерыванию, по диапазону адресов ввода-вывода, а в некоторых случаях по каналу DMA. Учитывая все это, производители перевели все современные модели сетевых адаптеров в режим PnP.

Рисунок 3.27 – Внешний вид сетевого адаптера:

Концентратор – это активный многопортовый повторитель с функцией автосегментации. Автосегментация позволяет изолировать от общей среды трансляции порт, подключенный к сегменту сети с аномально искаженным трафиком. Обработка ошибок и текущий контроль состояния каналов связи осуществляется самим концентратором.

Концентраторы можно *каскадировать*, т. е. соединять друг с другом, увеличивая тем самым размер сети и создавая сложные топологии. Недостатком такой технологии является то, что трафик получаемой системы будет входить в общий широковещательный сегмент, т. е. увеличивается вероятность возникновения глобальных ошибок и сбоев. Также ограничение на число подключенных узлов может распространяться на всю объединенную систему.

Все порты концентратора равноправны. Получив сигнал от одной из подключенных к нему станций, концентратор транслирует его на все свои активные порты. При этом, если на каком-либо из портов обнаружена неисправность, то этот порт автоматически отключается (сегментируется), а после ее устранения снова делается активным.

Концентраторы могут быть активными и пассивными, то есть без функции восстановления формы сигнала. Простейшие концентраторы представляют собой единую точку подключения к сети, позволяющую физически реализовать в виде звезды логическую шинную сеть Ethernet или маркерное кольцо. Такие концентраторы также называются неуправляемыми и предназначены они для очень маленьких сетей, содержащих до 12 узлов.

Концентраторы применяются в сетевых топологиях «звезда», «звезда-шина», «звезда-кольцо». В зависимости от конкретной топологии внутренняя логическая начинка, а значит, и механизм работы устройства будут разными (рисунок 3.28).

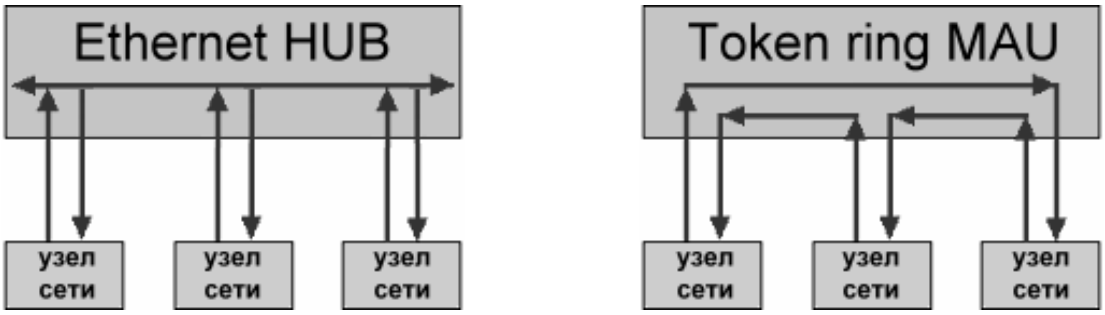


Рисунок 3.28 – Примеры внутренней структуры концентраторов

Большинство концентраторов были выпущены для сетей со скоростью обмена 10 Мбит/с (HUB Ethernet), либо 20 Мбит/с (MAU TokenRing). Сейчас концентраторы практически полностью исчезли с рынка.

Сплитеры и мультиплексоры в современных оптических сетях применяются для формирования сигнала для передачи на порт назначения. Например, стандарт GPON FTTH предполагает доставку смешанного трафика на все порты пассивной оптической сети. Необходимую часть трафика отфильтровывает оптический терминал (optical network terminal, ONT). Задача мультиплексора – собрать сигнал из независимых сетевых интерфейсов и передать в сетевую среду с достаточной скоростью передачи для последующего разделения на принимающей стороне (рисунок 3.29).

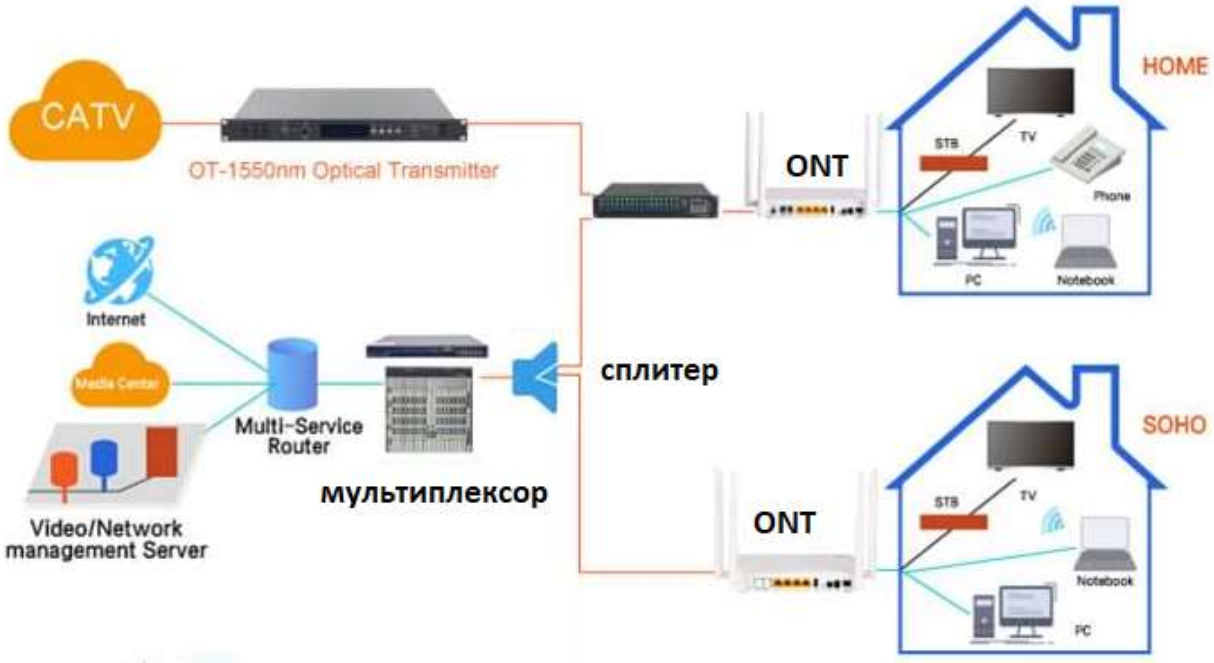


Рисунок 3.29 – Доставка сигнала в пассивной оптической сети

В сетевых структурах семейства POTS мультиплексоры объединяли независимые устройства DialUp в устройство, называемое «модемный пул».

4 Немаршрутизируемые сетевые среды

4.1 Канальный уровень ISO/OSI (L2)

Задача *канального уровня* в локальной сети – компоновать передаваемые биты данных в виде фреймов (*frame – кадр*). Каждый кадр должен быть сформирован таким образом, чтобы после передачи данных от узла к узлу их можно было бы собрать в исходном порядке. Этот уровень формирует данные в стандартизованном виде, после чего отформатированные кадры поступают на физический уровень, где передающий узел может отправить их в коммуникационную среду.

Принимающий узел получает кадр данных из физического уровня сети отправления, декодирует электрический сигнал, преобразует его в кадр, требуемый на физическом уровне сети назначения, проверяет наличие ошибок в кадре. Кадр данных может иметь структуру, указанную на рисунке 4.1.

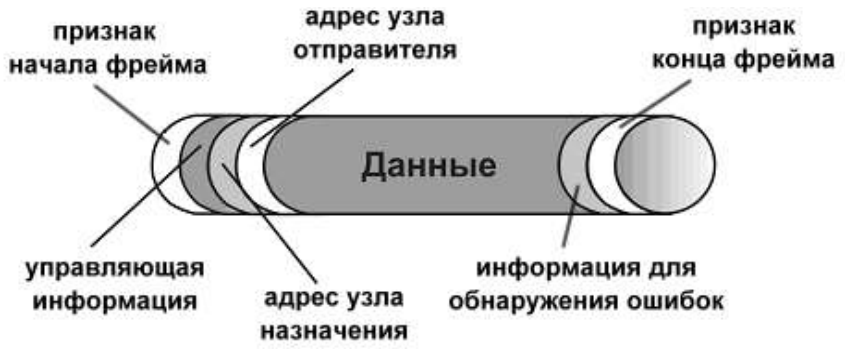


Рисунок 4.1 – Формирование кадра данных согласно модели OSI

Канальный уровень (Data Link Layer) делится в локальных сетях на два подуровня:

- управление логическим каналом связи (Logical Link Control, LLC);
- управления доступом к среде (Media Access Control, MAC).

Уровень MAC появился из-за существования в локальных сетях разделяемой среды передачи данных. Этот уровень обеспечивает корректное совместное использование общей среды, предоставляя ее в соответствии с определенным алгоритмом в распоряжение той или иной станции сети. Подуровень MAC задает или распознает физическую адресацию кадра.

После того, как доступ к среде получен, ею может пользоваться более высокий уровень – уровень LLC. Этот уровень отвечает за передачу кадров данных между узлами с различной степенью надежности, а также реализует функции интерфейса с прилегающим к нему сетевым уровнем. Именно через уровень LLC сетевой протокол запрашивает у канального уровня нужную ему транспортную операцию с нужным качеством. На уровне LLC существует несколько режимов работы, отличающихся наличием или отсутствием на этом уровне процедур восстановления кадров в случае их потери или искажения, то есть отличающихся качеством транспортных услуг этого уровня.

Следует отметить, что протоколы и алгоритмы канального уровня не ориентированы на установление соединения. Процесс передачи может быть начат, пристановлен или отменен, но информация об успешности доставки кокретного кадра данных нигде не фиксируется. Более того при нарушении структуры сети кадры данных могут попасть в ситуацию бесконечной ретрансляции, что, в свою очередь, заблокирует сегмент сети где произошла аномалия для дальнейшей работы.

Для формирования кадра данных PDU протоколов уровня L3 инкапсулируются в качестве блока данных и дополняются необходимые служебные поля, соответсвующие требованиям сетевого стандарта. Процесс инкапсуляции многоуровневый, на канальном уровне формируется финальная форма, которую допустимо транслировать в сетевую среду (рисунок 4.2).

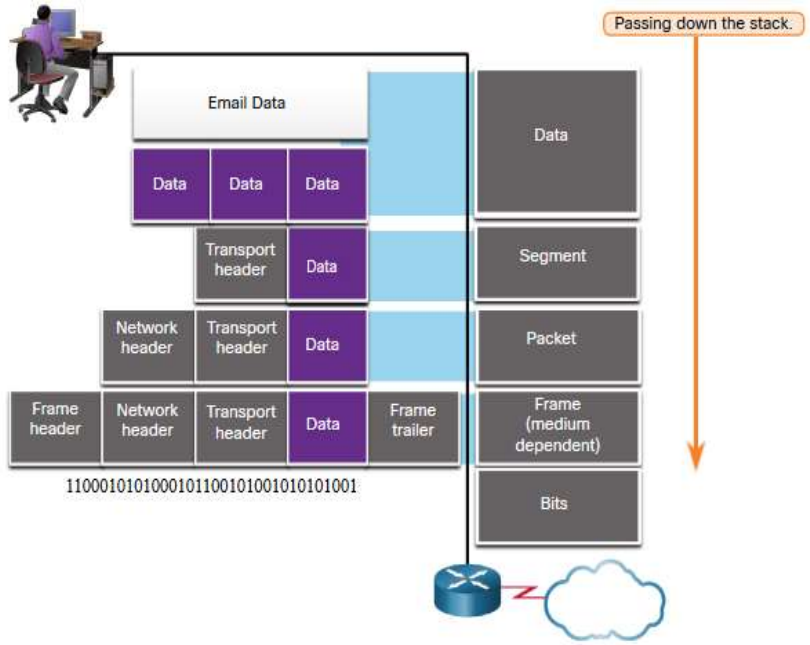


Рисунок 4.2 – Инкапсуляция данных в PDU разных уровней

4.2 Сетевые структуры

Порядок участия устройств связи в процессе сетевого обмена является результатом выполнения ряда условий и ограничений, имеющих в ряде случаев физические обоснования. Поэтому рассмотрение тем, связанных с методами доступа к среде, следует делать одновременно с изучением структуры и иерархии сетевых связей.

Общие подходы к анализу сетевых структур делятся на две части:

Логическая структура сети подчинена структуре информационных потоков. Она является первичной и ключевой при разработке физической структуры сети.

Под термином *физическая структура сети* следует понимать базовый принцип, который используется при размещении узлов и рабочих станций, а также активного оборудования сети на территории предприятия (в здании, группе зданий и между ними), то есть *топологию компьютерной сети*.

С точки зрения проектирования компьютерных сетей, топология – это описание основной компоновки сети.

Топология определяет следующие свойства:

- тип кабельной системы;
- тип и характеристики передающего оборудования, применяемого для передачи данных;
- физическое размещение компьютеров, силовых и информационных кабелей, а также других компонентов сети;
- способ прокладки кабеля;
- возможность расширения сети;
- способ управления сетью.

На текущий момент наиболее популярными являются четыре типа базовых топологий, называемых «чистыми»: «*шина», «кольцо», «звезда», «ячейка»*, и два типа комбинированных: *«звезда-шина», «звезда-кольцо»*. Остальные относят к сложным или смешанным топологиям.

Сложные топологии – это топологии с программируемой структурой, которые настраиваются под решаемую задачу. Некоторые варианты сложных топологий представлены на рисунке 4.3. Вариант 4.3, *а* является примером нерегулярной топологии, а вариант 4.3, *б* – иерархический случай связи (древовидная топология).

а) б)

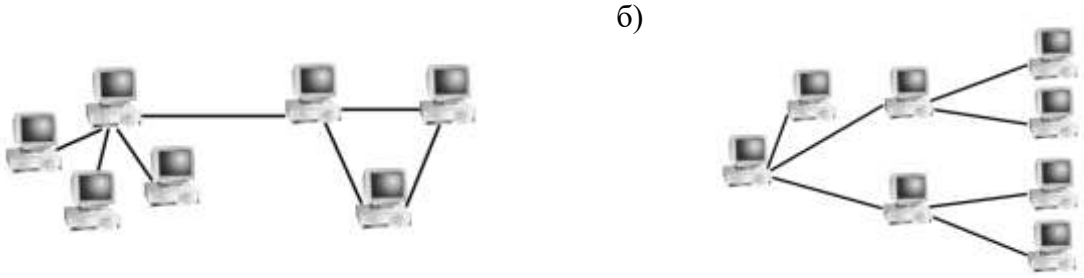


Рисунок 4.3 – Примеры сложных топологий вычислительных сетей

Если топологии *«шина», «кольцо», «звезда», «ячейка»*, «*звезда-шина», «звезда-кольцо»* чаще применимы для локальных сетей, то более сложные схемы типичны для региональных и глобальных сетей. Некоторые современные вычислительные сети используют и другие сетевые структуры: «*решетки», «кубы», «гипердеревья», «гиперкубы»* и т. д. (рисунок 4.4).

Топология часто определяет способ взаимодействия компьютеров в сети, в частности – метод доступа к среде.

а) б) в)

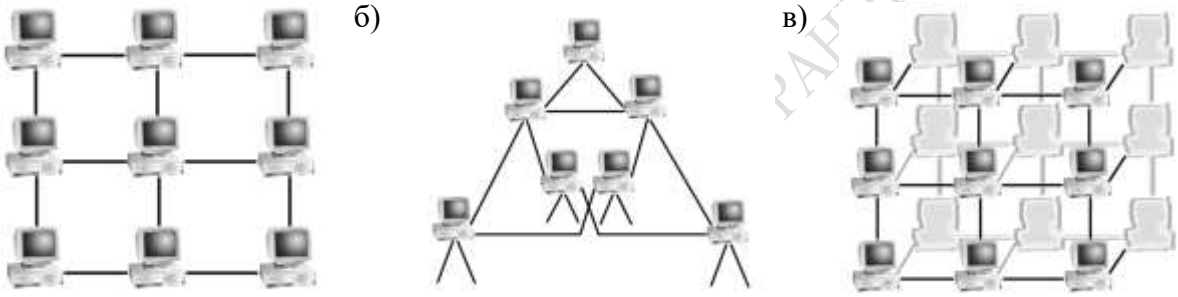


Рисунок 4.4 – Структуры топологий сложных вычислительных систем: *а*) «решетка»; *б*) «гипердерево»; *в*) «куб»

Выбор топологии локальной или региональной сети существенно сказывается на ее стоимости и рабочих характеристиках. При этом важной характеристикой для однородной сети является среднее число шагов между узлами *D*.

$$D = \sum_{d=1}^{n} \frac{\alpha \cdot N_d}{n-1},$$

где n – полное число узлов в сети; α – расстояние между крайними узлами сети, N_d – число узлов сети на расстоянии α.

Как правило, обычная локальная сеть, которая проектируется с нуля, подчинена одному из четырех типов «чистых» топологий. После проведения модификации и/или адаптационных работ ее топология становится сложной или смешанной.

Шинная топология использует принцип последовательного соединения узлов сети в виде цепочки. В случае использования кабеля к каждому концу сегмента шины подключается терминатор для «гашения» отраженного сигнала. Передаваемый пакет принимается всеми узлами сегмента, и на прохождение всего сегмента требуется некоторое количество времени, называемое задержкой (рисунок 4.5).

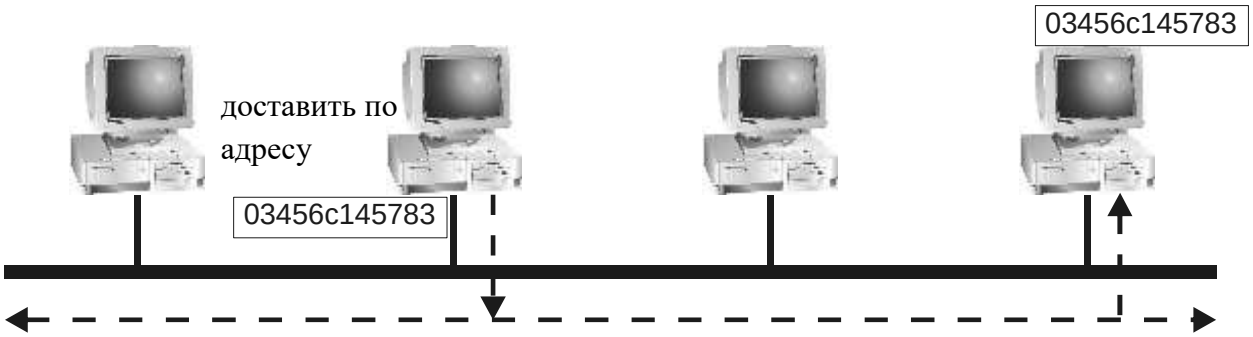


Рисунок 4.5 - Доставка данных адресату в топологии «шина»

Наличие терминатора для шинной топологии обязательно, поскольку терминатор указывает на физическое окончание сегмента. На практике терминатор представляет собой электрическое сопротивление, гасящее сигнал, когда тот достигает конца сети. Без терминатора сегмент не соответствовал бы спецификациям IEEE и сигналы могли бы отражаться обратно, возвращаясь в тот же кабель, по которому они были переданы. Отраженный сигнал сбивает синхронизацию сети и может сталкиваться с новыми сигналами, передаваемыми по сети.

Кроме классических стандартов сетевых архитектур с использованием данной топологии – ArcNet и Ethernet, следует упомянуть и сетевые архитектуры для данной топологии, разработанные в СССР, такие, как FishNet (100 Ом) и Iola (75 Ом). Сети кабельного телевидения и системы CaTV также используют шинную топологию для подключения отдельных пользователей к общей информационной среде или одной из информационных сред. Также следуют упомянуть, что стандарты ИК-сетей часто реализуются по топологии «шина».

При топологии «кольцо» компьютеры подключаются к кабелю, замкнутому в кольцо. Поэтому у кабеля просто нет свободного конца, на который надо поставить терминатор. Продвижение информации осуществляется от первому ко второму, от второго к третьему и так далее, а от последнего к первому (рисунок 4.6).

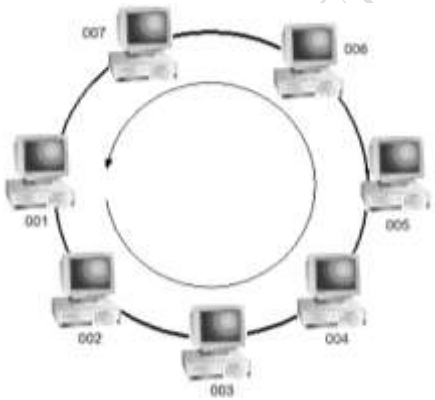


Рисунок 4.6 – Пример сети, построенной топологии «кольцо»

Кольцевой топологией легче управлять, чем шинной, поскольку оборудование, используемое для построения кольца, упрощает локализацию дефектного узла или неисправного кабеля. Данная топология хорошо подходит для передачи сигналов в локальных сетях, поскольку она справляется с большим сетевым трафиком лучше, чем шинная топология. В целом можно сказать, что по сравнению с шинной топологией, кольцевая обеспечивает более надежную передачу.

Сигналы передаются по кольцу в одном, либо обоих направлениях и проходят через каждый компьютер. В отличие от пассивной топологии «шина», здесь каждый компьютер

выступает в роли повторителя, усиливая сигналы и передавая их следующему компьютеру. Поэтому, если выйдет из строя один компьютер, прекращает действовать вся сеть. Интерфейс связи может быть реализован в виде внешнего трансивера, либо быть встроенным в сетевой адаптер. Для обеспечения бесперебойной работы он должен быть всегда включен и иметь возможность замыкания кольца при отключении узла сети (рисунок 4.7).

Рисунок 4.7 — Пример работы сети с топологией «кольцо»

Расширяемость сети, то есть степень простоты добавления новых элементов, в отличие от топологии «шина», – достаточно трудоемкий процесс, особенно если вновь подключаемый элемент расположен в стороне от уже существующей кабельной инфраструктуры.

Звездообразная топология (star topology), или просто «звезда», является старейшим способом передачи сигналов, имеющим свое начало в коммутационных телефонных станциях. Несмотря на возраст, достоинства при использовании в сетях делают звездообразную топологию удачным выбором для современных сетей.

В этом случае все компьютеры, подключаемые к сети, соединяются кабелем с «центральным элементом», в качестве которого может использоваться специальный компьютер – узел сети (рисунок 4.8).

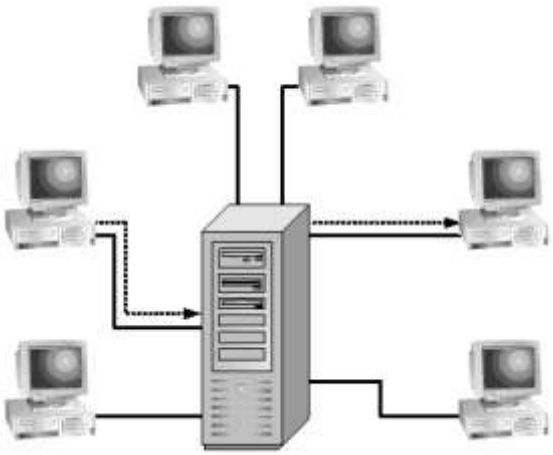


Рисунок 4.8 – Передача информации в топологии «звезда»

Сигналы от передающего компьютера поступают через центральный элемент (например, сервер) ко всем остальным, что является основой терминальных систем.

Звезда является частным случаем дерева, поэтому сети с топологией звезда образуют иерархически подчиненную систему.

Несмотря на большие расходы кабеля, чем у топологии «шина», топология звезда считается дешевой, а поэтому – довольно распространенной. Максимальная скорость

передачи ограничена типом центрального элемента и возможностями передающей среды. Надежность центрального элемента является узким местом и основным недостатком сети.

С точки зрения организации качественного обслуживания запросов пользователей (например, при организации работы сети терминальных клиентов) данная структура остается актуальной.

Расширяемость такой сети, то есть степень простоты добавления новых элементов, довольно высокая. Достаточно соединить новый узел с центральным элементом сети. Если свободных портов в центральном элементе нет, его можно заменить или установить дополнительный специализированный многопортовый сетевой адаптер (рисунок 4.9).

Недостатком «звезды» является то, что центральный элемент является единственной точкой отказа и при выходе его из строя все подключенные узлы теряют возможность передачи данных.

Другим недостатком является то, что для «звезды» требуется больше кабеля, чем для «шины», но этот недостаток уже считается несущественным, поскольку кабельные системы топологии «звезда», как правило, поддерживают гораздо более высокие скорости информационного обмена.

Рисунок 4.9 – Многопортовый сетевой адаптер Ethernet

Более дешевой практической реализацией топологии «звезда» стали комбинированные варианты топологий «звезда-шина» и «звезда-кольцо» со специализированным центральным элементом (рисунок 4.10).

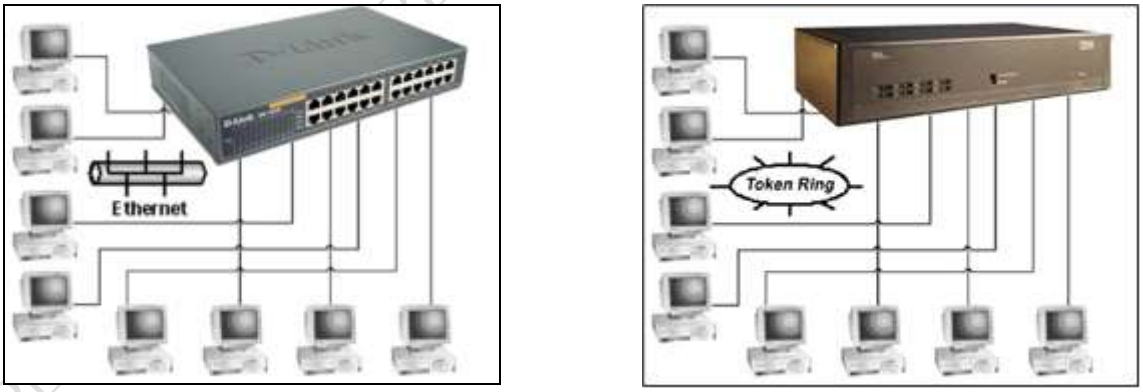


Рисунок 4.10 – Пример внешнего подобия физических структур сетей с комбинированными топологиями «звезда-шина» и «звезда-кольцо»

Применение в качестве центрального элемента активного устройства, рассчитанного на объединение с себе подобными в плоскостные или иерархические структуры (рисунок 4.11), серьезно удешевляет стоимость сети по сравнению с первоначальной топологией «звезда». Этот факт позволил комбинированным топологиям серьезно потеснить применение последней при проектировании локальных сетей.

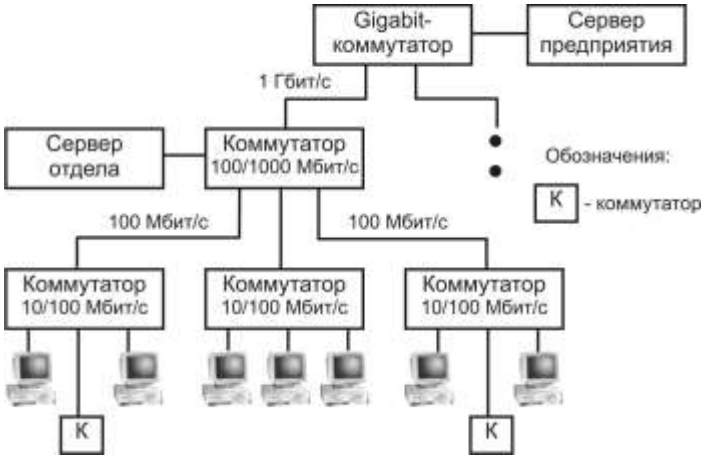


Рисунок 4.11 – Каскадное построение сетевой структуры

Сеть с *ячеистой топологией* обладает высокой избыточностью и надежностью, так как каждый компьютер в такой сети соединен с любым возможным участником соединения отдельным кабелем, то есть реализуется принцип «каждый с каждым» (рисунок 4.12).

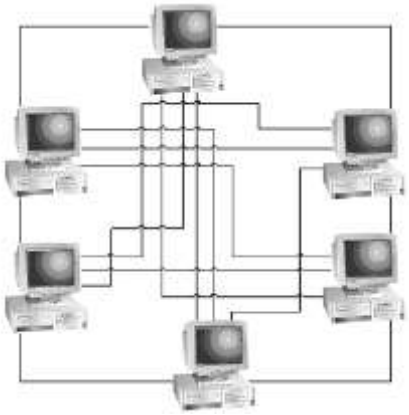


Рисунок 4.12 – Пример сети, построенной по ячеистой топологии

Сигнал от передающего узла к принимающему узлу может проходить по разным маршрутам, поэтому разрыв кабеля не сказывается на работоспособности сети.

Нередко ячеистая топология может быть реализована частично на наиболее важных направлениях в комбинации с остальными топологиями при построении относительно больших сетей (рисунок 4.13).

Высокая скорость доставки сообщений в такой сети обусловлена непосредственной пересылкой от передающего узла к принимающему или по маршруту с минимальным числом пересылок, в случае отсутствия прямого пути.

Такая топология применяется только в тех случаях, когда необходимо обеспечить максимальную надежность и скорость доставки сообщений. Поэтому изначально сети данной топологии проектировались по заказу военных.

Расширяемость сети для такой топологии – очень сложная и дорогостоящая операция, по сравнению с другими топологиями. Чаще всего отдельные элементы этой топологии реализованы в глобальных сетях, для чего используются линии связи общего доступа. Большие затраты на прокладку кабеля компенсируются высокой надежностью и простотой обслуживания.

Смешанная топология, как правило, является продуктом объединения разнородных сетей в рамках общей информационно-вычислительной системы.

К свойствам сетей со смешанной топологией можно отнести следующие технические моменты, которые невозможно реализовать в рамках других топологий:

− использование сетевого оборудования различных сетевых архитектур в рамках единой сети;

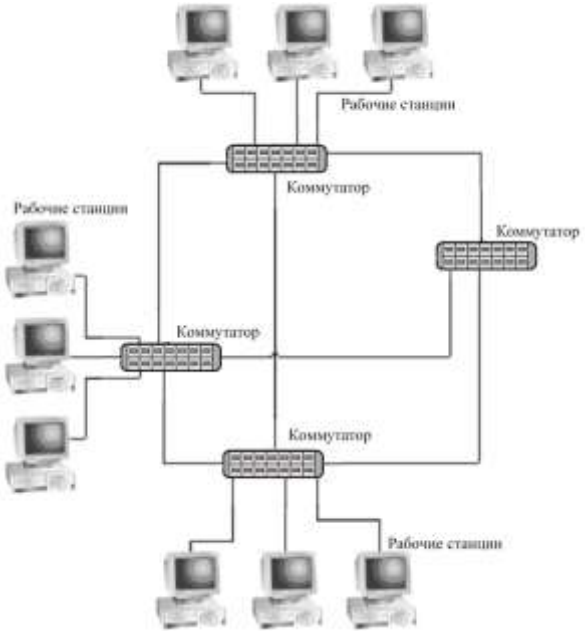


Рисунок 4.13 – Пример сети с элементами ячеистой топологии

− использование разнородных сред передачи данных (за исключением случаев, описанных спецификациями сетевых стандартов);

− возможность объединения в одну информационно-вычислительную систему архитектурно несовместимых вычислительных комплексов и машин;

− организация эффективного обмена информацией в сетях с несколькими вариантами маршрутов доставки сообщений от узла-отправителя к узлу-получателю;

− организация эффективного обмена данными с клиентом сети, находящимся в состоянии движения.

Для локальных сетей применение смешанных топологий является дорогостоящим и, на текущий момент времени, редко применяемым решением. Причиной этого является сложность разработки системы управления и поддержки работоспособности подобной структуры.

Для сетей масштаба города (MAN) смешанная топология является удобным решением при организации обмена данными, которое максимально соответствует всем задачам сетей данного масштаба.

Для глобальных и виртуальных частных сетей – это единственный возможный вариант реализации обмена данными.

Чаще всего для объединения разнородных сегментов применяется специализированное оборудование, осуществляющее трансформацию пакетов из вида, приемлемого для сети отправителя в приемлемый для сети назначения. К числу такого оборудования относятся мосты, маршрутизаторы, шлюзы и их гибриды.

При использовании иерархических схем объединения сетевых сегментов, одна из используемых топологий будет считаться сетеобразующей, а остальные будут выступать в качестве расширения.

Например, топология «звезда» является сетеобразующей для следующей сложной сети (рисунок 4.14).

В других случаях сеть верхнего уровня не считается сетеобразующей, а выполняет только функцию общей информационной магистрали (рисунок 4.15).

Таким образом, можно видеть, что смешанные топологии могут быть изначально заложены в проект сети, чтобы иметь возможность воспользоваться лучшими из их характеристик.

Рисунок 4.14 – Иерархическая сеть

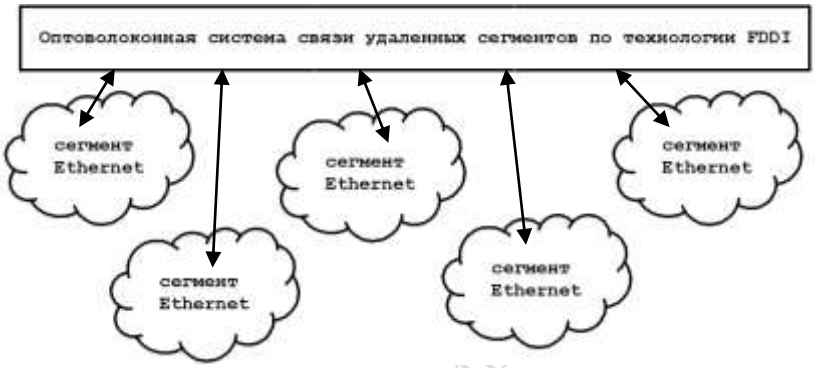


Рисунок 4.15 – Локальная сеть Ethernet с использованием скоростной магистрали дальнего действия FDDI

Практика построения и эксплуатации сетевых технологий показала, что иногда смешанная топология может также стать средством применения специализированного оборудования, несовместимого с сетевым стандартом основной сети.

4.3 Методы доступа к среде

Процедура определения возможности хостом права размещения своих данных в сетевой среде в первую очередь является алгоритмом. В случае соединения двух абонентов прямой линией связи (point to point) алгоритм является простым, линейным и передается на протоколы более высоких уровней ISO/OSI. В случае необходимости управляемого доступа к среде множества абонентов алгоритмы строятся с учетом технических и/или программных ограничений.

Метод с передачей маркера неконкурентный – в нем два компьютера не могут начать передавать сигнал одновременно. В этом случае специальный служебный кадр (*маркер*) курсирует по строго определенной траектории. Если какой-либо из компьютеров нуждается в разрешении провести передачу, он дожидается момента, когда этот маркер приходит к нему, дополняет или заменяет его информацией и отправляет дальше. Получившийся кадр следует дальше, пока не достигнет пункта назначения или не вернется к отправителю.

Когда кадр достигает компьютера, адрес которого указан в заголовке, сетевой адаптер компьютера копирует данные, добавляет к пакету подтверждение об успешном приеме и передает дальше по кругу. Компьютер, передавший эти данные, получает кадр с подтверждением, после чего освобождает маркер, т. е. возвращает его к исходному виду. Этот процесс показан на рисунке 4.16.

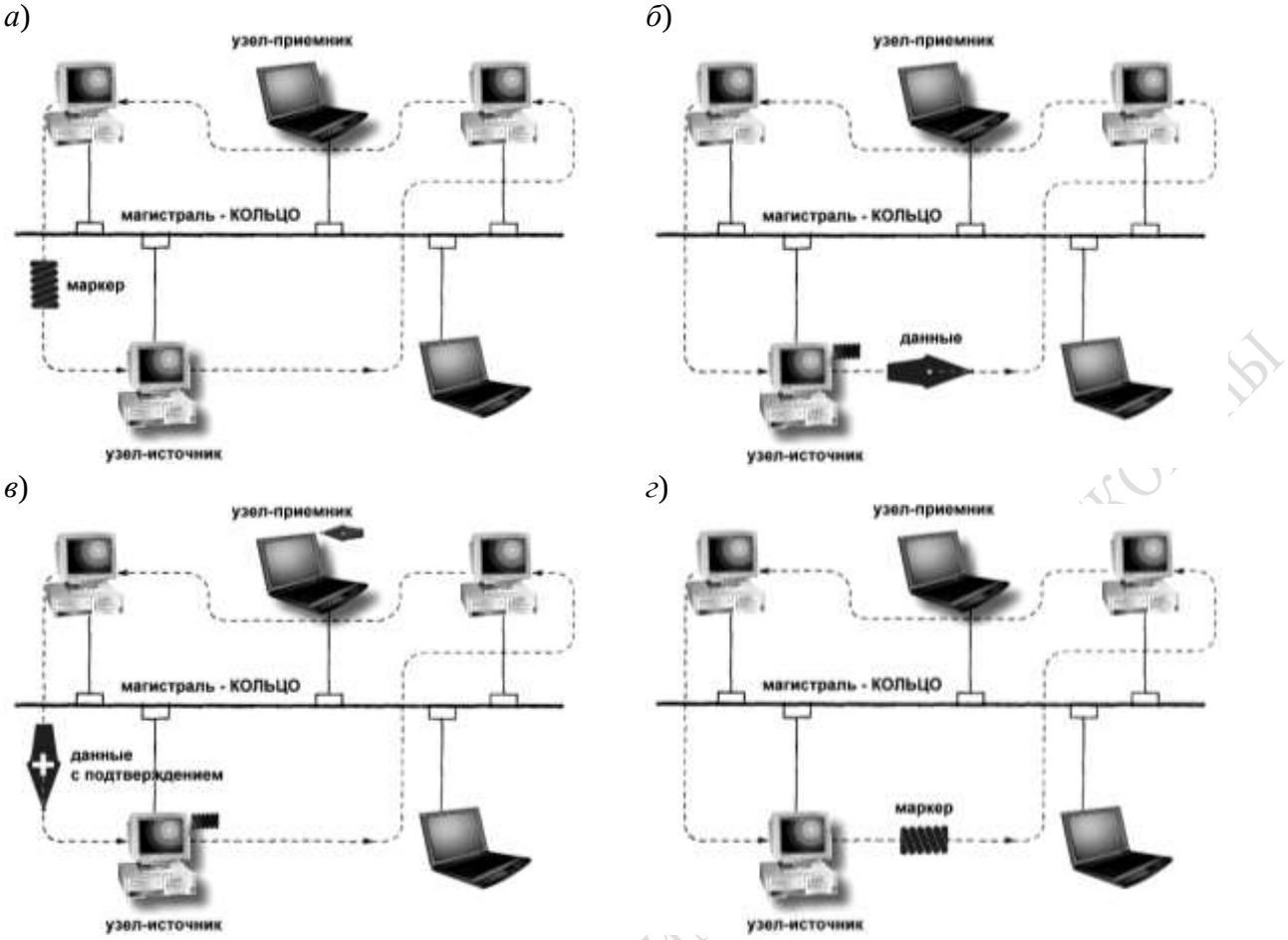


Рисунок 4.16 – Принцип действия маркерного доступа:
а) ожидание маркера; б) передача кадра;
в) возврат кадра; г) освобождение маркера.

Время удержания одной станцией маркера ограничивается *тайм-аутом удержания маркера,* после истечения которого станция обязана передать маркер далее по кольцу. В сетях Token Ring 16 Мб/с используется также несколько другой алгоритм доступа к кольцу, называемый алгоритмом *раннего освобождения маркера (Early Token Release).* В соответствии с ним станция передает маркер доступа следующей станции сразу же после окончания передачи последнего бита кадра, не дожидаясь возвращения по кольцу этого кадра с битом подтверждения приема.

Каждая станция применяет механизмы обнаружения и устранения неисправностей сети, возникающих в результате ошибок передачи или переходных явлений (например, при подключении и отключении станции).

Не все станции в кольце равны. Одна из станций обозначается как *активный монитор,* что означает дополнительную ответственность по управлению кольцом. Активный монитор осуществляет управление тайм-аутом в кольце, порождает новые маркеры (если необходимо), чтобы сохранить рабочее состояние, и генерирует диагностические кадры при определенных обстоятельствах. Активный монитор выбирается, когда кольцо инициализируется, и в этом качестве может выступить любая станция сети. Если монитор отказал по какой-либо причине, существует механизм, с помощью которого другие станции (резервные мониторы) могут договориться, какая из них будет новым активным монитором.

Для различных видов сообщений передаваемым данным могут назначаться различные *приоритеты.* Каждый кадр или маркер получает приоритет, устанавливаемый битами приоритета (от 0 до 7). Станция может воспользоваться маркером, если только она получила

маркер с приоритетом, меньшим или равным, чем ее собственный. Сетевой адаптер станции, если ему не удалось захватить маркер, помещает свой приоритет в резервные биты маркера, но только в том случае, если записанный в резервных битах приоритет ниже его собственного. Эта станция будет иметь преимущественный доступ при последующем поступлении к ней маркера.

Чаще всего методы с использованием маркера применяются в сетях с *кольцевой топологией* (например, Token Ring и FDDI), однако ничто не мешает передавать маркер и в сетях с другими видами топологий (например, ArcNet – маркерная шина).

Carrier Sense Multiple Access with Collision Detection (CSMA/CD) - множественный доступ с контролем несущей и обнаружением коллизий.

Несущая (*Carrier*) – это информационный сигнал, транслируемый любым сетевым устройством во время передачи данных. Если узел, готовящийся начать передачу, опознает несущую (*Carrier-Sense, CS*), то он откладывает передачу своего кадра данных до окончания чужой передачи.

Компьютеры постоянно конкурируют за право передачи. Для этого все сетевые адаптеры, независимо от того, собираются они передавать информацию или нет, «прослушивают» среду передачи, стремясь обнаружить передаваемые данные.

Это позволяет решить следующие задачи:

− любой компьютер сети находится в постоянной готовности принять информацию, адресованную ему;

− производится поиск момента, когда среда передачи освобождается, ведется только отправителем.

Основная ошибка в конкурентных методах доступа к среде – это *коллизия* (*collision, столкновение кадров*). Она возникает в случае одновременной попытки передачи информационных кадров от двух и более компьютеров одновременно (рисунок 4.17), что обусловлено особенностями распространения сигнала в сетях передачи данных, построенных по шинной топологии. В этом случае передаваемые данные взаимно разрушаются.

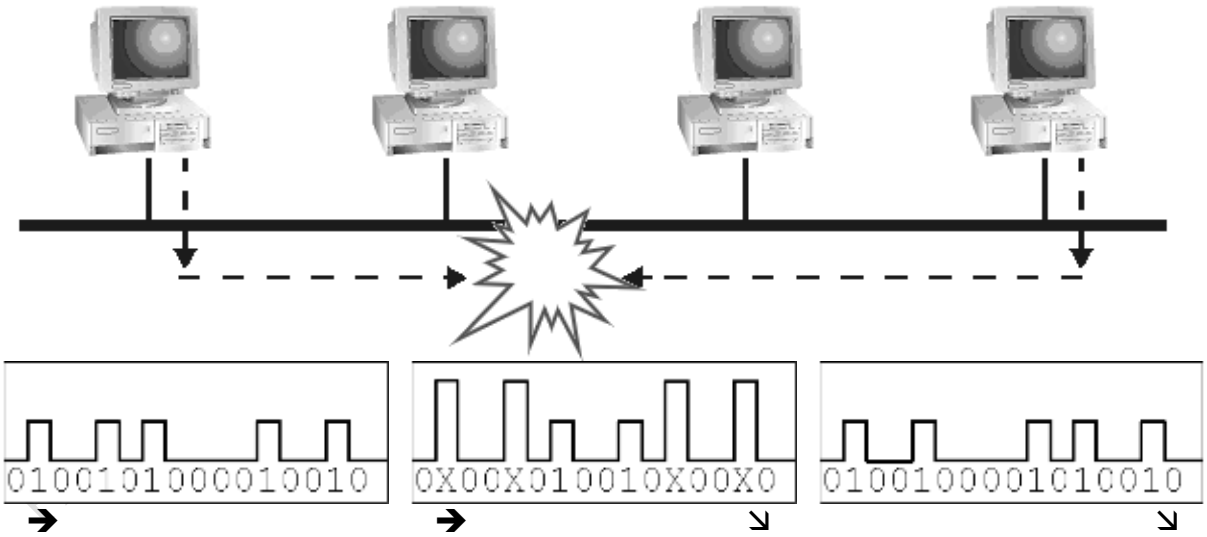


Рисунок 4.17 – Возникновение коллизии в сети с общей шиной

Вероятность возникновения коллизии тем выше, чем дальше находятся друг от друга участники соединения и чем большее число компьютеров подключено к сегменту сети. Вероятность возникновения повторной коллизии выше, чем у первичной коллизии.

Обнаружение коллизии может осуществляться по увеличению амплитуды при взаимном наложении сигнала. Направление движения пакетов на рисунке показано стрелочками.

Чтобы корректно обработать коллизию, все станции одновременно наблюдают за возникающими на кабеле сигналами. Если передаваемые и наблюдаемые сигналы отличаются, то фиксируется обнаружение коллизии (*Collision Detection, CD*). Для увеличения вероятности немедленного обнаружения коллизии всеми станциями сети, ситуация коллизии усиливается посылкой в сеть станциями, начавшими передачу своих кадров, специальной последовательности битов, называемой jam-последовательностью.

После обнаружения коллизии передающая станция обязана прекратить передачу и ожидать в течение случайного интервала времени, а затем может снова сделать попытку передачи кадра. Узел делает максимально 16 попыток передачи этого кадра информации, после чего отказывается от его передачи. Величина задержки выбирается как равномерно распределенное случайное число из интервала, длина которого экспоненциально увеличивается с каждой попыткой – такой выбор величины задержки снижает вероятность коллизий и уменьшает интенсивность выдачи кадров в сеть.

Метод доступа CSMA/CD применяется в стандарте сетевой технологии Ethernet, что определяет его широкую популярность.

Метод доступа с использованием приоритетов (Demand Priority) –разрабатывался как способ повышения пропускной способности сети по сравнению с методом доступа CSMA/CD. Применялся в сетях Fast Ethernet – 100 Anylan Voice Guide с использованием UTP Cat 3 или оптоволокна.

При использовании UTP Cat 3 все четыре пары кабеля используются для передачи данных. Каждая пара поддерживает скорость передачи 30 Мбит/с. Используется схема кодирования 5B/6B. Содержимое MAC-кадра сегментируется на квинтеты и сопровождается битом четности. После кодирования передача идет по 4 каналам в круговом порядке.

Передачи не являются широковещательными на все другие компьютеры сети. Компьютеры не борются самостоятельно за доступ к среде, но работают под централизованным управлением. Для этого необходима сеть с организацией кабельной системы по топологии «звезда». Центральным узлом сетевой архитектуры может быть компьютер, мост, маршрутизатор или коммутатор.

Каждому компьютеру – участнику сетевого соединения присваивается характеристика, называемая приоритетом передачи данных. Эти приоритеты бывают статические и динамические. В одних сетях предполагалось, что они будут назначаться администратором, а в других – сетевыми менеджерами.

В случае, если два компьютера одновременно отправляют свои данные, центральный элемент сравнивает приоритеты и осуществляет передачу лишь тех данных, которые имеют более высокий приоритет. Данные второго компьютера отбрасываются (рисунок 4.18). При равном приоритете передаваемых данных сохраняемый блок данных выбирается случайным образом.

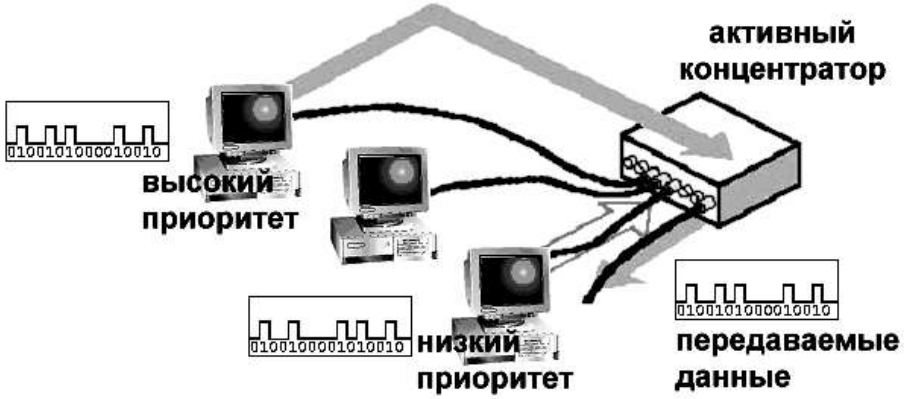


Рисунок 4.18 – Предотвращение коллизии в сетях Demand Priority

Статическое распределение приоритетов может заключаться в закреплении приоритета за номером порта центрального элемента с последовательным уменьшением или увеличением.

При динамическом назначении приоритетов центральный элемент автоматически управляет доступом к сети, делая циклические опросы всех узлов сети, проверяя их работоспособность и переопределяя приоритеты. При этом, если компьютер долгое время не участвует в сетевом обмене, его приоритет можно повысить.

Метод доступа *Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)* – множественный доступ с контролем несущей и предотвращением коллизий практически аналогичен CSMA/CD. В нем компьютеры также конкурируют за право передачи, и для этого постоянно ведется контроль несущей. Отличие заключается в том, что для разрешения передачи информации отправитель запрашивает подтверждение от всех компьютеров в сети, для этого он формирует и передает в сеть сигнал запроса на передачу – RTS (*Request to Send*).

Получив пакет RTS, компьютер, который не собирается сам передавать информацию, сразу отправляет разрешение. Если компьютер сам собирается передавать информацию и уже отправил свой RTS, то он сравнивает временные отметки своего RTS и полученного, после чего решает: высылать разрешение или поставить пришедший RTS в очередь. В таком случае вероятность возникновения коллизии минимальна, но в сети большое количество широковещательных сообщений (рисунок 4.19). Поэтому эффективность использования канала связи у CSMA/CA ниже, чем у CSMA/CD. Ранее метод использовался в *иерархических топологиях* («*звезда», «дерево»*), примером являлась сетевая архитектура AppleTalk.

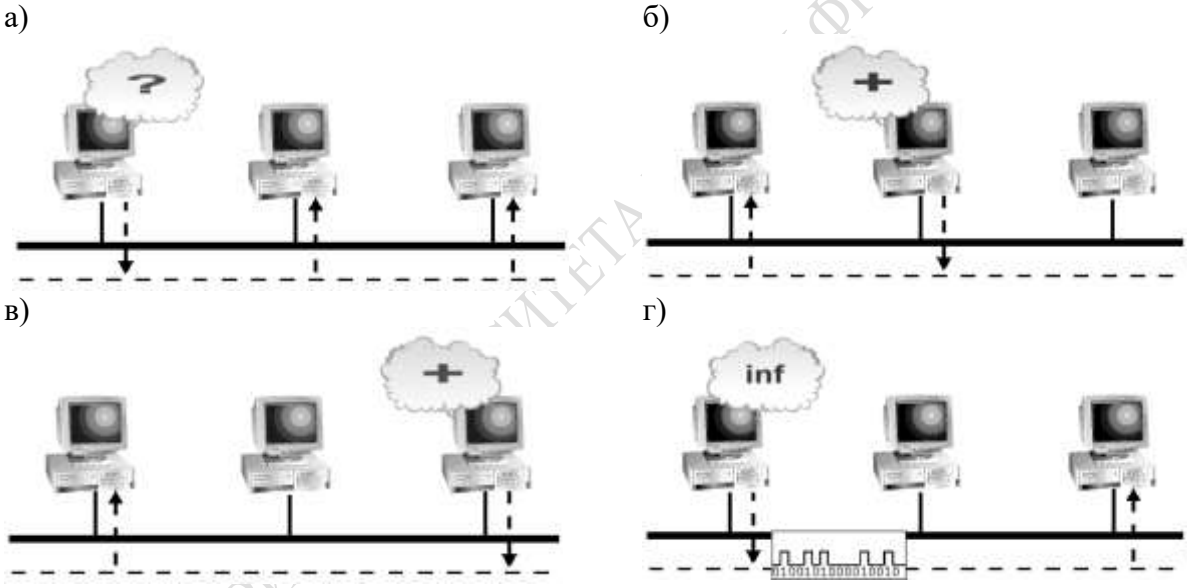


Рисунок 4.19 – Процесс сетевого обмена в сетях CSMA/CA:
а) запрос на право доступа к среде; б) и в) подтверждение на доступ к среде от всех участников сетевого обмена; г) передача данных.

Обновленная версия CSMA/CA, которая также называется функцией распределенной координации (*distributed coordination function*), применяется в беспроводных сетях.

В этом случае станция, ожидающая возможности передачи, прослушивает частоту коммуникаций и определяет ее занятость, проверяя уровень индикатора мощности сигнала в приемнике (Receiver Signal Strength Indicator, RSSI). В тот момент, когда передающая частота свободна, наиболее вероятно возникновение конфликтов между двумя станциями, которые одновременно захотят начать передачу. Когда передающая частота освобождается, каждая станция ждет несколько секунд (их число определяется параметром DIFS), чтобы убедиться в том, что частота остается незанятой.

DIFS – это аббревиатура от термина *Distributed coordination function's Intra Frame Space* – интервал между кадрами функции распределенной координации, который определяет заранее установленное время обязательного ожидания (задержки).

Если станции ожидают в течение времени, определенного интервалом DIFS, вероятность возникновения конфликта между станциями уменьшается, поскольку для каждой станции, требующей передачи, вычисляется разное значение времени задержки (отсрочки), по истечении которого станция снова будет проверять занятость передающей частоты.

Если на момент истечения интервала DIFS:

− частота остается незанятой, то передачу начинает станция, имеющая минимальное время отсрочки;

− частота оказывается занятой, то станция, требующая передачи, ждет, пока частота не освободится, после чего простаивает еще в течение индивидуального времени отсрочки.

При определении времени отсрочки длительность заранее заданного интервала времени умножается на случайное число. Временной интервал – это некоторое значение, хранящееся в базе управляющей информации, имеющейся на каждой станции. Значение случайного числа лежит в диапазоне от нуля до величины максимального размера окна конфликтов. Размер окна конфликтов также хранится в базе управляющей информации станции. Таким образом, для каждой станции, ожидающей передачи, определяется уникальное время отсрочки, что позволяет станциям избегать конфликтов.

Важной модификацией при построении алгоритмой доступа к среде стали механизмы распараллелизации ее использования (*уплотнение*) однотипным оборудаванием неконкурентными способами. Примеры уплотнение каналов связи представлены в таблице 4.1.

Таблица 4.1 – Свойства методов уплотнения каналов связи

Метод уплотнения каналасвязи	Разделяемый ресурс	Преимущества
Frequency Division Multiple Access, FDMA	Частота	Простота реализации.
Time Division Multiple Access, TDMA	Время	Масштабируемость.
Code Division Multiple Access, CDMA	Код	Максимальное распределение ресурсов канала связи

FDMA разбивает весь частотный спектр канала связи на поддиапазоны равной/неравной ширины, симметричные/несимметричные в обоих направлениях. Каждый из этих поддиапазонов представляет собой канал связи, который назначается отдельной паре абонентов. Этот канал будет им доступ на протяжение всего времени сеанса связи. FDMA обычно используется в аналоговых системах связи. В сотовой связи применяется в стандартах: NMT (Nordic Mobile Telephone); LTE (Long Term Evolution); Mobile WIMAX (Worldwide Interoperability for Microwave Access) и др.

TDMA предусматривает, что весь канал связи, со всей полосой пропускания будет предоставлен каждому из абонентов, но на небольшой промежуток времени – таймслот. Через некоторое время ему снова будет доставлен этот же канал на такой же по длительности промежуток времени и т.д. пока будет длиться сеанс связи. TDMA обычно применяется для передачи цифровых сигналов, потому что им требуется широкая полоса пропускания, ресурс по времени может быть ограничен и разбит на короткие промежутки. Этот метод нашел применение в стандартах сотовой связи GSM (Global System for Mobile Communications), UMTS (Universal Mobile Telecommunications System), LTE.

Принцип *CDMA* заключается в том, что перед передачей в эфир информационный сигнал перемножается со специальным ортогональным кодом. Если на приемном конце снова

перемножить эту последовательность на первоначальный ортогональный код, то мы получим исходный сигнал. Попытка восстановить сигнал от другого источника окажется неуспешной. Главная проблема данного метода заключается в том, что невозможно сгенерировать много абсолютно ортогональных кодов. На практике используют *почти ортогональные коды (almost orthogonal / virtually orthogonal codes).* Метод CDMA нашел применение в североамериканском стандарте сотовой связи CDMA 2000.

В современных сетевых структурах LAN часто применяются аналогичные методы уплотнения или их комбинации. Наиболее ярко это можно увидеть при анализе 802.11 (WiFi).

Для установления связи между узлами необходимо применять единый подход к режиму трансляции: симплекс, полудуплекс, дуплекс, мультиплекс.

4.4 Технические спецификации проекта IEEE 802.X

Спецификации протоколов и оборудования, работающих на нижних уровнях сетевых моделей описываются в наборе стандартов проекта IEEE 802. Они охватывают только два нижних уровня модели OSI – физический и канальный. Это связано с тем, что данные уровни составляют основу локальных сетей.

Таким образом, спецификации 802.X распространяются:

- на платы сетевых адаптеров;
- на оборудование глобальных вычислительных сетей;
- на компоненты кабельных и беспроводных сетей.

То есть, спецификации данного проекта определяют способы, в соответствии с которыми платы сетевых адаптеров осуществляют доступ к физической среде и передают по ней данные. Сюда относятся соединение, поддержка и разъединение сетевых устройств.

В рамках данного параграфа затрагиваются:

- 802.3 - набор стандартов и спецификаций Ethernet
- 802.11 - набор стандартов и спецификаций по беспроводным локальным сетям (Wireless LAN)
- 802.15 - набор стандартов и спецификаций по беспроводным персональным сетям (Wireless Personal Area Network, WPAN)
- 802.16 - набор стандартов и спецификаций по системам широкополосного беспроводного доступа (Broadband Wireless Access)

Стандарт Ethernet (802.3) является продуктом совместной разработки Xerox Corporation, Digital Equipment и Intel в 1979 году на основе разработок Xerox Corporation, сделанных еще в 1975 году.

Основная топология сети – «шина» и «звезда – шина».

Метод доступа к среде – CSMA/CD.

Скорость передачи данных зависит от реализации (таблица 4.2).

Физическая среда передачи – коаксиальный кабель, оптоволокно, витая пара и другие виды кабельных и беспроводных связей.

На физическом уровне Ethernet используют кодирование сигнала, которое для соблюдения технологии совместимости осуществляется «сверху-вниз» практически во всех стандартах одинаково. Эффективная длина сегмента зависит от используемой среды передачи и колеблется от 100 м для витой пары до 80 км при использовании оптоволокна.

Формат кадра для сети Ethernet является его основной логической единицей, обеспечивающей совместимость различных версий. Его структура представлена на рисунке 4.20. Максимальная длина кадра 802.3 - 1522 байта.

Таблица 4.2 - Выдержка перечня спецификаций IEEE 802.3

Ethernet standard	Date	Description
IEEE 802.3 standard	1983	10BASE5 10 Mbit/s (1.25 MB/s) over thick coax. Same as Ethernet II (above) except Type field is replaced by Length, and an 802.2 LLC header follows the 802.3 header. Based on the CSMA/CD Process.
802.3a	1985	10BASE2 10 Mbit/s (1.25 MB/s) over thin Coax (a.k.a. thinnet or cheapernet)
802.3i	1990	10BASE-T 10 Mbit/s (1.25 MB/s) over twisted pair
802.3j	1993	10BASE-F 10 Mbit/s (1.25 MB/s) over optical fiber
802.3u	1995	100BASE-TX, 100BASE-T4, 100BASE-FX Fast Ethernet at 100 Mbit/s (12.5 MB/s) with autonegotiation
802.3y	1998	100BASE-T2 100 Mbit/s (12.5 MB/s) over voice-grade twisted pair
802.3z	1998-07	1000BASE-X Gbit/s Ethernet over optical fiber at 1 Gbit/s (125 MB/s)
802.3ab	1999-06	1000BASE-T Gbit/s Ethernet over twisted pair at 1 Gbit/s (125 MB/s)
802.3ae	2002-06	10 Gigabit Ethernet over fiber; 10GBASE-SR, 10GBASE-LR, 10GBASE-ER, 10GBASE-SW, 10GBASE-LW, 10GBASE-EW
802.3an	2006-06	10GBASE-T 10 Gbit/s (1,250 MB/s) Ethernet over unshielded twisted pair (UTP)
802.3bm	2015-02	100G/40G Ethernet for optical fiber
802.3bq	2016-06	25GBASE-T/40GBASE-T Ethernet for 4-pair balanced twisted pair cabling with 2 connectors over 30 m distances
802.3bs	2017-12	200GbE (200 Gbit/s) over single-mode fiber and 400GbE (400 Gbit/s) over optical physical media
802.3bz	2016-09	2.5GBASE-T and 5GBASE-T – 2.5 Gigabit and 5 Gigabit Ethernet over Cat-5e/Cat-6 twisted pair
802.3cb	2018-09	2.5 Gbit/s and 5 Gbit/s Operation over Backplane
802.3cn	2019-11	50 Gbit/s (40 km), 100 Gbit/s (80 km), 200 Gbit/s (four λ, 40 km), and 400 Gbit/s (eight λ, 40 km and single λ, 80 km over DWDM) over Single-Mode Fiber and DWDM
802.3df	(TBD)	200 Gb/s, 400 Gb/s, 800 Gb/s, and 1.6 Tb/s using 200 Gbit/s lanes, also using eight/sixteen 100 Gbit/lanes for 800 and 1600 Gbit/s, chaired by John D'Ambrosia
802.3dg	(TBD)	100BASE-T1 and 1000BASE-T1 extended length to 500 m

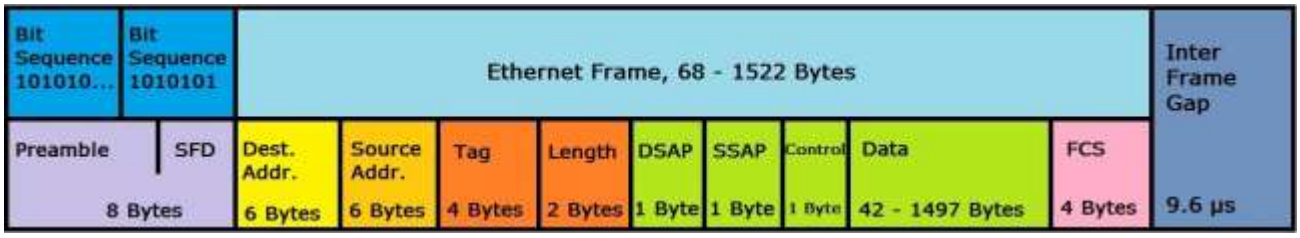


Рисунок 4.20 – Формат кадра для сети Ethernet

Стандарт WiFi (802.11) является товарным знаком Wi-Fi Alliance. Стандарт вышел на рынок в 1997 году. По состоянию на 2017 год в Wi-Fi Alliance входило более 800 компаний со всего мира.

Модель обслуживания – базовый набор услуг (BSS) и независимый базовый набор услуг (IBSS).

Метод доступа к среде – CSMA/CA.

Скорость передачи данных зависит от реализации (таблица 4.3).

Таблица 4.3 - Выдержка перечня спецификаций IEEE 802.11

Generation	IEEE Standard	Maximum Linkrate (Mbit/s)	Adopted	Radio Frequency (GHz)
Wi-Fi 7	802.11be	40000	TBA	2.4/5/6
Wi-Fi 6E	802.11ax	600 to 9608	2020	2.4/5/6
Wi-Fi 6			2019	2.4/5
Wi-Fi 5	802.11ac	433 to 6933	2014	5
Wi-Fi 4	802.11n	72 to 600	2008	2.4/5
(Wi-Fi 3*)	802.11g	6 to 54	2003	2.4
(Wi-Fi 2*)	802.11a	6 to 54	1999	5
(Wi-Fi 1*)	802.11b	1 to 11	1999	2.4
(Wi-Fi 0*)	802.11	1 to 2	1997	2.4
*: (Wi-Fi 0, 1, 2, 3, are unbranded common usage.)				

Физическая среда передачи – радиочастотный диапазон от 1 до 7 ГГц.

Для обеспечения более высокой скорости сетевого обмена в рамках одного сеанса связи в 802.11 предусмотрена возможность объединения независимых частотных каналов в логическую группу (рисунок 4.21).

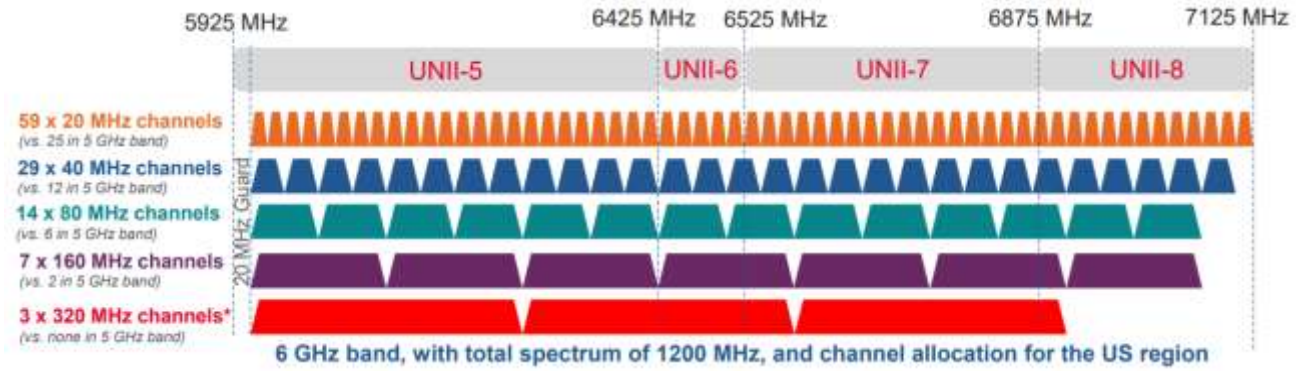


Рисунок 4.21 – Объединение частотных каналов WiFi

Максимальная длина кадра 802.11 - 2346 байтов (рисунок 4.22).

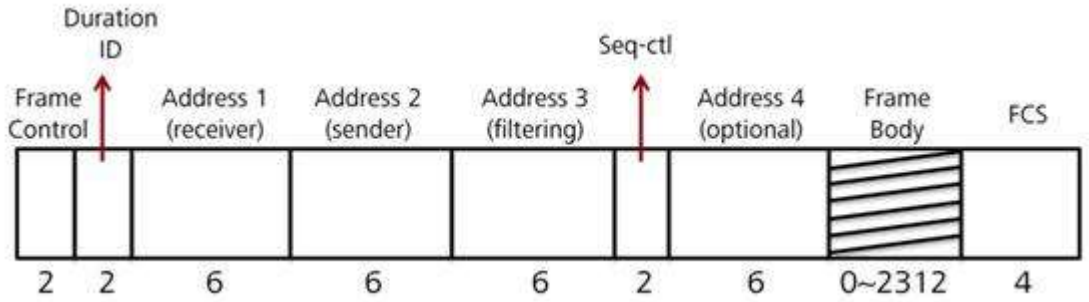


Рисунок 4.22 – Формат кадра для сети WiFi

Стандарт Bluetooth (802.15) в первой версии был опубликован в 1999 году как результат разработок Ericsson Mobile, IBM и Intel, стартовавших в 1994 году (рисунок 4.23).

Основная топология сети – «точка-точка» и «звезда».

Метод доступа к среде – централизованное управление.

Скорость передачи данных переменная из-за требований оптимизации мощности сигнала. В зависимости от режима от 1 до 50 Мбит/с.

Физическая среда передачи – радиочастотный диапазон 2,4 ГГц.

Эффективная зона покрытия – 10 м.

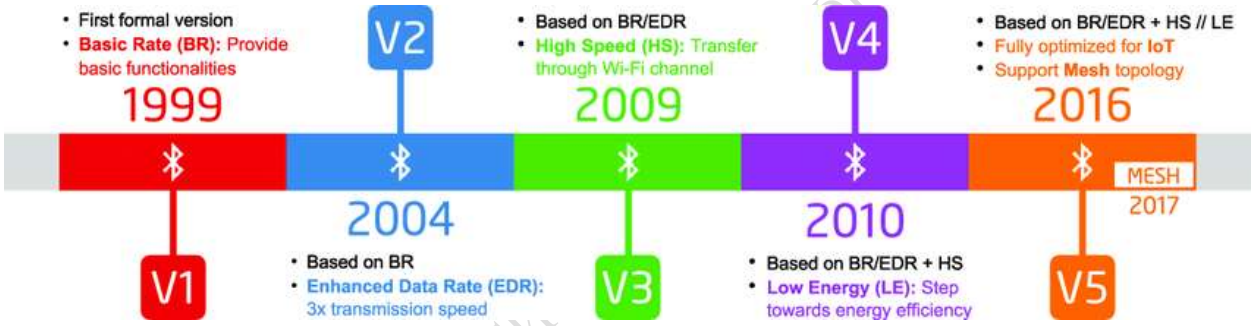


Рисунок 4.23 – Развитие стандарта Bluetooth

Все кадры передаются между главным и подчиненными узлами по логическому каналу, называемому соединением. Существует два типа соединений. Первый называется ACL (Asynchronous ConnectionLess – асинхронный без установления связи) и он используется для коммутации пакетов данных, которые могут появиться в произвольный момент времени. Кадры могут теряться и пересылаться повторно. У подчиненного узла может быть только одно ACL-соединение со своим главным узлом. Второй вид соединения называется SCO (Synchronous Connection Oriented – синхронный с установлением связи). Он предназначен для передачи данных в реальном масштабе времени – это требуется, например, при телефонных разговорах. Такой тип канала получает фиксированный временной интервал для передачи в каждом из направлений. Кадры, переданные по данному типу канала, никогда не пересылаются заново.

Максимальная длина кадра Bluetooth - 2744 байта (рисунок 4.24).

Рисунок 4.24 – Формат кадра для сети Bluetooth

Сеть Bluetooth состоит из одного главного узла и нескольких (до семи) активных подчиненных узлов. Помимо активных узлов, один главный узел может поддерживать до 255 так называемых «отдыхающих» узлов. Это устройства, которые главный узел перевел в режим пониженного энергопотребления.

4.5Локализация трафика уровня L2

Подуровень MAC канального уровня модели OSI работает с физическими адресами, которые называются MAC-адресами.

Физические адреса источника и места назначения канального уровня необходим для доставки кадра канала данных от одной сетевой интерфейсной платы (NIC) к другой сетевой интерфейсной плате в той же сети. MAC-адреса аппаратно прошиты в чипсет сетевого адаптера и являются основной локальной адресацией.

MAC-адресация применяется в сетях Ethernet, Fast Ethernet, Token-Ring, FDDI, 100 VG-AnyLAN и представляют собой 12 шестнадцатеричных цифр (48 бит), записанных в микросхему сетевого адаптера (например, 17:A4:2C:43:2F:09).

В качестве MAC-адреса могут использоваться данные двух типов:

- 48-битный расширенный уникальный идентификатор (Extended Unique Identifier);
- EUI-48 - это идентификатор, созданный путём соединения 24-битного OUI с 24-битным OUA (рисцнок 4.25).

дополнительным идентификатором, который назначается организацией, получившей OUI

Эти 48 бит имеют жесткую структуру (рисунок 8.1), при этом два старших разряда адреса управляющие, они определяют тип адреса и способ использования остальных 46 разрядов.

Рисунок 4.25 – Структура MAC-адреса

Старший бит I/G (Individual/Group) указывает на тип адреса. Если он установлен в 0, то индивидуальный, если в 1, то групповой (многопунктовый или функциональный). Пакеты с групповым адресом получат все имеющие этот групповой адрес сетевые адаптеры. Причем групповой адрес определяется 46 младшими разрядами.

Второй управляющий бит U/L (Universal/Local) называется флажком универсального/местного управления и определяет то, как был присвоен адрес данному сетевому адаптеру. Обычно он установлен в 0. Установка бита U/L в 1 означает, что адрес задан не производителем сетевого адаптера, а организацией, использующей данную сеть. Это случается довольно редко.

Для широковещательной передачи (всем абонентам сети одновременно) применяется специально выделенный сетевой адрес, все 48 битов которого установлены в единицу. Его принимают все абоненты сети независимо от их индивидуальных и групповых адресов.

Следующие 22 разряда адреса называются OUI (Organizationally Unique Identifier) – уникальный идентификатор, выделяемый организации.

IEEE присваивает один или несколько OUI каждому производителю сетевых устройств. Это позволяет исключить совпадения адресов адаптеров от разных производителей. Всего возможно свыше 4 миллионов разных OUI, это означает, что теоретически может быть зарегистрировано 4 миллиона производителей. Также за этим полем закрепилось второе название «адресный диапазон».

Существуют сервисы, позволяющие определить производителя по MAC-адресу, они часто реализованы online, чтобы расшифрованные данные были актуальными (рисунок 4.26).

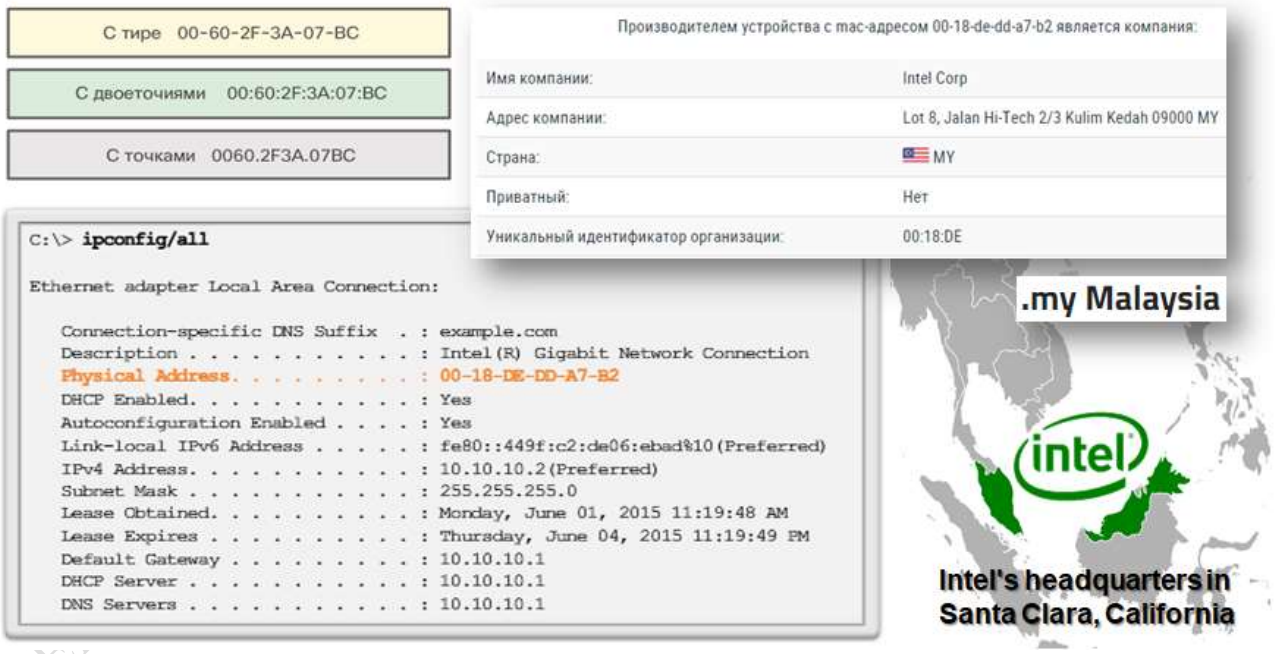


Рисунок 4.26 – Формат представления MAC-адреса и его данные

Младшие 24 разряда называются OUA (Organizationally Unique Address) – уникальный адрес, назначаемый организацией. Именно это поле заполняет каждый из зарегистрированных производителей сетевых устройств. То есть, приобретя всего 1 OUI, возможно назначить 2^{24} адресов, это свыше 16 миллионов комбинаций.

Фактически любая организация может приобрести любое количество адресных диапазонов, но предусмотрена возможность выкупа диапазона частями (таблица 4.4).

Таблица 4.4 – Размер OUI-адренды

Name	Full name	Previously named	Number of Addresses
MA-L	MAC Address Block Large	OUI (Organizationally Unique Identifier)	2^{24} ~= 16 Million
MA-M	MAC Address Block Medium	-	2^{20} ~= 1 Million
MA-S	MAC Address Block Small	OUI-36 (encompasses IAB Assignments)	2^{12} ~= 4,096

Полный адресный диапазон MAC:

2^{48} = 281.474.976.710 656 адресов ≈ 281,5 триллиона адресов

Недостатком MAC-адресации считается сложность структуры сетевых адаптеров, а также большая доля служебной информации в передаваемом кадре (адреса источника и приемника вместе требуют уже 96 бит кадра или 12 байт).

Во многих сетевых адаптерах предусмотрен так называемый циркулярный режим. В этом режиме адаптер принимает все кадры, приходящие к нему, независимо от значения поля адреса приемника. При этом один компьютер принимает и контролирует все кадры, проходящие по сети, но сам ничего не передает. В данном режиме работают сетевые адаптеры мостов и коммутаторы, которые должны обрабатывать перед ретрансляцией все кадры, приходящие к ним.

Система MAC-адресации используется в таких сетях как: Ethernet, Fast Ethernet, Token Ring, FDDI, 100 VG-AnyLAN.

Согласно исходной концепции MAC-адресации: *не должно существовать двух сетевых интерфейсов с одинаковыми MAC-адресами.* Однако на практике при работе с виртуальными машинами и клонированием L2-адресов в ряде сетевых сервисов такая ситуация сейчас обрабатывается штатно. Повторяющиеся MAC-адреса могут вызвать проблемы, если два сетевых интерфейса с одинаковым MAC-адресом принадлежат одному и тому же домену широковещательных рассылок.

Для собственных целей администраторы сетей часто меняют MAC-адрес как динамический параметр «перезаписываемой» микросхемы. Например, сетевые адаптеры, интегрированные в материнские платы отдельных производителей, имеют ручную настройку этого параметра в CMOS-настройках BIOS материнской платы.

Широковещательный домен (broadcast domain) - группа доменов коллизий, соединенных с помощью устройств L2 ISO/OSI. В пределах этого логического участока все узлы могут передавать данные друг другу через конкурентную среду передачи данных, используя алгоритмы методов доступа к среде, без дополнительной обработки кадров данных.

Например, в топологии «точка-точка» это два абонента, связанные единственной линией связи. Для топологии «шина» стандарта 802.3 допустимое число абонетов с конкурентным методом доступа к среде – 1024. За счет локализации зон действия («прозрачности») L2 адресов снижается вероятность возниконовения сбоев и повышается эффективность использования среды передачи данных.

Для реализации части своего функционала L2-устройства накапливают информацию о MAC-адресах присоединенных устройств. Для ускорения процесса применяется особый тип памяти *Content Addressable Memory* (CAM), поэтому часто результирующую таблицу,

размещенную в этой памяти называют CAM-table. Достоинство CAM в том, что она возвращает результат за фиксированное время, не зависящее от количества и размера записей в таблице. Достигается это за счёт того, что значение сравнивается одновременно со всеми записями.

Ограничения в размерах данного модуля памяти и алгоритма работы с ним приводят к двум значительным видам уязвимостей с точки зрения информационной безопасности:

- исчерпание CAM с переводом устройства в режим неуправляемой ретрансляции;
- многочисленные обновления CAM при нарушении требований к избыточности физических соединений, с вероятностью возникновения «широковещательного шторма».

4.6 Сетевые устройства уровня L2

Устройства уровня L2 привязаны к набору спецификаций IEEE 802, поскольку являются исполнительным устройством низкого уровня и от их производительности зависит скорость работы конечного сегмента сети.

К устройствам этого типа можно отнести следующие:

- сетевой мост (*BRIDGE*);
- сетевой коммутатор (*SWITCH*);
- устройства информационной безопасности L2.

Сетевой *Мост* – это устройство, соединяющее между собой сегменты локальной сети или целые сети. Мосты позволяют решать следующие задачи:

- расширить локальную сеть в случае, когда достигнут лимит на максимальное количество соединений (например, если сегмент Ethernet имеет 30 узлов);
- объединить две однородные сети через промежуточный канал другого типа связи (например, модемный мост между сегментами сети);
- расширить локальную сеть и обойти ограничения на длину сегментов (например, если нужно нарастить сегмент Ethernet на тонком кабеле, который уже имеет длину 185 м);
- сегментировать локальную сеть для ликвидации узких мест в сетевом трафике;
- объединять две сети разных сетевых архитектур (например, сеть с топологией «кольцо» можно объединить с сетью с топологией «шина»);
- предотвратить неавторизованный доступ к сети.

Часто мосты применяют для объединения более двух сетей одновременно (рисунок 4.27).

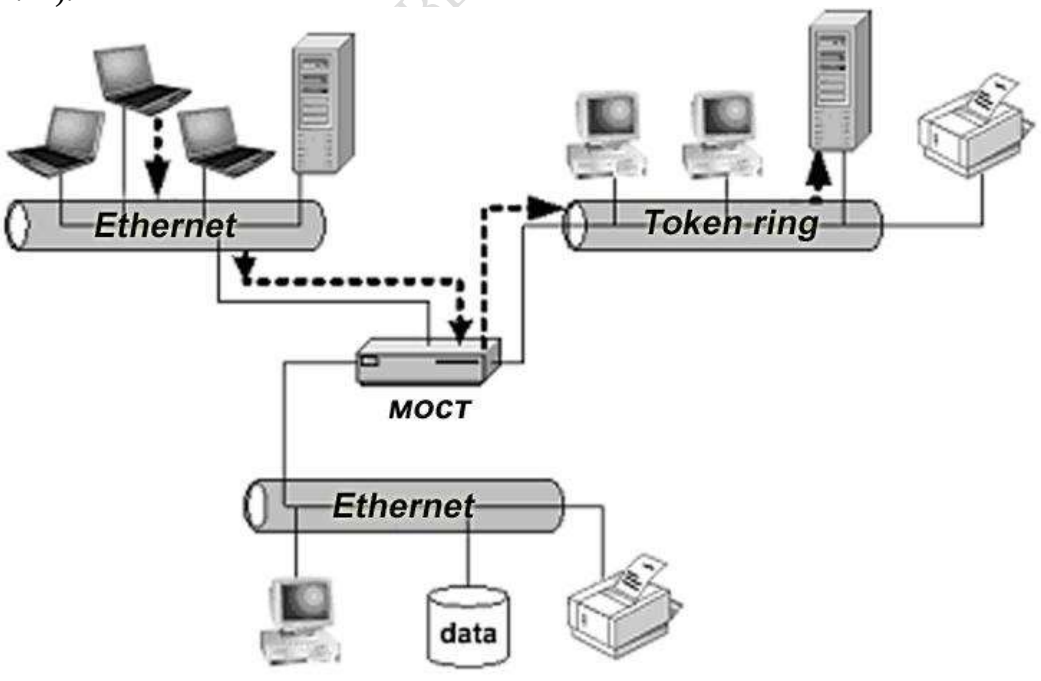


Рисунок 4.27 – Объединение сетей с помощью моста

Мосты могут работать в паре на удаленных друг от друга сетевых сегментах, изолируя внутреннюю сетевую среду от той среды, по которой мосты связываются между собой. Примером такой практики является технология ADSL.

Мосты функционируют в так называемом беспорядочном режиме (*promiscuous mode*), что подразумевает просмотр физического целевого адреса каждого кадра перед его пересылкой. Этим мосты отличаются от повторителей и концентраторов.

Чаще всего используются два типа мостов.

Прозрачные мосты – считывают исходный и целевой физические адреса кадра. Для этого они перехватывают весь сетевой трафик и анализируют целевой адрес каждого кадра, определяя, следует ли пересылать данный кадр в следующую сеть. Для этого мост просматривает MAC-адреса передаваемых через него кадров и строит *таблицу целевых адресов* CAM-table. Если CAM-table дает отклик о том, что MAC-адрес назначения кадра данных находится в удаленной сети, такой кадр обслуживается. В противном случае кадр считается локальным и ретрансляции не подлежит.

Мост транслирует кадр только в нужный сегмент сети через соответствующий порт. Если мосту не известен целевой сегмент, он передает кадр во все сегменты, за исключением исходного сегмента, и этот процесс называется *лавинной маршрутизацией* (*лавинной адресацией*) (*flooding*).

Главным достоинством мостов является то, что они сосредотачивают трафик в конкретных сетевых сегментах. Мост может выполнять фильтрацию и пересылку с довольно высокой скоростью, поскольку он просматривает информацию только на канальном уровне и игнорирует информацию на более высоких уровнях.

Транслирующие мосты могут дополнительно преобразовывать кадры данных, относящиеся к одному методу доступа и передающей среде, в кадры другого стандарта (например, Ethernet – Token Ring) и наоборот. Такой мост должен уметь изменять или добавлять: очередность битов в адресах; формат MAC-адреса; элементы маршрутной информации; функции, имеющиеся в кадрах Token Ring, не имеющие эквивалентов в Ethernet; зондирующие (*explorer*) кадры Token Ring, которых нет в сетях Ethernet. В современных сетевых средах часть функционала мостов данного типа реализуется *медиаконверторами*.

Важно знать что, если в сети присутствует более одного моста, может возникнуть ситуация, когда они не смогут правильно опознать, какой компьютер к какой из сетей относится, т. к. механизм регистрации узлов сети в таблице маршрутизации не лишен некоторых недостатков.

Функционал локализации L2-трафика по привязке MAC-адресата к порту сетевого устройства доказал свою эффективность. Появившееся устройство-гибрид HUB-BRIDGE быстро выделилось в отдельный тип, который получил название *коммутатора*.

Ключевой проблемой проектирования и эксплуатации LAN является распределение пропускной способности кабеля между всеми станциями, подключенными к сети. Например, в сети 10BASE-T при подключении 100 рабочих станций каждая из них получает возможность передавать данные в среднем со скоростью:

$$\frac{10 Мбит/с}{100} = 0{,}1 Мбит/с.$$

Иначе говоря, пропускная способность канала для одной станции в такой сети составляет 100 Кбит/с. С развитием мультимедийных приложений, позволяющих передавать звук, видео и статические изображения высокого качества, значительно возросли требования к параметрам локальных сетей.

Коммутаторы позволяют уплотнить передачу в границах своих внутренних ресурсов, позволяя оперировать независимыми каналами связи с 100% скоростью работы сетевых интерфейсов (рисунок 4.28).

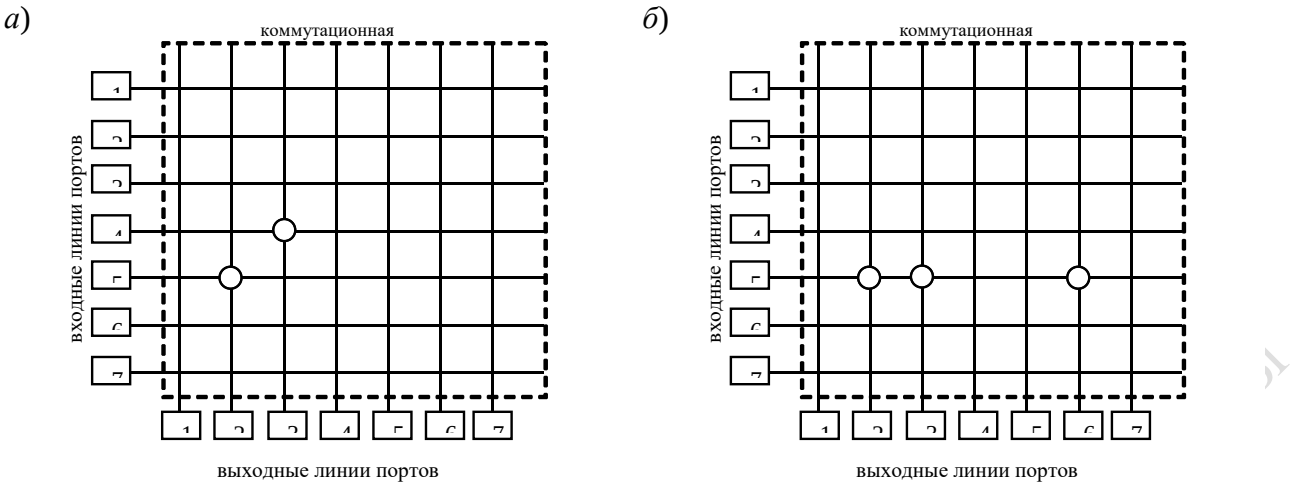


Рисунок 4.28 – Логическая структура коммутатора:
а) одновременная передача по двум каналам;
б) широковещательная рассылка

Обратите внимание, что подключение двух файловых серверов (Data) к отдельным портам коммутатора позволяет одновременно устанавливать два канала связи между рабочими станциями и файловыми серверами, что увеличивает максимальную скорость доступа к данным в сети вдвое.

Другими словами, в коммутаторе выполняется функция трансляции сигнала конкретному порту назначения (виртуальный канал или коммутируемая линия), а при наличии более одной коммутируемой линии – организации несколько одновременных сеансов обмена.

Ключевым звеном коммутатора является архитектура защиты магистрали от блокирования (*non-blocking*), которая позволяет установить множественные связи между разными парами портов одновременно, причем кадры не теряются в процессе коммутации. При этом параллельный трафик между взаимодействующими сетевыми устройствами остается локализованным. Локализация осуществляется с помощью адресных таблиц, устанавливающих связь каждого порта с адресами сетевых устройств, относящихся к сегменту этого порта. Таблица заполняется в процессе анализа коммутатором адресов станций отправителей в передаваемых ими кадрах.

Кадр передается через коммутатор локально в соответствующий порт только тогда, когда адрес станции назначения, указанный в поле кадра, уже содержится в адресной таблице этого порта. В случае отсутствия в таблице CAM-table адреса станции назначения, кадр рассылается во все остальные сегменты. Если коммутатор обнаруживает, что MAC-адрес станции назначения приходящего кадра находится в таблице MAC-адресов, приписанной за портом, то этот кадр сбрасывается – его получит станция назначения, находящаяся в исходном сегменте.

Если приходящий кадр является широковещательным (*broadcast*), то такой кадр будет размножен коммутатором (подобно концентратору), т. е. направлен во все остальные порты.

Внешний вид коммутаторов представлен на рисунке 4.29.

Рисунок 4.29 – Примеры коммутаторов

Максимальное количество коммутируемых линий в коммутаторе можно рассчитать по формуле: ***m = div (n/2)***, где ***m*** – число коммутируемых линий, а ***n*** – число портов коммутатора.

Коммутаторы используют один из двух способов пересылки для коммутации данных между сетевыми портами (рисунок 4.30):

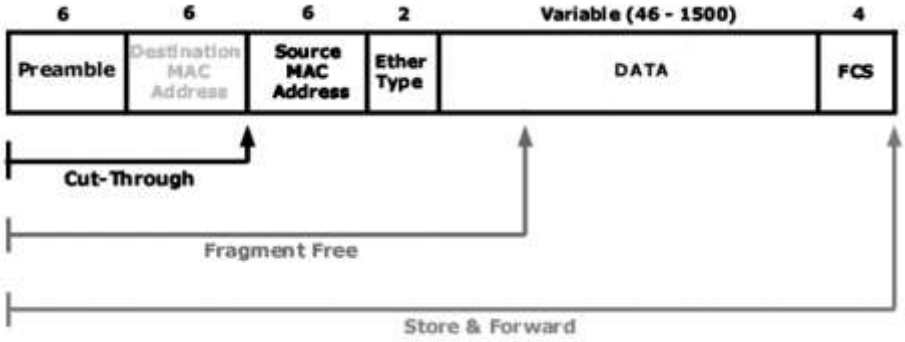


Рисунок 4.30 – Принцип обработки кадров в различных режимах

- *коммутация с промежуточным хранением (Store&Forward)* - в этом методе пересылки кадров коммутатор получает кадр целиком и вычисляет циклический избыточный кода (CRC). Если значение CRC допустимо, коммутатор ищет адрес назначения, который определяет выходной интерфейс. Затем кадр перенаправляется к правильному порту.

- *коммутация со сквозной пересылкой (Cut-Through)* - в этом режиме коммутатор пересылает данный кадр до его полного получения. Самый быстрый режим пересылки. Не защищен от ошибок трансляции и коллизий.

- к*оммутация с исключением фрагментов (Fragment Free)* - представляет собой компромисс между большой задержкой с высокой целостностью (коммутация с промежуточным хранением) и малой задержкой с меньшей целостностью (коммутация с быстрой пересылкой), коммутатор сохраняет и выполняет проверку ошибок на первых 64 байтах кадра перед пересылкой. Поскольку большинство сетевых ошибок и конфликтов происходят в течение первых 64 байт, это гарантирует, что столкновение не произошло перед переадресацией кадра.

Большим преимуществом *коммутации с промежуточным хранением* является то, что режим определяет, есть ли у кадра ошибки перед распространением кадра. Если же в кадре обнаружена ошибка, коммутатор отклонит его. Отклонение кадров с ошибками позволяет уменьшить ширину полосы пропускания, потребляемую поврежденными данными.

Коммутация с промежуточным хранением необходима для обеспечения сервиса *качества обслуживания сервисов (QoS)* в конвергентных (мультисервисных) сетях, в которых требуется классификация кадра для назначения приоритетов проходящего трафика. Например, при передаче речи по IP потоки данных должны иметь больший приоритет, чем трафик, используемый для просмотра веб-страниц.

5 Маршрутизируемые сетевые среды

5.1 Сетевой уровень ISO/OSI (L3)

Сетевой уровень управляет прохождением пакетов по сети. Все сети содержат физические маршруты передачи информации (кабельные тракты).

Сетевой уровень выполняет четыре основные операции: *L3-адресация оконечных устройств; инкапсуляция; маршрутизация; деинкапсуляция.*

Сетевой уровень анализирует адресную информацию протокола передачи пакетов и посылает их по более подходящему маршруту – физическому или логическому, обеспечивая максимальную эффективность сети. Также этот уровень обеспечивает пересылку пакетов между сетями через маршрутизаторы.

Контролируя прохождение пакетов, сетевой уровень выступает в роли «управляющего трафиком»: он направляет пакеты по наиболее эффективному из нескольких возможных

трактов передачи данных. Для определения наилучшего маршрута сетевой уровень постоянно собирает информацию о расположении различных сетей и узлов, этот процесс называется обнаружением маршрута (discovery).

Сетевой уровень может отправлять данные по параллельным маршрутам, либо выбирать единственный маршрут на весь сеанс связи, создавая виртуальные каналы (virtual circuit). Виртуальные каналы представляют собой логические коммуникационные линии для передачи и приема данных. Виртуальные каналы, представленные только на сетевом уровне, образуются между сетевыми узлами, обменивающимися информацией. Поскольку сетевой уровень управляет данными, поступающими по нескольким виртуальным каналам, то эти данные могут поступать в неправильной очередности. Для устранения этих издержек сетевой уровень проверяет и при необходимости корректирует порядок передачи пакетов перед отправкой их следующему уровню стека. Также на сетевом уровне пакеты получают сетевые адреса и выполняется форматирование пакетов в соответствии с сетевым протоколом принимающей стороны. Кроме того, обеспечивается передача пакетов с такой скоростью, чтобы принимающий уровень успевал обрабатывать их.

Методы переадресации пакетов между сетями (рисунок 5.1):

- *процессорная коммутация* - устаревший механизм пересылки пакетов. Центральный процессор устройства маршрутизирует каждый пакет;

- *быстрая коммутация* - механизм пересылки пакетов, использующий кэш-память быстрого переключения для хранения данных следующего перехода. Маршрутизация производится центральным процессорам однократно на одну цепочку пакетов;

- *проприетарные решения.* Напимер, Cisco Express Forwarding (CEF) на базе предварительно собранной и долговременно хранимой базе адресов доставки FIB.

Основной материал раздела 5 данного пособия излагается в реалиях сетевого уровня ISO/OSI (уровня межсетевой связи DoD) стека протоколов TCP/IP (рисунок 5.2).

Доставка IP-пакетов может осуществляться одним из следующих способов:

- *одноадресная передача (Unicast)* - подключение «один к одному».

- *многоадресная передача (Multicast)* - от одного узла множеству узлов, но речь идет об ограниченной группе;

- *ближайшему узлу (Anycast)* – всем доступным узлам сервиса в IPv6;

- *широковещательная передача (Broadcast)* - от одного узла всем узлам

Протокол IP инкапсулирует сегмент транспортного уровня в пакет версии протокола L3, используемого для связи (рисунок 5.3).

Сетевой уровень устанавливает размер максимального блока передачи данных (MTU).

Протокол IP не устанавливает соединение с пунктом назначения до отправки пакета. Управляющая информация (синхронизация, подтверждения и т.д.) не требуется. Пункт назначения получит пакет, когда он прибудет, но предварительные уведомления по IP не отправляются. Если существует потребность в трафике, ориентированном на соединение, то другой протокол будет обрабатывать это (обычно TCP на транспортном уровне).

IP-пакет не имеет отношения к типу кадра, необходимому на канальном уровне, или к типу носителя на физическом уровне.

IP-пакет может передаваться по любому типу носителя: медь, оптоволокно или беспроводные каналы.

Современными протоколами связи уровня L3 являются IP версии 4 (IPv4) и IP версии 6 (IPv6).

а)

б)

в)

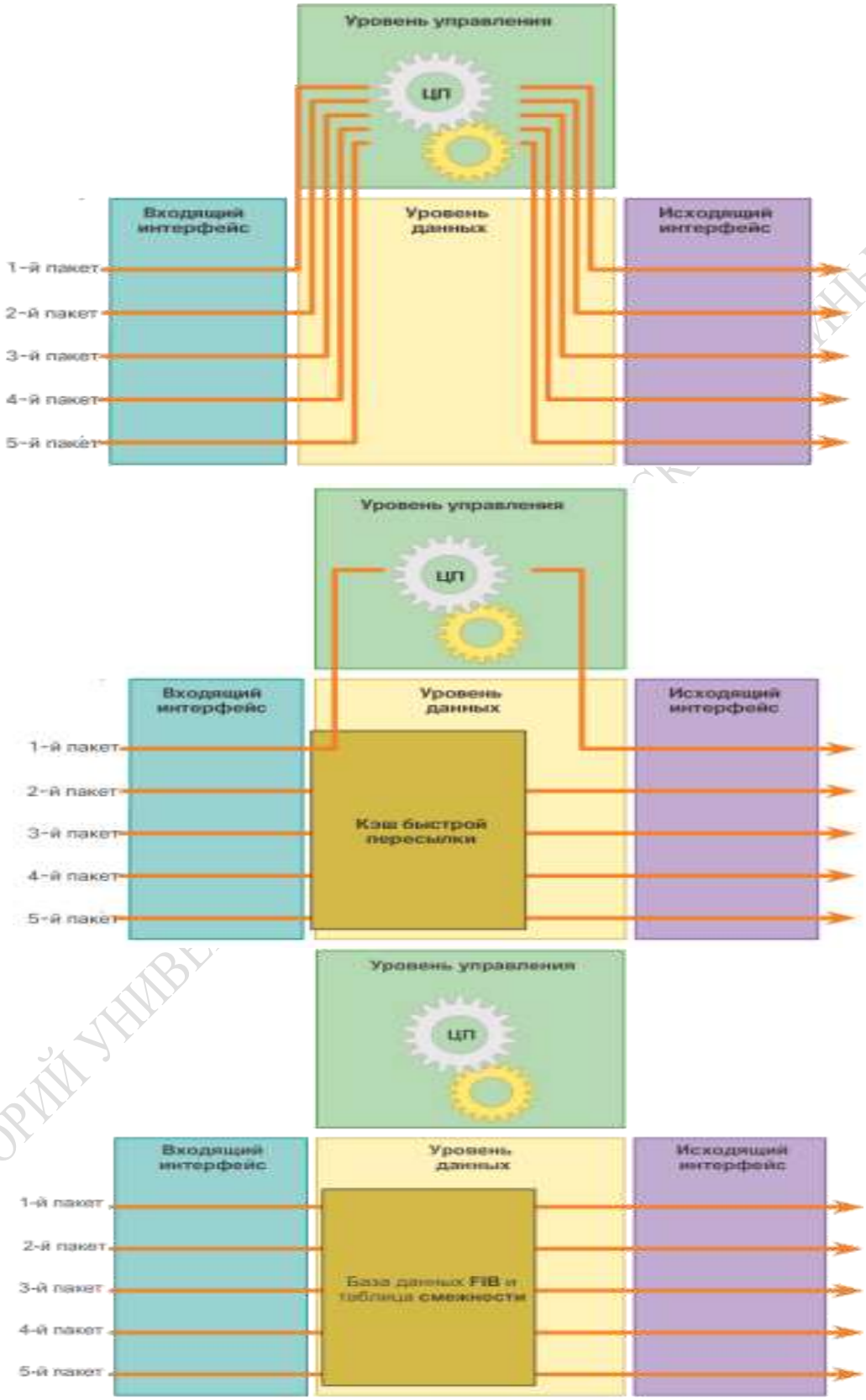


Рисунок 5.1 – Переадресация пакетов между сетями:
а) процессорная коммутация; *б)* быстрая коммутация; *в)* Cisco Express Forwarding

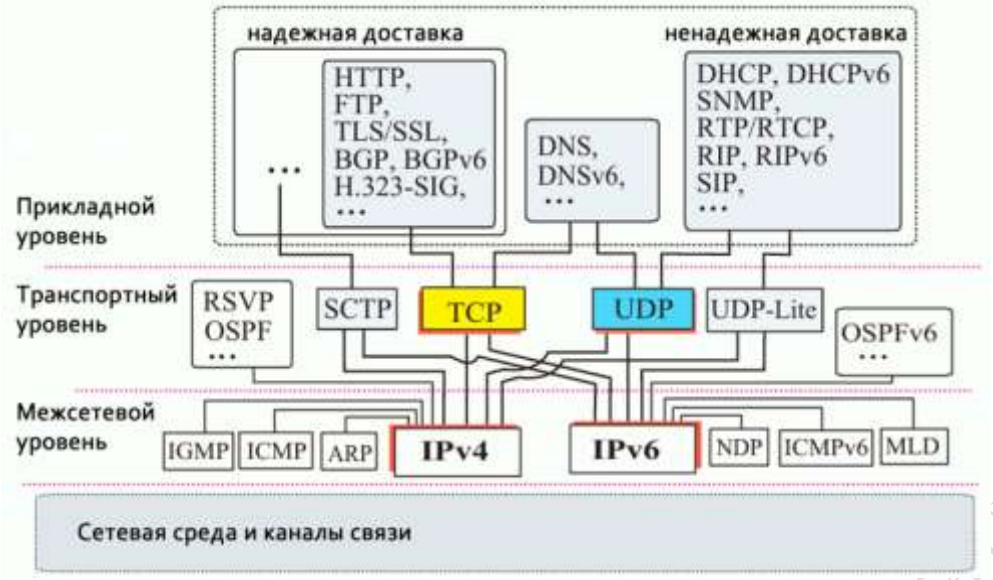


Рисунок 5.2 – Протоколы и сервисы TCP/IP

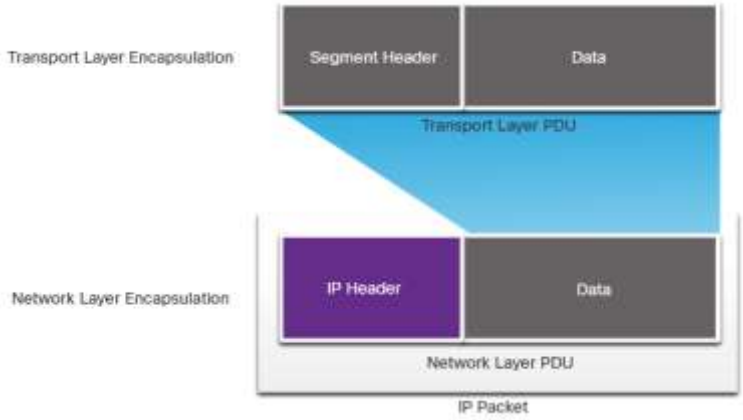


Рисунок 5.3 – Инкапсуляция сегмента в пакет сетевого уровня

5.2 Адресуемость операционных систем узлов сети

Как уже описалось в п.1.1 пособия объем потребляемого сетевого трафика растет и нагрузка на каналы связи (L1+L2) требует повышения полосы пропускания. В рамках функций уровня L3 для решения этой задачи реализуется разделение трафика клиентской операционной системы и доставка его до пункта назначения различными маршрутами.

Важно знать, что у современных операционных систем клиентских версий и операционных систем узлов ретрансляции существует ограничение по использованию нескольких сетевых интерфейсов одновременно.

Получение IP-адреса для работы с глобальным сетевым трафиком в общем случае предполагает следующую иерархию:

- IANA - администрация адресного пространства Интернета. Задачи: распределение номеров AS и IP-адресов в глобальном масштабе, назначаение RIR. Подчиняется напрямую ICANN.
- RIR - региональный интернет-регистратор. Задачи: выделение крупных блоков адресов, регистрация LIR и распределение AS.
- LIR – локальный интернет-регистратор. Задачи: поддержка работы сетей, распределение PI и номеров AS. Как правило, совмещает свои функции с задачами провайдера интернет (ISP). Минимальный блок адресного пространства для LIR - 4096 IP-адресов.

- AS - автономная система. Содержит в себе адресное пространство (IP-адреса), имеет уникальный ASN - номер, позволяющий однозначно идентифицировать AS в Интернете. Номер AS - ключевая часть маршрутизации протокола BGP, обслуживающего трафик между ISP.

- PI - Provider Independent. Провайдеро-независимые IP адреса. Находятся в определенной AS, маршрут к ним зависит только от политики маршрутизации. Принадлежат конечному пользователю [компании или LIR], а не его вышестоящему провайдеру. Следственно, сохраняются при смене ISP/подключении дополнительного ISP.

Путь распределения пространства:

ICANN-IANA -> RIR -> LIR (-> end-user) [-> PI-owner -> end-user].

Разграничение регионов между RIR представлено на рисунке 5.4.

Рисунок 5.4 – Карта RIR

Визуализация по методике Гильберта хорошо показывает, как распределено адресное IPv4 пространство (рисунок 5.5).

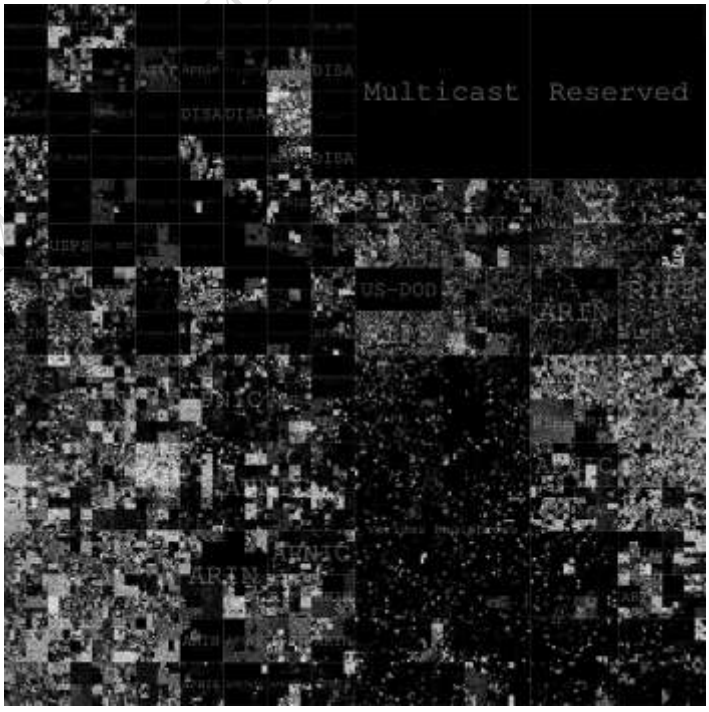


Рисунок 5.5 – Плотность «занятости» адресов интернета в 2018 году

5.3 IP-адресация

Механизм адресации предполагает деление адреса на 2 части: номер сети и номер узла (рисунок 5.6).

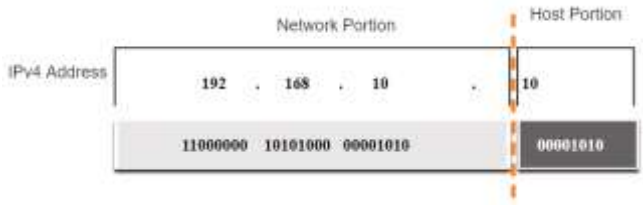


Рисунок 5.6 – Сетевая и узловая части адреса IP

В IP v.4 адресная информация занимает 4 байта и при применении классовой системы адресов разделяется по границе байта.

Спецификации IP v.4 адреса разделяют на 5 классов (рисунок 5.7).

	1 байт		**2 байт**	**3 байт**	**4 байт**
A	0	№ сети	№ узла		
B	10	№ сети		№ узла	
C	110	№ сети			№ узла
D	1110	Адрес группы Multicast			
E	11110	Зарезервирован			

Рисунок 5.7 – Классы адресов IP v.4

Классу **A** соответствует диапазон адресов 1.0.0.0 – 127.255.255.255.
Классу **B** соответствует диапазон адресов 128.0.0.0 – 191.255.255.255.
Классу **C** соответствует диапазон адресов 192.0.0.0 – 223.255.255.255.
Классу **D** соответствует диапазон адресов 224.0.0.0 – 239.255.255.255.
Классу **E** соответствует диапазон адресов 240.0.0.0 – 247.255.255.255.

Класс **A** используется для самых крупных сетей, насчитывающих до 16 677 216 узлов. Таких сетей не может быть больше 126.

В классе **B** максимально – 65 536 узлов, количество сетей – 2 142.

Класс **C** оперирует количеством адресов, не превышающим 254 узла. Это наиболее распространенный и эффективный класс адресов.

Требования к распределению адресного пространства излагаются в стандартах RIPE-185, RIPE-127, RFC 1918, RFC 1112. Исключительным случаем применения этих механизмов является использование бесклассовой адресации.

Бесклассовая адресация (Classless InterDomain Routing – CIDR) – метод IP-адресации, позволяющий гибко управлять пространством IP-адресов, не используя жёсткие рамки классовой адресации.[6] Способ основывается на переменной длине маски подсети (Variable Lenght Subnet Mask – VLSM) в то время, как в классовой адресации длина маски строго фиксирована 0, 1, 2 или 3 установленными байтами.

Вот пример записи IPv4-адреса с применением бесклассовой адресации: 10.1.2.33/27 (рисунок 5.8). Длина маски подсети 27 бит.

октеты IP-адреса	10								1								2								33							
биты IP-адреса	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0	1
биты маски подсети	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0
октеты маски подсети	255								255								255								224							

Рисунок 5.8 – Организация отдельной подсети для 32 узлов

Особые IP-адреса. Для технических нужд система адресации IP v.4 использует адреса, которые по синтаксису одинаковые для всех типов сети:

− если весь IP-адрес состоит из двоичных нулей – это адрес того узла, который сгенерировал этот пакет;

− если нулевым является только номер сети по умолчанию, то считается, что узел назначения принадлежит той же сети, что и узел, отправивший пакет;

− если адрес состоит из одних единиц, то это ограниченное широковещательное сообщение BroadCast. Пакет доставляется всем узлам, принадлежащим к той же сети;

− если поле номера узла состоит из одних единиц, пакет доставляется всем узлам, находящимся в сети с заданным номером.

Помимо этих адресов существует набор специализированных (отладочных) адресов. Например: 127.0.0.0, 127.0.0.1 и др. Такие адреса принято называть Loopback. Данные не передаются по сети, а воспринимаются узлом-отправителем как только что принятые.

Частные (private) IP-адреса. В соответствии со стандартом RFC 1918 несколько диапазонов адресов класса A, B и C были зарезервированы. В диапазон локальных адресов входит одна сеть класса A (10.0.0.0/8), 16 сетей класса B (172.16.0.0/16 – 172.31.0.0/16) и 256 сетей класса C (192.168.0.0/24 – 192.168.255.0/24). IP-адреса из этих диапазонов не обслуживаются ISP, то есть такой трафик может быть только локальным. Таким образом, сетевые администраторы получили определенную степень свободы в плане предоставления внутренних адресов для локальных адресных пространств.

Система адресации IP v.4 – прозрачная, но малоэффективная и практически исчерпала свои возможности. Для продолжения ее использования системному администратору необходим определенный базовый набор знаний и серьезный опыт работы. Но поскольку число IP-сетей быстро растет, подготовка квалифицированного персонала отстает, что создает проблемы с управляемостью. Есть и другие недостатки адресации IP v.4. В частности, динамический уровень агрегирования адреса не позволяет снизить временные затраты на маршрутизацию пакетов на уровне оборудования.

Под агрегированием адреса понимается процедура выбора сети назначения пакета на основе анализа не всего адреса целиком, а лишь его фиксированной части (рисунок 5.9).

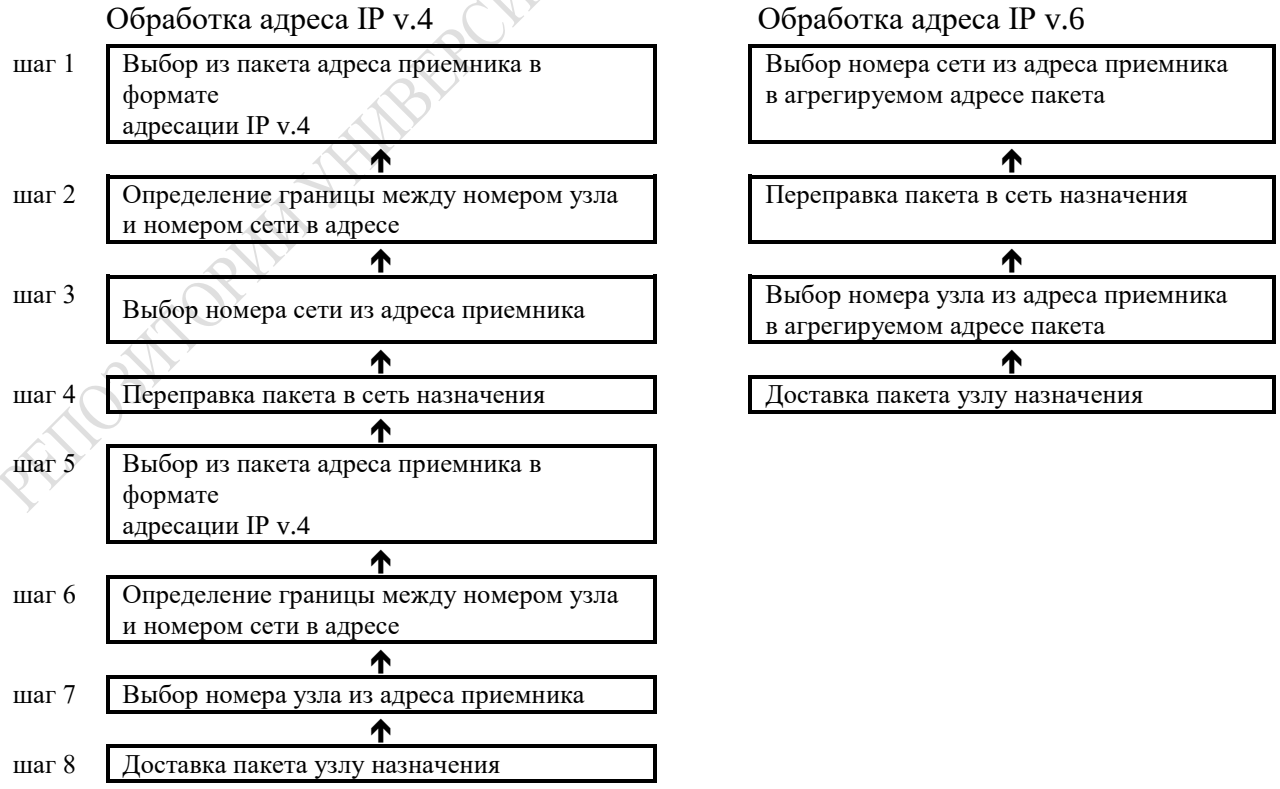


Рисунок 5.9 – Маршрутизация IP v.4 и с агрегированного адреса

Прогнозы аналитиков выявили угрозу дефицита IP-адресов формата IP v.4. Поэтому в середине 90-х годов начался процесс разработки новой версии IP-адресации – IP v.6 (RFC 1883).

Свойства адресации IP v.6:

- связь одного адреса с несколькими интерфейсами;
- автоматическое назначение адреса и CIDR-адресация.

Размер поля адреса в 128 разрядов описывает пространство для 340 289 366 920 938 463 463 374 607 431 762 211 456 узлов сети.

В IP v.6 определяется уникальный агрегируемый IP-адрес конечного интерфейса (рисунок 5.10).

3	13	8	24	16	64
FP	TLA		NLA	SLA	Interfase ID

Рисунок 5.10 – Структура агрегированного уникального адреса IP v.6

Поле префикса формата FP назначено для определения типа адреса и для глобального агрегированного уникального адреса имеет значение 001.

TLA-префикс верхнего уровня предназначен для агрегирования верхнего уровня, который используют при назначении сети провайдеры самого верхнего уровня (.by, .com, .ru).

Поле 8 бит – предназначено в дальнейшем для расширения TLA, если 8196 сетей будет исчерпано.

NLA-префикс следующего уровня предназначен для размещения номеров сетей средних и мелких провайдеров. Значительный размер поля (24 бита) позволяет построить сложную структуру номеров сетей, т. е. использует технологию SIDR в пределах данного поля.

SLA-префикс местного уровня, предназначен для адресации подсетей отдельного компонента, например, подсетей корпоративной сети. Размер в 16 бит позволяет агрегировать адресное подпространство этого поля в своих пределах.

Идентификатор интерфейса Interface ID (64 бита) позволяет использовать в качестве адреса узла:

- MAC-адрес сетевого адаптера (48 бит);
- адрес X.25 (60 бит);
- адрес конечного узла ATM (48 бит);
- IP-адрес в системе IP v.4.

Примеры записи IPv6-адреса представлены на рисунке 5.11.

```
C:\> ipconfig
Настройка протокола IP для Windows
Подключение Ethernet-адаптера по локальной сети:
Connection-specific DNS Suffix . :
IPv6 Address. . . . . . . . . . . : 2001:db8:acad:1:fc 99:47ff:fe75:cee0
Link-local IPv6-адрес. . . . . : fe80::fc99:47ff:fe75:cee0
Шлюз по умолчанию . . . . . . . . . : fe80::1
C:\ >
```

Рисунок 5.11 – Синтаксис адресации IPv6

На момент издания пособия внедрение системы адресации IP v.6 поддержано на уровне операционных систем и является стандартом для международных организаций. 6 июня

2012 года состоялся Всемирный запуск IPv6, но в практике управления сетевыми структурами LAN по-прежнему лидирующее место занимает адресация IP v.4.

IPv6 как и IPv4 считается ресурсоемкой системой обеспечения адресного пространства. Экспоненциальный рост числа устройств IoT с минимальным набором ресурсов памяти и вычислительной мощности создает ситуацию, когда функции адресации и маршрутизации контента будут отвлекать преобладающую часть ресурсов сетевой инфраструктуры.

Система адресации NewIP предлагает гибридную модель адресации с переменной длиной адресного поля, удобной для операционных систем устройств IoT (рисунок 5.12).

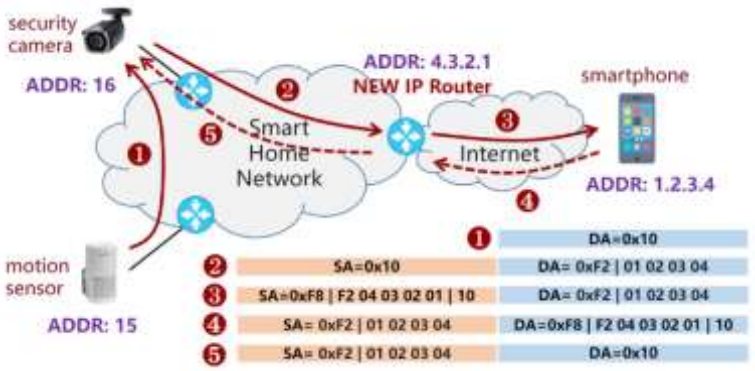


Рисунок 5.12 – Система адресации NewIP Huawei

При подобном подходе на каждом этапе продвижения данных информация об источнике трафика остается доступной для анализа и выбора оптимального пути, но каждая из операционных систем может ограничиться той частью адресного поля, которая является значимой для выполнения ее функций.

5.4 Сетевые устройства уровня L3

Устройства уровня L3 осуществляют высокоуровневую обработку трафика и реализацию сетевых сервисов. По сути они являются не специализированными устройствами, а унифицированными вычислительными системами. Это подтверждается миграцией современных операционных систем устройств L3 к общераспространенным версиям ядра Linux. Ресурсы такой вычислительной системы могут быть расширены. Например, на рисунке 5.13 показано шасси маршрутизатора с расширяемыми банками оперативной памяти.

К специфичным устройствам L3 можно отнести следующие:

- модемы и ONT-устройства;
- сетевые маршрутизаторы (*ROUTER*);
- шлюзы, межсетевые экраны *(GATEWAY, BRANDMAUER/FIREWALL)*;
- устройства NAT.

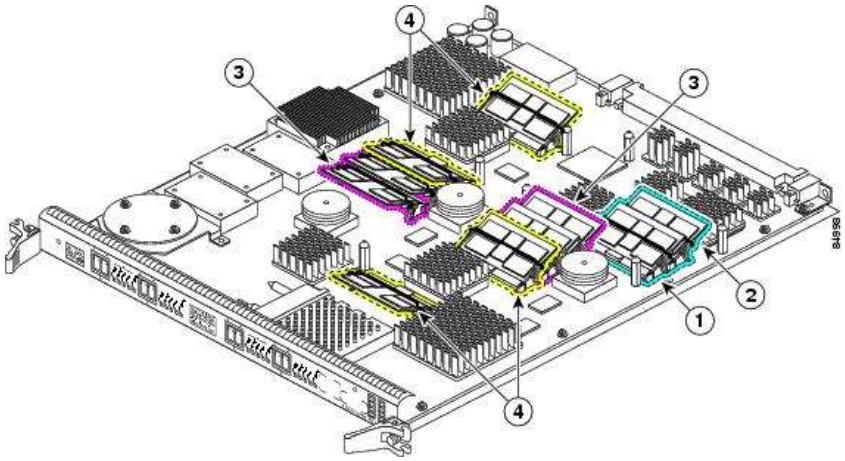


Рисунок 5.13 – Расширение оперативной памяти в blade-системе

Модемы ADSL, DialUp и ONT-устройства уже упоминались в п.3.6. Являясь устройствами гибридного типа, они выполняют задачи L3 для передачи данных из LAN пользователя в ISP и обратно.

Маршрутизатор – это устройство, предназначенное для определения и назначения наиболее оптимального маршрута продвижения пакетов при их перемещении по сети с несколькими вариантами маршрутов доставки.

Маршрутизатор выполняет некоторые функции моста, такие как анализ топологии, фильтрация и пересылка пакетов. Однако, в отличие от мостов, маршрутизаторы могут направлять пакеты в конкретные сети, а не только в присоединенные, анализировать сетевой трафик и быстро адаптироваться к изменениям сети.

Маршрутизаторы подразделяются на два основных типа:

− *статические* (*static*) – здесь необходимо, чтобы администратор вручную создал и сконфигурировал таблицу маршрутизации, а также указал каждый маршрут для передачи данных через сеть;

− *динамические (dynamic)* – автоматически определяют маршруты и поэтому требуют минимальной настройки. Они сложнее статических, так как анализируют информацию от других маршрутизаторов и для каждого пакета принимают отдельное решение о маршруте передачи данных в сети.

Процедура создания маршрута состоит в оценке и сравнении между собой нескольких вариантов путей прохождения информации через сеть, вычисленных согласно «метрикам» маршрутизации, значения которых хранятся в таблицах маршрутизации. Таблицы маршрутизации этих устройств намного сложнее, чем таблицы маршрутизации мостов.

Метрика маршрутизации – это свойство каналов связи, согласно которому в числовом эквиваленте определяется оптимальность данного маршрута в текущий момент времени. К примерам таких метрик можно отнести: цену аренды канала связи за единицу времени, скорость пропускания канала связи, длину сегмента, число заявок в единицу времени, длину очереди на обслуживание в текущий момент времени и пр. Часть характеристик может быть статическими, но некоторые могут измениться и потребуют обновления. Обновление осуществляется широковещательными пакетами, что отрицательно сказывается на сетевом трафике.

Положительный момент в применении маршрутизаторов – локализация трафиков, т. е. в соседней части сети будут транслироваться только те пакеты, которые не могут быть обслужены в пределах данного сегмента сети.

Отрицательным моментом является возможность организации «адресной петли». Например, в сети есть 6 узлов маршрутизации (рисунок 5.14). Необходимо доставить пакет от первого к шестому.

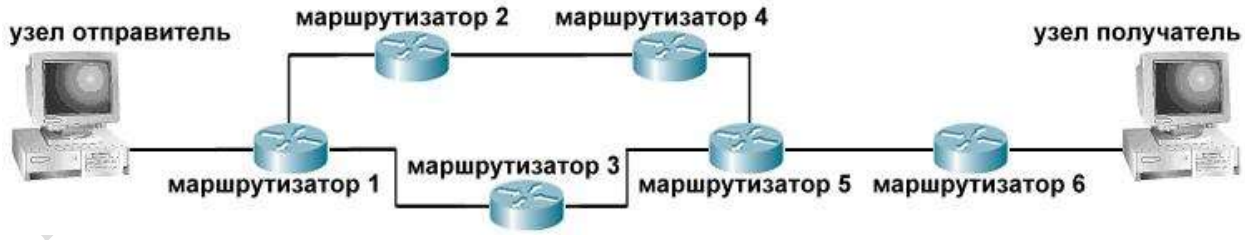


Рисунок 5.14 – Пример маршрутизации пакетов в сложных сетях

В этой сети от маршрутизатора 1 к маршрутизатору 6 есть два маршрута продвижения данных: «1–3–5–6» и «1–2–4–5–6».

При оценке маршрутизатором 1 может быть выбран оптимальным маршрутом первый путь – «1–3–5–6». Пакет пересылается маршрутизатору 3, а на самом маршрутизаторе 3 после анализа может сложиться ситуация, когда оптимальным маршрутом доставки пакета

маршрутизатору 6 будет выбран маршрут «3–1–2–4–5–6». Таким образом, пакет возвращается на исходный маршрутизатор и может блуждать по кольцу, пока не истечет срок его жизни.

IP-пакет обрабатывается всеми устройствами L3 по мере прохождения сети. Значение полей адресации IP-пакета не должно изменяться на всем пути от источника к адресату. Если на границе сети находится устройство NAT возможно преобразование адресов источника и пункта назначения в структуре пакета.

Сетевой *шлюз* обеспечивает связь между сетевыми сегментами, то есть является посредником при передаче данных. Функция маршрутизации – определить наиболее эффективного посредника при организации доставки пакета в сеть назначения и отправить пакет на адрес этого шлюза. Маршрутизатор для LAN предприятия является «шлюзом по умолчанию». В операционной системе любого сетевого устройства с любым числом интерфейсов «шлюз по умолчанию» может иметь единственное значение.

Межсетевые экраны используют технологию потоковой фильтрации. Эти устройства анализируют каждый IP-пакет по отдельности, не дожидаясь загрузки всей проверяемой цепочки пакетов. Поскольку службы L4 для создания сеанса связи согласовывают параметры пакетами L3, межсетевые экраны блокируют передачу данных до отправки данных.

Наряду с минимальными требованиями к размеру используемой памяти, этот процесс не требует дополнительных затрат на восстановление потока данных и не сказывается на пропускной способности и задержках, вносимых экраном, при любых размерах проверяемых файлов.

Операционная система маршрутизатора может выполнять функции межсетевого экрана с помощью *ACL-списков*, привязанных к входящим/исходящим потокам на интерфейсах.

Устройства NAT обеспечивают преобразование *частных адресов (private)* в *публичные адреса (public)*. Для того чтобы разрешить устройству с частным IPv4-адресом получать доступ к устройствам и ресурсам вне LAN через среду ISP, частный адрес сначала необходимо преобразовать в публичный адрес. Устройство NAT обычно работает на границе тупиковой LAN (рисунок 5.15).

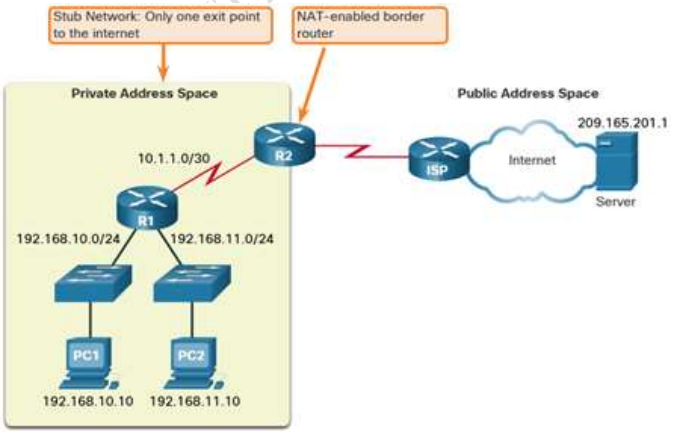
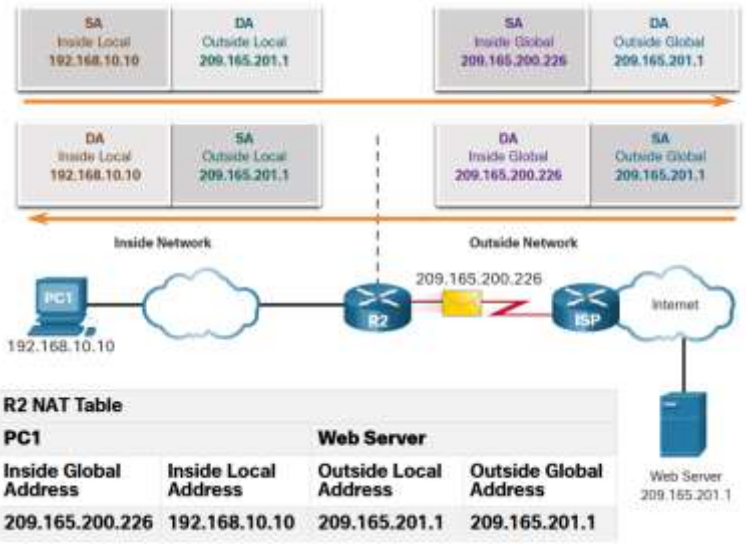


Рисунок 5.15 – Пример применения устройства NAT

В NAT предусмотрено 4 типа адресов:

- внутренний локальный адрес;
- внутренний глобальный адрес;
- внешний локальный адрес;
- внешний глобальный адрес.

Таблица NAT-преобразования строится на пограничном устройстве и обеспечивает трансляцию адресов при передаче информации в прямом и результатов ее обработки в обратном направлении (рисунок 5.16).



R2 NAT Table

PC1		Web Server	
Inside Global Address	**Inside Local Address**	**Outside Local Address**	**Outside Global Address**
209.165.200.226	192.168.10.10	209.165.201.1	209.165.201.1

Рисунок 5.16 – Пример процесса NAT-трансляции

Терминология NAT всегда применяется с точки зрения устройства с переведенным адресом:

- внутренний адрес - это адрес устройства, преобразуемый механизмом NAT;
- внешний адрес - это адрес устройства назначения;
- локальный адрес - это любой адрес, появляющийся во внутренней части сети;
- глобальный адрес - это любой адрес, появляющийся во внешней части сети.

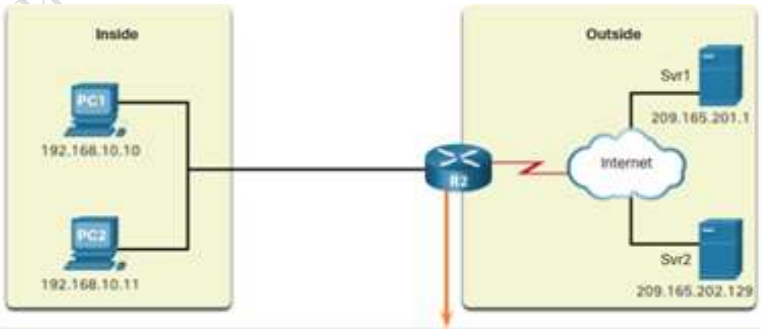
Обычно используется одна из следующих моделей NAT:

- *статический NAT* использует однозначное сопоставление локальных и глобальных адресов, настроенных сетевым администратором, которые остаются постоянными;

- *динамический NAT*. Когда внутреннее устройство запрашивает доступ к внешней сети, динамическое преобразование NAT назначает доступный публичный IPv4-адрес из пула. На каждый сеанс связи устройство из внутренней сети может получить произвольный адрес и пула.

- *преобразование адресов портов (PAT).* Преобразование адреса и номера порта (PAT), также называемое NAT с перегрузкой, сопоставляет множество частных IPv4-адресов одному или нескольким публичным IPv4-адресам (рисунок 5.17).

Еще одним способом передать данные между удаленными LAN является использование туннелирования.



NAT Table with Overload

Inside Local IP Address	Inside Global IP Address	Outside Local IP Address	Outside Global IP Address
192.168.10.10:1555	209.165.200.226:1555	209.165.201.1:80	209.165.201.1:80
192.168.10.11:1331	209.165.200.226:1331	209.165.202.129:80	209.165.202.129:80

Рисунок 5.17 – Пример процесса PAT-трансляции

5.5 Подходы к туннелированию трафика IPv6 в среде IPv4

Для успешной реализации миграции виртуальных хостов требуется стабильная сетевая инфраструктура. В контексте процедур перехода системы адресации сетевого уровня на IPv6 следует рассмотреть решение.

Если результаты эксперимента по интеграции Dual Stack не увенчаются успехом и/или трафик провайдера полностью перейдет в режим передачи данных IPv6 (что будет вероятной практикой для вновь создаваемых сетевых подключений), системный администратор сети сможет использовать туннельные решения для подключения сетевые среды IPv6 в сети IPv4. Пример таких временных зон поддержки протокола показан на рисунке 5.18. В используемом примере используется разрыв в поле непрерывной адресации IPv6 (разрыв IP).

Version IP	Segment 1	Segment 2	Segment 3	Segment 4			Segment 5	Segment 6
IPv4	+	+	+	+	+	+	–	–
IPv6	+	+	+	+	–	+	+	+

Рисунок 5.18 - Пример карты сети с разными уровнями поддержки IPv4/IPv6

Для решения задач гибридного туннелирования необходимо иметь эффективную связь между сегментами сети средствами второго IP-протокола. В сегменте Segment 3 достаточно объявить туннель IPv6 over IPv4. Канал IPv4 используется для доставки трафика IPv6. По условиям примера после прохождения туннеля все клиенты IPv6 смогут реализовать полноценную двустороннюю связь.

Следует подчеркнуть, что при инкапсуляции туннелируемого трафика пакет носителя IPv4 добавляет свои адресные данные поверх передаваемого пакета IPv6. Так как размер результирующего сетевого пакета (после инкапсуляции) не должен превышать лимит в 1500 байт. Для этого необходимо на стороне отправителя уменьшить поле блока данных на размер вложенных служебных данных, который в проиллюстрированном примере составляет 24 байта.

На рисунке 5.19 показаны разделы, доступные для запуска версий OSPF до настройки туннелирования.

	Segment 1	Segment 2	Segment 3	Segment 4			Segment 5	Segment 6
OSPFv2	+	+	+	+	+	+	–	–
OSPFv3	+	+	+	+	–	+	+	+

Рисунок 5.19 - Несоответствия в версиях протокола OSPF

Как видно из рисунка, OSPFv2 работает только в адресной зоне IPv4, а OSPFv3 - в адресной зоне IPv6. После строительства тоннелей картина немного меняется (рисунок 5.20).

	Segment 1	Segment 2	Segment 3	Segment 4			Segment 5	Segment 6
OSPFv2	+	+	+	+	+	+	–	–
OSPFv3	+	+	+	+			+	+

Рисунок 5.20 - Расширение зоны покрытия протокола OSPFv3

В этом режиме реализации DualStack работает не во всей сети, а только на стороне генерации и обслуживания трафика.

Поскольку протоколы динамической маршрутизации требуют сбора служебных данных о топологии сети для поиска оптимального маршрута пересылки IP-пакетов, параллельная работа двух версий OSPF может увеличить нагрузку на каналы связи. Каждая версия протокола OSPF отправляет сообщения канального уровня с описанием маршрутизаторов и сетей, которые вместе формируют базу данных состояния каналов (LSDB) на каждом маршрутизаторе.

Следует отметить, что данные для построения LSDB собираются на канальном уровне, а основная работа версий протокола — на сетевом уровне. Следовательно, есть возможность оптимизировать служебный трафик.

Рассмотренный пример использовался в качестве квалификационной задачи ко второму отборочному туру конкурса «Технологии передачи данных в локальных и глобальных сетях» XI Международной олимпиады «IT-Планета» 17 марта 2018 г. (рисунок 5.21).

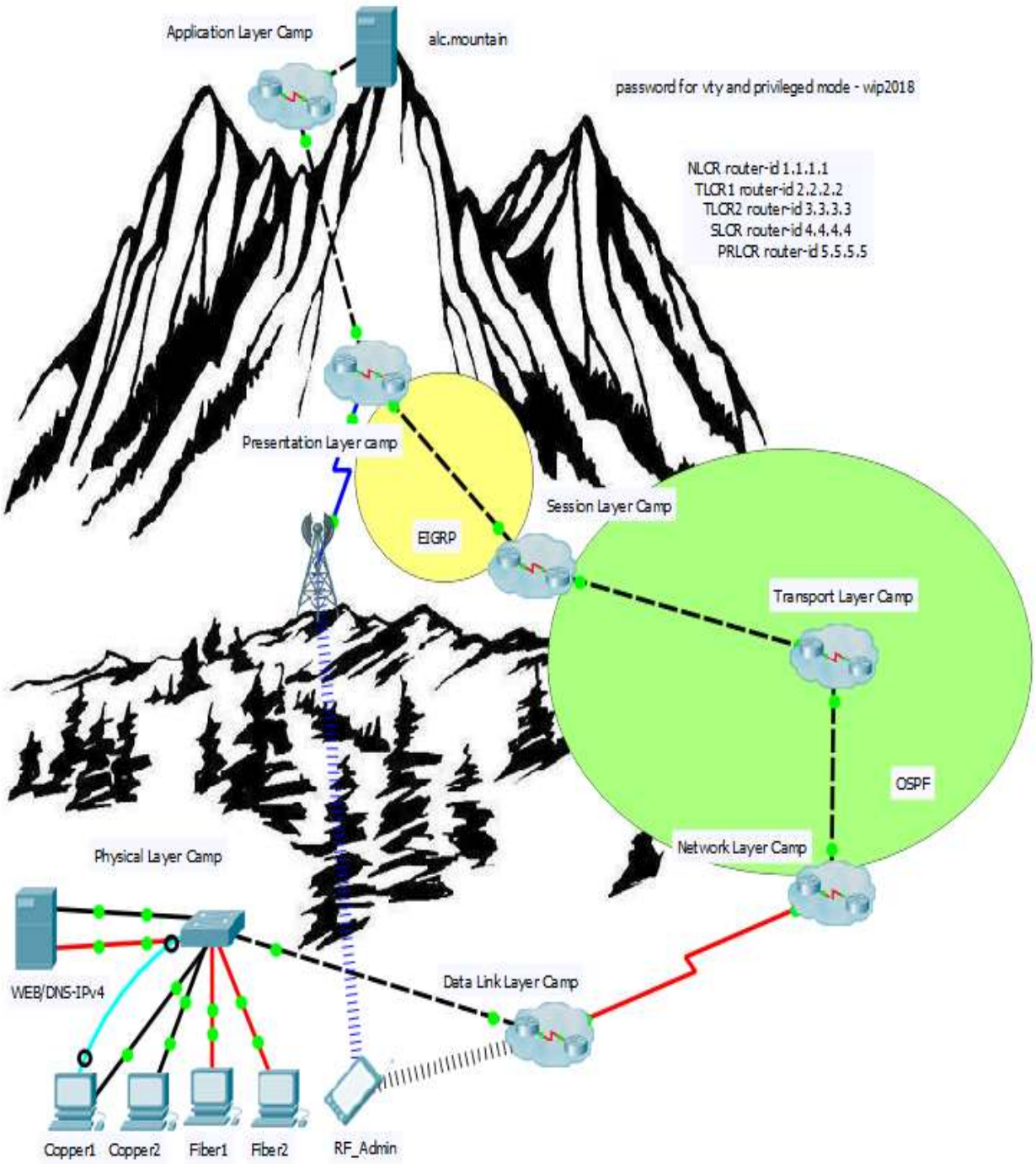


Рисунок 5.21 - L3 топология примера в среде Cisco Packet Tracer

6 Согласование трансляции данных

6.1 Протоколы ориентированные и неориентированные на установление соединения

Входящий поток данных сетевого интерфейса плохо поддается прогнозированию. В то же самое время любая система обладает реактивностью. Иными словами: когда система распознает факт передачи информации, часть входящей информации уже оказалась незафиксированной. Вторая проблема может состоять в том, что информационный поток, состоящий из блоков данных нерегламентированной длины на принимающей стороне может быть считан как единственный блок с разрушенной логической структурой.

На физическом уровне задача решается за счет внедрения избыточности. Например, при передаче по интерфейсу каждому байту данных предшествует СТАРТ-бит, сигнализирующий приемнику о начале блока, за СТАРТ-битом следуют биты данных. Завершает посылку СТОП-бит, гарантирующий паузу между посылками. СТАРТ-бит следующего байта посылается в любой момент после СТОП-бита, то есть между передачами возможны паузы произвольной длительности.

Внедряемая избыточность снижает эффективность использования канала связи, поэтому внедрение дополнительных служебных данных и процедур обратной связи между приемником и передатчиком чаще всего нецелесообразно.

Стоит учесть тот факт, что в разделяемых средах передачи данных при расширении канала связи для одной пары участников соединения можно снизить эффективность работы остальной сети.

Передача в режиме без установления соединения может быть описана как передача данных, в которой каждый пакет с префиксом заголовком, содержащим адрес назначения, достаточный, чтобы обеспечить автономную доставку пакета не прибегая к другим инструкциям и блокам данных. На принимающей стороне блок данных обрабатывается в тот момент, когда он поступает без синхронизации с другими блоками из того же источника.

Передача в режиме предварительного установления соединения может быть описана как передача данных, в которой каждый пакет содержащий данные имеет свое место в цепочке и предусмотрены механизмы восстановления последовательности даже при потере одного из блоков в среде передачи (рисунок 6.1). Сеанс связи также маркируется и все его параметры согласовываются между передающей и принимающей сторонами до передачи первого блока, содержащего целевые данные.

Процесс передачи данных на уровнях L1-L3 не ориентированы на соединение. Процессы обмена данными на уровнях L5-L7 могут критически зависить от качества и скорости передаваемых данных.

Рисунок 6.1 – Пример анализа эффективности использования канала

Протоколы транспортного уровня L4 – инструмент разрешения ситуации методом разделения типов соединений на надежную передачу данных с установлением соединения и меньшей скоростью и ускоренную пересылку потоков данных с возможностью игнорирования ошибок на стороне приемника.

В качестве примера рассмотрим согласование TCP L4 (рисунок 6.2):

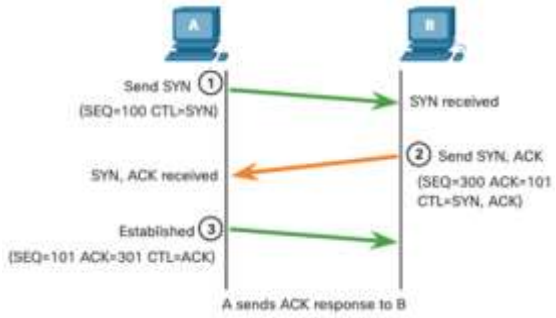


Рисунок 6.2 – Согласование TCP-сессии

Шаг 1. Инициирующий клиент запрашивает сеанс связи «клиент-сервер» с сервером.

Этап 2. Сервер подтверждает сеанс обмена данными «клиент-сервер» и запрашивает сеанс обмена данными «сервер-клиент».

Шаг 3. Инициирующий клиент подтверждает сеанс связи «сервер-клиент».

На уровне L3 все пакеты, участвующие в согласовании открытия TCP-сессии (SYN, ACK, SYN/ACK), передаются независимо могут быть потеряны, что приводит к некоторым ошибкам свзи, обрабатываеми программным слоем L7.

Прекращение TCP-соединения тоже требует согласования участников:

Шаг 1. Когда у клиента больше нет данных для отправки в потоке, он отправляет сегмент с установленным флагом FIN.

Шаг 2. Сервер отправляет подтверждение ACK, чтобы подтвердить получение FIN для завершения сеанса связи «клиент-сервер».

Шаг 3. Сервер отправляет FIN клиенту, чтобы завершить сеанс «сервер-клиент».

Шаг 4. Клиент отправляет в ответ сегмент ACK для подтверждения получения сегмента FIN от сервера.

6.2 Транспортный уровень ISO/OSI (L4)

Транспортный уровень подобно канальному и сетевому уровням выполняет функции, обеспечивающие надежную пересылку данных от передающего узла к принимающему. Транспортный уровень гарантирует, что данные на принимающей стороне собираются в правильном порядке, в независимости от порядка поступления составляющих их частей. Кроме этого, по завершении пересылки принимающий узел может послать этому подтверждение.

Транспортный уровень выполняет несколько функций:

- отслеживание отдельных сеансов связи;
- сегментация данных и последующая сборка сегментов;
- добавление информации заголовка L4;
- определение, разделение и управление несколькими сеансами связи.

Использует сегментацию и мультиплексирование для того, чтобы различные сеансы связи чередовались в одной сети

Когда в сети используются виртуальные каналы, транспортный уровень отслеживает уникальные идентификаторы, назначенные каждому каналу. Эти значения называются портами, идентификаторами соединения или сокетами, они назначаются сеансовым уровнем.

Также транспортный уровень обеспечивает проверку сегментов данных. При этом на самом верхнем уровне контроля гарантируется безошибочная передача пакетов от узла к узлу в заданный промежуток времени.

Таким образом, два этих уровня являются ключевыми в решении задачи безошибочной доставки сообщения. Поскольку на этих уровнях принимаются решения о необходимости:

- повтора пакета данных в случае сбоя при его передаче;
- ограничения числа маршрутов по доставке сообщений;
- обеспечения правильной сборки сообщения после доставки всех его составляющих для передачи более высоким уровням.

На рисунке 6.3 представлена ситуация когда транспортный уровень отправителя разбивает сообщение, передаваемое по сети на три сегмента. На сетевом уровне сегменты упаковываются в пакеты и направляются одновременно по трем разным маршрутам получателю. На стороне получателя сетевой уровень принимает пакеты, распаковывает их и передает транспортному уровню. Транспортный уровень считает и сортирует пакеты, собирает сообщение и передает его дальше.

Для выполнения своих функций протоколы этих двух уровней внедряют дополнительные поля в структуру передаваемых данных, а в некоторых случаях дополнительно порождают служебные пакеты для сбора информации.

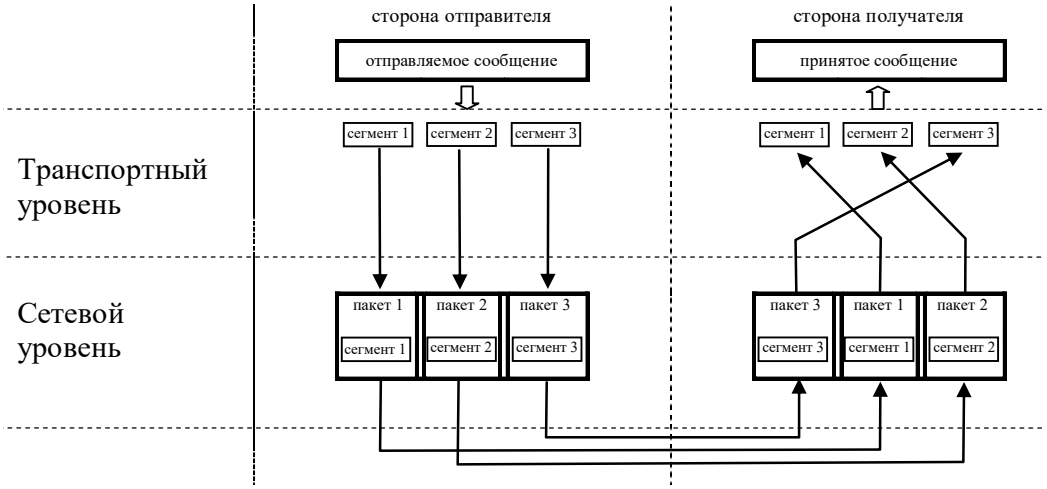


Рисунок 6.3 – Сегментирование и сборка информации на L4

6.3 Адресация транспортного уровня

Протоколы транспортного уровня используют номера портов TCP/IP для управления несколькими одновременными сеансами связи. Номер порта источника связан с исходным приложением на локальном узле, тогда как номер порта назначения связан с целевым приложением на удаленном узле. Порты классифицированы и назначаются строго в соответствии с алгоритмом (таблица 6.1).

Формально в структуре операционной системы для идентификации процесса существуют собственные индексы (рисунок 6.4).

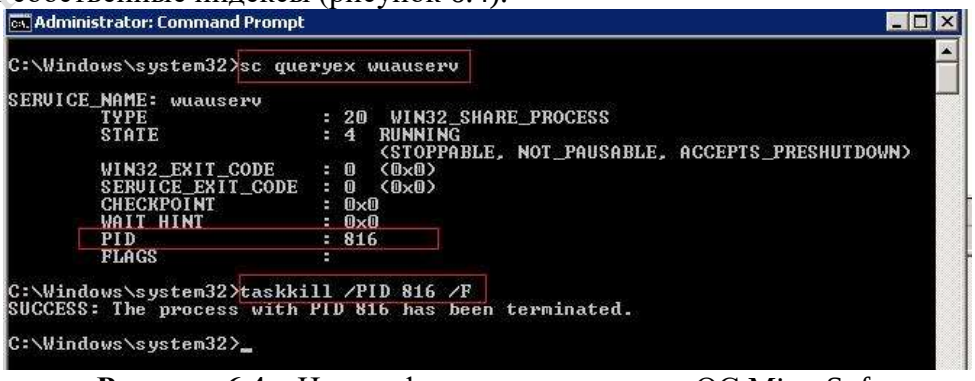


Рисунок 6.4 – Идентификация процессов в ОС MicroSoft

Номера порта источника и порта назначения инкапсулируются в PDU транспортного уровня. Затем эти сегменты инкапсулируются в пакете IP.

Сочетание IP-адреса источника и номера порта источника или IP-адреса назначения и номера порта назначения называется сокетом. Сокеты позволяют различать несколько процессов, выполняющихся на клиенте, а также распознавать различные подключения к процессу сервера. Фактически сокет обеспечивает однохначную связь «процес2процесс» в IP-сети любого масштаба для многозадачных операционных систем (рисунок 6.5).

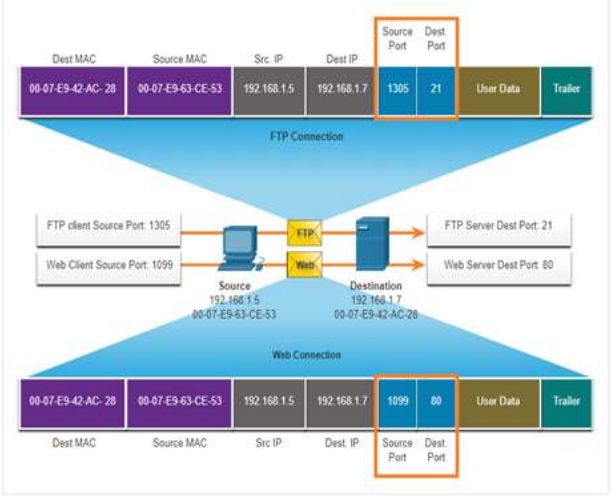


Рисунок 6.5 – Позиция полей значения портов TCP/IP в структуре кадра L2

Таблица 6.1 – Функции диапазонов портов TCP/IP

Группа портов	Диапазон номеров портов	Описание
Общеизвестные порты	От 0 до 1023	Они обычно используются приложениями, такими как веб-браузеры и почтовые клиенты, а также клиентами удаленного доступа. Определенные хорошо известные порты для общих серверных приложений позволяют клиентам легко определить требуемую службу.
Зарегистрированные порты	От 1024 до 49151	IANA по запросу организаций присваивает данные порты для каких-либо специфичных процессов или приложений. Эти процессы в основном представляют собой отдельные приложения, которые пользователь решил установить, а не широко распространенные приложения, которым обычно присваивают общеизвестные номера портов. Например, Cisco зарегистрировал порт 1812 для процесса аутентификации сервера RADIUS.
Частные и/или динамические порты	От 49152 до 65535	Эти порты также известны как эфемерные порты. Операционная система клиента обычно присваивает номера портов динамически при инициировании подключения к службе. После чего такой порт используется для определения клиентского приложения во время обмена данными.

Примеры общеизвестных портов TCP/IP и протоколов сервисной стороны, которые им назначены:

- 21: File Transfer Protocol (FTP).
- 22: Secure Shell (SSH).
- 25: Простой протокол передачи почты (SMTP).
- 53: Система доменных имен (DNS).
- 80: Протокол передачи гипертекста (HTTP).
- 443: HTTP Secure (HTTPS).
- 123: Протокол сетевого времени (NTP).
- 143: Internet Message Access Protocol (IMAP)
- 161: Простой протокол управления сетью (SNMP).

6.4 Протоколы транспортного уровня

Протоколы транспортного уровня не определяют способ доставки или передачи пакетов. Их задача выбрать способ передачи сообщений между узлами и отвечать за управление требованиями надежности сеанса связи.

Согласно RFC 1122 на транспортном уровне действуют два протокола - TCP и UDP (рисунок 6.6).

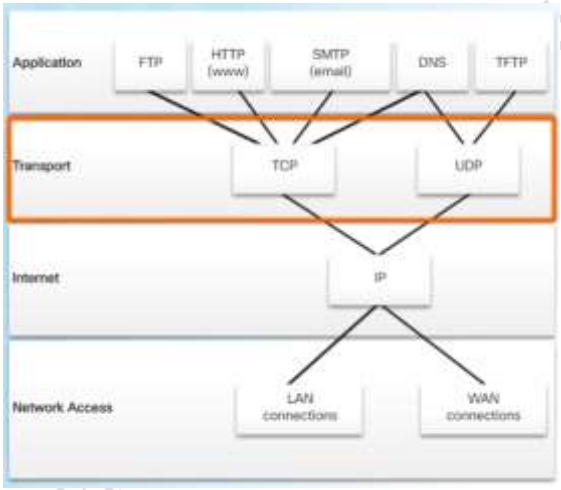


Рисунок 6.6 – Протоклоы транспортного уровня и их роли в TCP/IP

Протокол управления передачей (TCP) обеспечивает надежность и управление потоком данных от отправителя к получателю.

Основные операции TCP:

- отслеживание количества сегментов, отправленных на хост приложением;
- подтверждение полученных данных;
- повторная передача сегментов с неподтвержденными данными по истечении времени ожидания;
- восстановление последовательности данных, которые могут поступать в неправильном порядке;
- отправка данных с эффективной скоростью, приемлемой получателем.

Формат сегмента L4 TCP (20 байт) представлен на рисунке 6.7,а.

Протокол Пользовательских датаграмм (UDP) обеспечивает только основные функции для обмена сегментами данных между приложениями, при этом данный протокол отличается незначительными накладными расходами и практически отсутствием проверки данных. UDP — протокол транспортного уровня без установки соединения. В UDP нет подтверждения того, что данные получены в месте назначения.

Формат датаграммы L4 UDP (8 байт) представлен на рисунке 6.7,б.

а)

б)

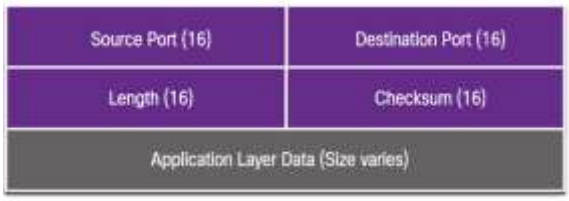


Рисунок 6.7 – Структура PDU транспортного уровня:
а) сегмент TCP; *б)* датаграмма UDP

Порт источника - 16-битное поле, используемое для идентификации исходного приложения по номеру порта сегмента или датаграммы.

Порт назначения - 16-битное поле, используемое для идентификации приложения назначения по номеру порта сегмента или датаграммы.

Порядковый номер - 32-битное поле, используемое для пересборки данных на принимающей стороне или запроса повторной передачи утраченного сегмента.

Номер подтверждения - 32-битное поле, используемое для указания того, что данные получены и ожидается следующий байт от источника.

Длина заголовка - 4-битное поле, которое указывает длину заголовка сегмента TCP.

Управляющие биты (6 бит) - включает двоичные коды или флаги, которые указывают назначение и функцию сегмента TCP.

Размер окна - 16-битное поле, используемое для указания количества байтов, которые могут быть приняты.

Контрольная сумма - 16-битное поле, используемое для проверки ошибок заголовка и данных сегмента или датаграммы.

Срочность - 16-битное поле, используемое для указания срочности содержащихся данных.

Одним из требований к надежному каналу связи в современных сетевых структурах стала конфедициальность. Внедрение Hypertext Transfer Protocol Secure (HTTPS) в 1994 году привело к негативному эффекту. Разорванная TCP-сессия либо могла быть восстановлена с большой задержкой, либо не восстановлена вообще. Решение проблемы заняло много времени и промышленные стандарты, сложившиеся в этот период, не уступают рынок. Quick UDP Internet Connections (QUIC) начали внедрять в 2012 году (рисунок 6.8). По состоянию на 2017 год существовало 4 активно поддерживаемых варианта релиза протокола.

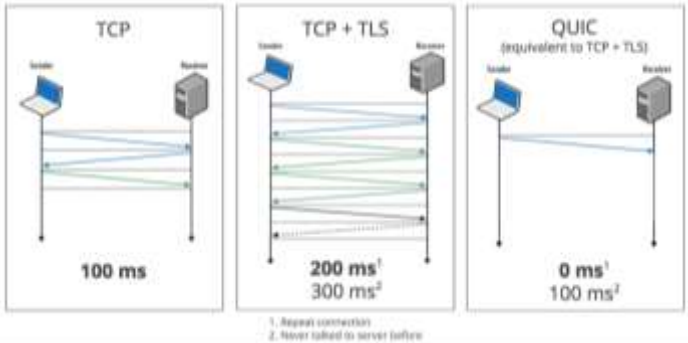


Рисунок 6.8 – Сравнение задержек в восстановлении защищенной сессии

QUIC позволяет мультиплексировать несколько потоков данных между двумя компьютерами, работая поверх протокола UDP и содержит возможности шифрования, эквивалентные TLS и SSL (рисунок 6.9).

Рисунок 6.9 – Внедрение механизмов надежной передачи в датаграмму UDP

По состоянию на август 2022 года только около 8% сайтов сети Интернет используют QUIC.

7 Взаимодействие между процессами

7.1 Сеансовый уровень ISO/OSI (L5)

Сеансовый уровень отвечает за установление и поддержку коммуникационного канала между двумя узлами. Сеансовый уровень определяет продолжительность работы узла на передачу, а также способ восстановления информации после ошибок передачи. По окончанию сеанса связи этот уровень подает команды отключения узлов.

Например, поле «Порядковый номер» заголовка TCP ограничен размером в 32 бита. Если считать границу контроля на каждый передаваемый байт, то максимальный размер транслируемых одной TCP-сесии:

$V = 2^{32}$ *байт = 4 Гбайт*

Версия ядра Linux 5.19 (август 2022) содержит интеграцию BIG TCP, позволяющих увеличить максимальный размер пакета TCP-пакета до 4ГБ для оптимизации работы высокоскоростных внутренних сетей дата-центров.

Функции сеансового уровня:

- создание и поддержание диалогов между исходными и конечными приложениями;
- обеспечение обмена данными для установления связи, поддержания ее в активном состоянии и для перезапуска сеансов, которые были прерваны или неактивны в течение продолжительного времени.

Программное обеспечение уровня L5 крайне редко генерирует сообщения для пользовательского интерфейса, поэтому возникает необходимость дополнительного информирования пользователя об ограничении сеансового уровня (рисунок 7.1).

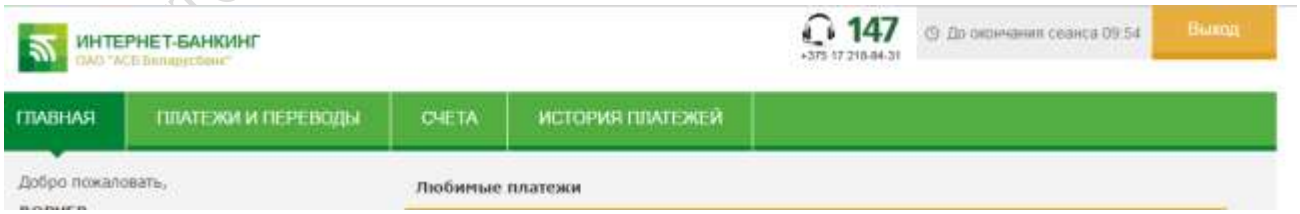


Рисунок 7.1 – Пример вывода данных о времени истечения сеанса

Сеансовый уровень отвечает за установление контрольных точек и восстановление. Он позволяет соответствующим образом совмещать и синхронизировать информацию нескольких потоков, возможно от разных источников.

Примером применения является организация видеоконференций в сети, когда звуковой и видеопотоки должны быть синхронизированы для избежания проблем с синхронизацией движения губ с речью. Управление правами на участие в разговоре гарантирует, что тот, кто

показывается на экране, действительно является собеседником, который в данный момент говорит. Ещё одним применением являются передачи в прямом эфире, в которых необходимо без резких переходов накладывать звуковой и видеопотоки и переходить от одного потока к другому во избежание перерывов в эфире или излишних наложений.

7.2 Представительский уровень ISO/OSI (L6)

Представительский уровень управляет форматированием данных, поскольку прикладные программы нередко используют различные способы представления информации. В некотором смысле, он выполняет функции программы проверки синтаксиса. Он гарантирует, что числа и символьные строки передаются именно в том формате, который понятен принимающему узлу.

Три основные функции уровня L6:

- форматирование или представление данных из исходного устройства в форме, подходящей для получения устройством назначения;
- сжатие данных таким образом, чтобы их можно было распаковать на устройстве назначения;
- шифрование данных для передачи и дешифрование при получении.

Часть требуемого функционала оптимально оказалось реализовать предложив разработчикам операционных систем ограниченный набор форматов документов, которые по умолчанию должны поддерживаться на обеих сторонах сетевого обмена (рисунок 7.2).

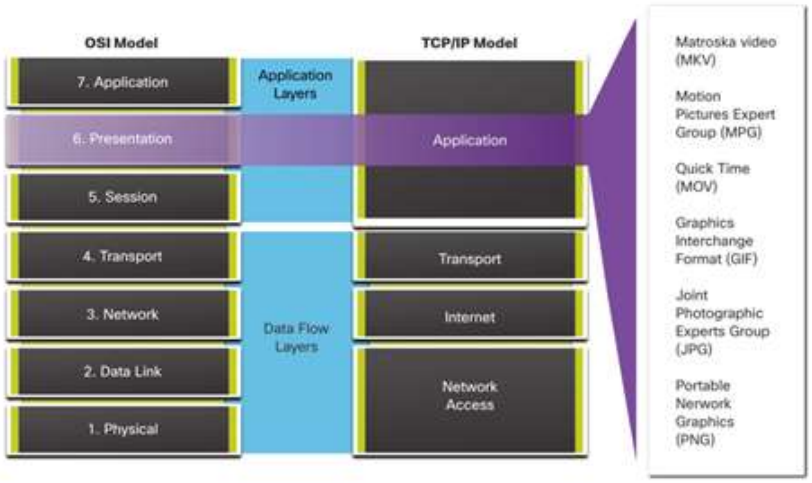


Рисунок 7.2 – Рекомендуемые форматы медиаданных

Шифрование и дешифрование транслируемых данных нагружает ресурсы на отправляющей и принимающей сторонах (в качестве таких устройств могут быть устройства-организаторы IP-туннеля), ретранслирующие сетевые устройства передают данные PDU L1-L4 без дополнительного вмешательства. В качестве примера этого сервиса рассмотрим IPsec (рисунок 7.3).

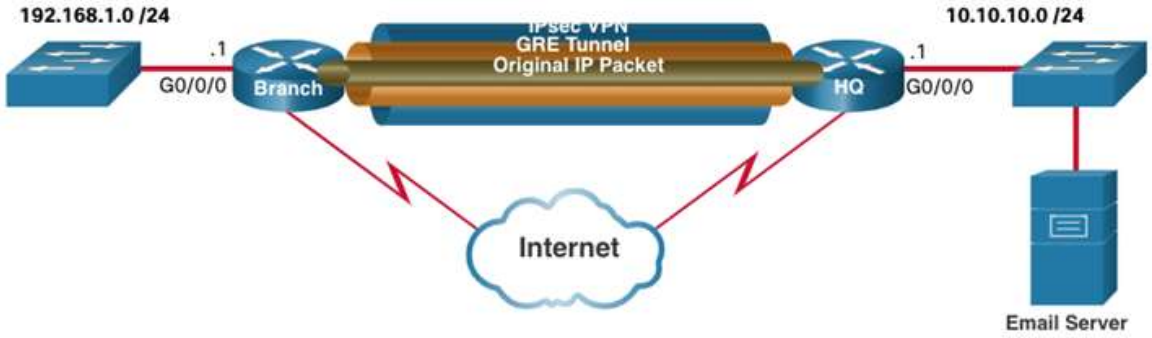


Рисунок 7.3 – Защита туннелированного трафика в публичных сетях

Для обеспечения безопасной связи протокол IPsec не привязан ни к каким специальным правилам. Открытые слоты, показанные в структуре IPsec на рисунке 7.4, могут быть заполнены любым из вариантов, доступных для этой функции IPsec, для создания уникальной ассоциации безопасности (SA).

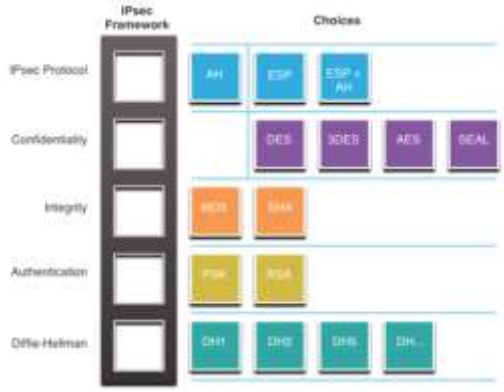


Рисунок 7.4 – Набор параметров IPsec

Пример команды активации набора IPsec в режиме защиты туннеля Site-to-Site устройств Cisco:

crypto ipsec transform-set esp-sha-hmac ah-sha-hmac esp-des

7.3 Прикладной уровень ISO/OSI (L7)

Прикладной уровень управляет доступом к приложениям и сетевым службам. Примером таких служб являются передача файлов, управление файлами, удаленный доступ к файлам, управление сообщениями электронной почты.

Например, на прикладном уровне работает редиректор сетевой операционной системы. Редиректор – это служба, позволяющая видеть компьютер в сети и обращаться к нему. Если в сети разрешается общий доступ к некоторой папке, то при помощи редиректора другие компьютеры могут видеть эту папку и использовать ее. Таким образом, локально выполняемое приложение не ощущает разницы между локальным и сетевым диском при своем обращении к файловой системе.

Работа редиректора может приводить к негативным последствиям. Например, если в файловой системе операционной системы используются присоединенные диски (рисунок 7.5) и возникнет проблема их текущей недоступности. Любая файловая операция L7 будет обращаться к протоколам уровня L5 для проверки доступности этих устройств вне зависимости обращается приложение к присоединенному сетевому ресурсу или не обращается.

Рисунок 7.5 – Пример присоединенных сетевых устроств

Для успешного обмена данными протоколы уровня приложений на узлах источника и назначения должны быть совместимыми. Совместимость обеспечивается в том числе сверкой версий реализации протоколов и сервисов. Например, если на стороне web-хостинга прошло обновление части программных модулей, может потребоваться обновить программное обеспечение браузера на стороне клиентской операционной системы.

При этом протоколы, используемые в современных сетевых структурах, могут иметь достаточно значительную историю изменений и обновлений:

- Domain Name Server (DNS), год внедрения 1985 - переводит доменные имена, такие как cisco.com, в IP-адреса.
- Bootstrap Protocol (BOOTP), год внедрения 1985 – в современных сетевых структурах вытеснен DHCP.
- Dynamic Host Configuration Protocol (DHCP), год внедрения 1993 – динамически назначает IP-адреса клиентским станциям при запуске.
- Simple Mail Transport Protocol (SMTP), год внедрения 1985 - позволяет клиентам отправлять электронную почту на почтовый сервер.
- Post Office Protocol (POP), год внедрения 1988, Internet Message Access Protocol (IMAP), год внедрения 1986 - позволяют клиентам получать электронную почту с почтового сервера.
- File Transfer Protocol (FTP), год внедрения 1971 - надежный, ориентированный на соединение протокол доставки файлов.
- Trivial File Transfer Protocol (TFTP), год внедрения 1981 - простой протокол передачи файлов без установления соединени.
- Hypertext Transfer Protocol (HTTP), год внедрения 1989 - набор правил для обмена текстом, графическими изображениями и т.д.
- Hypertext Transfer Protocol Secure (HTTPS), год внедрения 1994 - использует шифрование и аутентификацию для безопасной связи.
- Quick UDP Internet Connections (QUIC), год внедрения 2012 - позволяет мультиплексировать несколько потоков данных между двумя компьютерами, работая поверх протокола UDP и содержит возможности шифрования, эквивалентные TLS и SSL.

В качестве примера рассмотрим принцип работы протокола DHCP. На стороне сервера DHCP работает как сервис прикладного уровня L7, настороне клиента DHCP может стартовать до назначения IP-адресации L3, чтобы получить широкий набор параметров, необходимых для успешной работы клиентской операционной системой с сетевыми ресурсами.

Процесс взаимодействия DHCP (рисунок 7.6):

- Когда устройство IPv4, на котором настроено использование DHCP, загружается или подключается к сети, клиент выполняет широковещательную рассылку DHCPDISCOVER с целью идентификации доступных серверов DHCP в сети.
- Сервер DHCP отвечает сообщением с предложением DHCP (DHCPOFFER), которое предлагает клиенту «арендовать» адрес. Если клиент получает несколько предложений из-за нескольких DHCP-серверов в сети, он должен выбрать одно.
- Клиент отправляет сообщение с запросом DHCP (DHCPREQUEST), в котором клиент указывает конкретный сервер и предложение аренды, которое он принимает.
- Затем сервер возвращает сообщение DHCPACK, подтверждающее клиенту, что аренда завершена.
- Если предложение больше недействительно, выбранный сервер отвечает сообщением с отрицательным подтверждением DHCP (DHCPNAK) и процесс должен начаться с нового сообщения DHCPDISCOVER.

DHCPv6 содержит набор сообщений, схожий с сообщениями для DHCPv4. Сообщения DHCPv6: SOLICIT, ADVERTISE, INFORMATION REQUEST и REPLY.

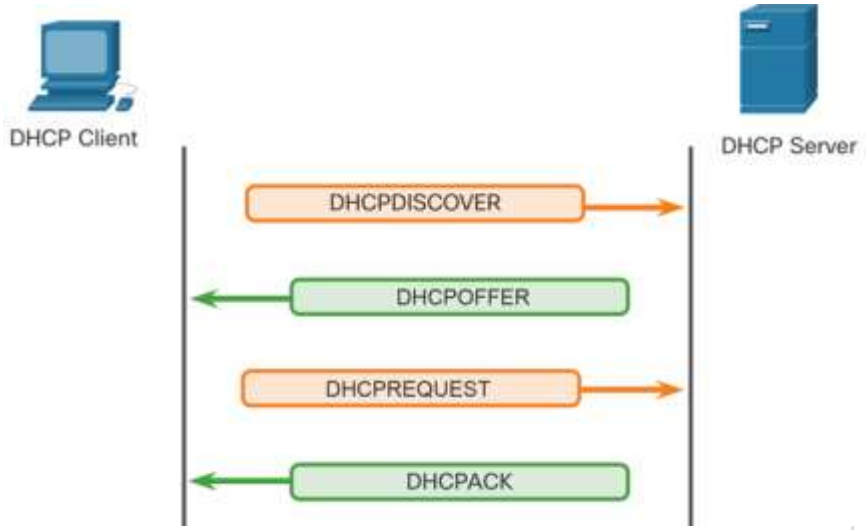


Рисунок 7.6 – Пример успешного соединения DHCPv4

7.4 Устройства и сервисы уровня приложений TCP/IP

Уровень приложений TCP/IP (DoD) является фунционально объединяющим для уровней L5-L7 ISO/OSI (рисунок 7.7).

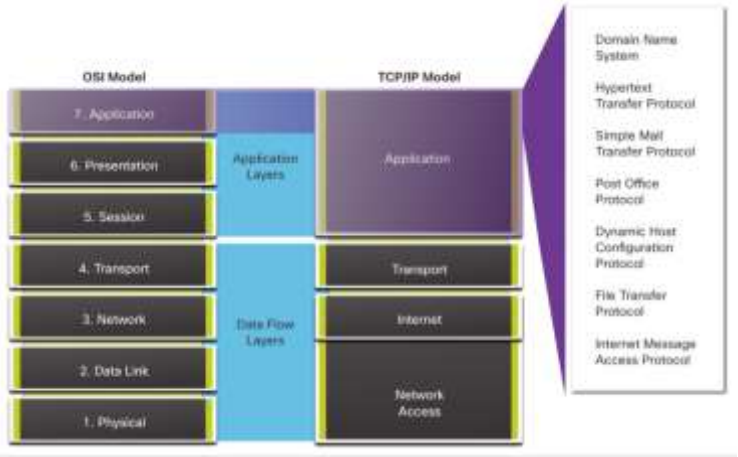


Рисунок 7.7 – Функциональное объединение уровней L5-L7 ISO/OSI

Высокоуровневый фунционал часто включают в состав устройств, котрые формально считаются гибридными (ADSL-модем, ONT), но не менее часто входит в состав профессиональных устройств L2 и L3. В рамках пособия все ранее не рассмотренные сервисы уровня приложений TCP/IP вынесены в этот параграф.

В частности, промышенные сетевые шлюзы и устройства информационной безопасности охватывают в своей работе все семь уровней модели OSI. Шлюз принимает данные из одной среды, удаляет старый протокольный стек и переупаковывает их в протокольный стек системы назначения. Для этой работы необходимо ведение расширенных таблиц адресации и маршрутизации.

Обычно в качестве такого устройства используют выделенный сервер. Попутно он может собирать обширную статистику о запросах пользователя как, например, сервера типа *PROXY*.

Если шлюз используется в качестве коммуникационного центра гетерогенной сети, то он должен выполнять функции переводчика (транслятора протоколов) и/или конвертора (преобразователя сигналов).

Обрабатывая данные, шлюз выполняет следующие операции (рисунок 7.8):

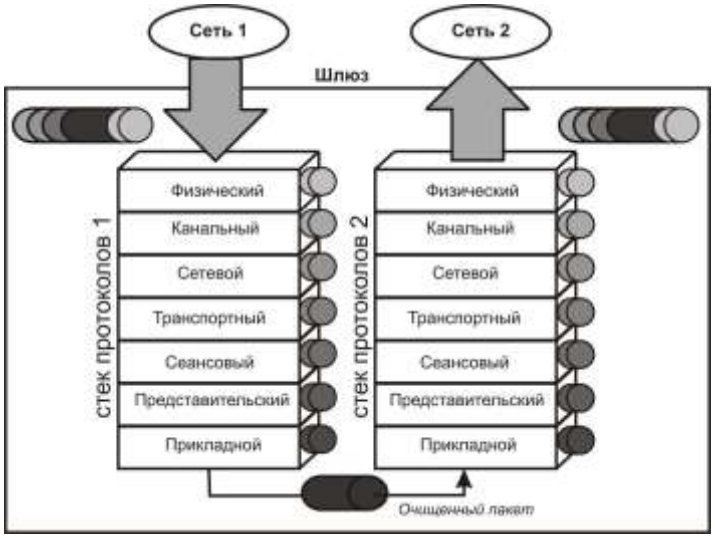


Рисунок 7.8 – Преобразование пакета данных шлюзом

− извлекает данные из приходящих пакетов, пропуская их снизу вверх через полный стек протоколов передающей сети;

− заново упаковывает полученные данные, пропуская их сверху вниз через стек протоколов сети назначения.

Еще одно назначение современных сетевых шлюзов – роль узла обработки трафика IoT-устройств в модели туманных вычислений LAN.

Одним из новых направлений, которому следует уделить особое внимание при проведении исследований, является граница перехода сетевого трафика беспроводной сети между разнородными стандартами. Например, WiFi-Ethernet, WiFi-ZigBee, ZigBee-Bluetooth или Bluetooth-NFC. В рамках гибридного устройства связи такой переход осуществляется с помощью проприетарных программных средств. Примеры уязвимостей информационной безопасности в этой точке движения сетевого трафика были зафиксированы в 2019 и 2020 годах.

К специфичным устройствам L7 можно отнести следующие:

- сетевое устройство печати;
- голосовой шлюз VOIP;
- сетевое хранилище NAS;
- Cisco Email Security и Cloud Web Security.

Сетевая печать – это частный случай распределенной печати. Организация распределенной печати, т. е. распределение ресурсов печатающих устройств между несколькими пользователями является наиболее популярным сервисом в локальной сети. Основной причиной этого можно считать следующую постановку вопроса:

– если обеспечить всех клиентов сети локальными печатающими устройствами, то большую часть времени они будут простаивать;

– обслуживание большого количества печатающих устройств и контроль за их использованием по назначению – дорогостоящая и очень сложная задача;

– скорость и качество печати на этих устройствах будут низкими, так как большое количество дорогостоящих устройств приобретаться не будет, а дешевые и бюджетные решения обладают низкими скоростью и качеством отпечатков.

Таким образом, для любой организации, применяющей в своем производственном процессе вычислительные сети, будет выгодным приобрести оптимальное количество качественных печатающих устройств и организовать обслуживание пользователей.

Разделенную печать можно реализовать следующими способами:

− *применением несетевых специализированных промежуточных устройств подключения к принтеру* (Switcher – переключатель). Такие устройства являются наиболее дешевым и простым с точки зрения пользователя решением данной проблемы. Компьютеры

пользователей подключаются к Switcher-у с помощью стандартных портов: COM, LPT, USB (рисунок 7.9). Switcher является «прозрачным» для запросов пользователя и, таким образом, принтер как бы локально подключен к компьютеру. Очередность доступа к принтеру передается последовательно между всеми портами Switcher-а. Если одно из устройств начало печатать, для остальных принтер переходит в состояние «занят». Очередь печати управляется операционной системой клиента;

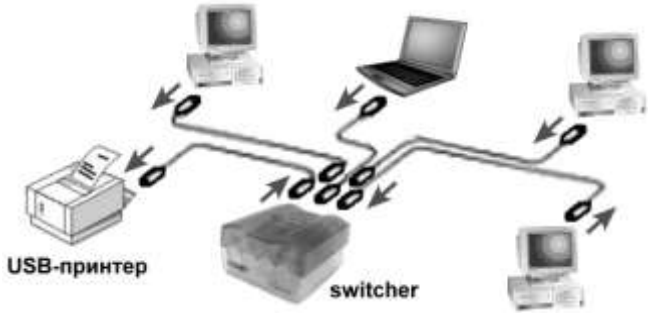


Рисунок 7.9 – Схема подключения к принтеру через Switcher

− *использованием аппаратных принт-серверных средств* (принтер подключается к сети непосредственно или через специализированное устройство). Если в предыдущем случае уровень физического доступа к печати был ограничен числом портов Switcher-а, то здесь все клиенты сети физически подключены к печатающему устройству потому что оно, в свою очередь, подключено к сети. Ограничение доступа к таким устройствам осуществляется назначением прав сетевой политики;

− *с помощью программно-эмулируемых принт-серверных устройств*. Самый медленный способ организации сетевой печати. В этом случае часть производительной мощности сервера выделяется на обслуживание заданий печати. Очередь на печать строится в пределах операционной системы сервера. Управление заданиями печати возлагается на сервер и его администратора, но часть прав по управлению этой очередью можно передать и клиентам сети.

Права доступа к принтеру определяются двумя способами:

− авторизовано (на уровне пользователей);

− на уровне ресурсов (общий пароль доступа).

Управление правами доступа, как правило, осуществляется с помощью специализированного ПО, поставляемого вместе с аппаратным принт-сервером, либо посредством протокола удаленного управления (например, TELNET).

Балансирование нагрузки между несколькими принтерами. В случае когда несколько принтеров, подключены и доступны для печати их можно объединить их в «Пул принтеров». Операционная система будет вести одну очередь для этого логичского устройства и будет сама выберет выбирать свободный принтер для отправки задания на печать.

Резервное копирование (*backup*) – процесс создания копии данных на носителе (жёстком диске, дискете и т. д.), предназначенном для восстановления данных в оригинальном месте их расположения в случае их повреждения или разрушения.

Резервное копирование необходимо для возможности быстрого и недорогого восстановления информации (документов, программ, настроек и т. д.) в случае утери рабочей копии информации по какой-либо причине.

Виды резервного копирования:

- полное резервирование (*Full Backup);*
- дифференциальное резервирование *(Differential Backup)*;
- добавочное резервирование *(Incremental Backup);*
- пофайловый метод.

Для резервного копирования очень важным вопросом является выбор подходящей схемы ротации носителей (например, магнитных лент, DVD дисков). Наиболее часто используют следующие схемы:

- одноразовое копирование;
- простая ротация;
- «дед, отец, сын»;
- «ханойская башня»;
- «10 наборов».

Схемы «ханойская башня» и «10 наборов» используются нечасто, так как многие системы резервирования их не поддерживают.

В некоторых случаях для увеличения вероятности сохранности данных комбинируются локальные и глобальные технологии передачи данных. Тогда схема общей системы резервного копирования данных может стать такой же сложной, как показано на рисунке 7.10.

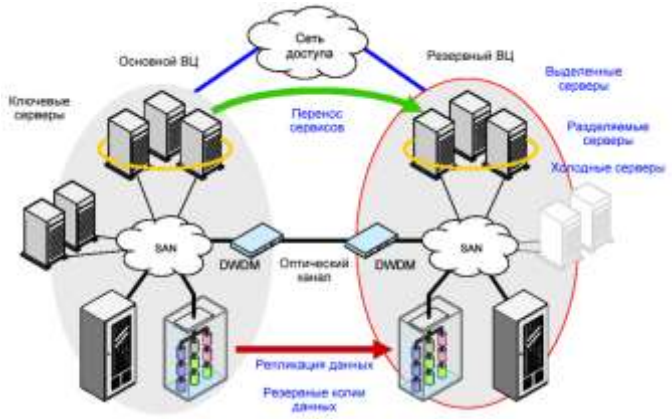


Рисунок 7.10 – Пример схемы резервного копирования

Самыми важными свойствами резервных копий являются: их наличие и защита от несанкционированного доступа. В случае потери основной копии данных – резервная дает возможность минимизировать финансовые убытки, которые вызовет остановка производственного цикла, либо полномерная ревизия текущей обстановки. Наличие механизмов защиты в резервных копиях снижает вероятность убытков от промышленного шпионажа.

DNS (Domain Name Service – служба доменных имен) обеспечивает поиск имен хостов, используя распределенную по сетевым серверам имен базу данных. Когда клиент выполняет запрос, процесс DNS-сервера сначала ищет это имя в своих записях, чтобы разрешить его. Если имя не удалось разрешить по локальным записям, сервер обращается к другим серверам для разрешения имени (рисунок 7.11).

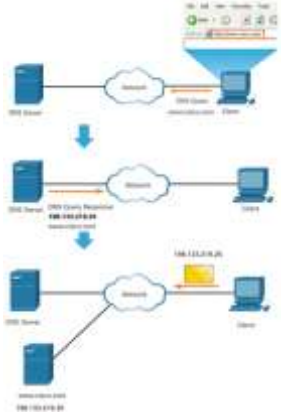


Рисунок 7.11 – Последовательность операций DNS-resolving

Когда совпадение найдено, числовой адрес возвращается исходному серверу, который определенное время хранит эту запись на случай повторного запроса.

В DNS используется иерархическая структура для создания базы данных и разрешения имен. У каждого DNS-сервера имеется отдельный файл с базой данных. Сервер управляет привязкой имен к IP-адресам только в отдельной небольшой части общей структуры DNS.

Примеры доменов верхнего уровня:

- .com - коммерческие или промышленные предприятия
- .org - некоммерческие организации
- .au - Австралия
- .by - Беларусь

Служба времени и календаря на базе Network Time Protocol (*NTP*) позволяет всем устройствам в сети синхронизировать свои настройки времени с NTP-сервером, что обеспечивает более согласованные настройки времени, установление точной последовательности событий в распределенных системах, планирование запуска сервисов и многое другое. NTP можно настроить для синхронизации с частным генератором тактовых импульсов или общедоступным сервером NTP в Интернете.

Протокол использует структуру распространения информации между серверами точного времени, образующими самоорганизующуюся иерархическую структуру «ведущий-ведомый» (master-slave) для синхронизации локальных часов устройства или сетевой структуры (рисунок 7.12).

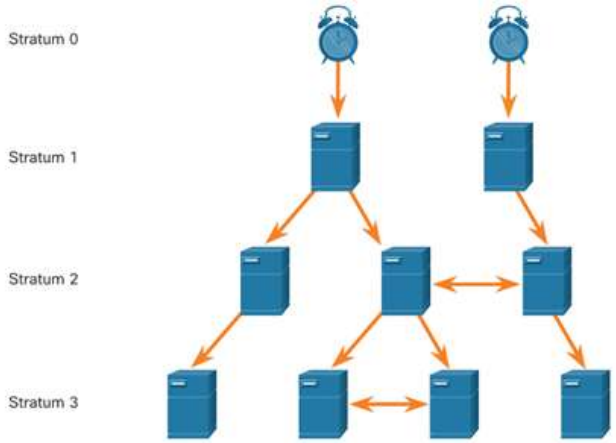


Рисунок 7.12 – Иерархия взаимодействия NTP-устройств

Каждый уровень иерархической системы называется часовым слоем (stratum). Уровень часового слоя определяется как количество переходов от доверенного источника. Для распределения синхронизированной информации о времени по сети используется протокол NTP.

Максимальное количество переходов равно 15. Часовой слой 16 имеет самый низкий уровень и указывает на то, что устройство не синхронизировано. Серверы времени, находящиеся в одном часовом слое, могут работать как равноправные серверы времени на одном уровне часового слоя для обеспечения резервирования или проверки правильности времени.

Устройства слоя 0: Эти доверенные источники времени, также называемые устройствами часового слоя 0, являются высокоточными устройствами хранения времени, которые считаются точными и работают практически без задержек.

Устройства слоя 1 подключены напрямую к доверенным источникам времени. Они выступают в роли основного стандарта сетевого времени.

Слой 2 и ниже. Серверы слоя 2 подключены к устройствам слоя 1 через сеть. Устройства часового слоя 2, например клиенты NTP, синхронизируют свое время с помощью пакетов NTP, которые они получают от серверов часового слоя 1. Эти устройства могут также выступать в роли серверов для устройств часового слоя 3.

8 Управление компонентами сети

8.1 Формализация процессов сетевого управления

Различают два варианта организации управления компонентами сети – одноранговые сети и сети на основе сервера, что соответствует *децентрализованной* и *централизованной* системе управления.

Одноранговые или *пиринговые* сети (*peer-to-peer, P2P – равный с равным*) – это компьютерные сети, основанные на равноправии участников. В таких сетях отсутствуют выделенные серверы, а каждый узел (peer) является как клиентом, так и сервером.

В качестве клиента (потребителя ресурсов) каждая из машин может посылать запросы на предоставление каких-либо ресурсов другим машинам в пределах этой сети и получать их. Как сервер, каждая машина должна обрабатывать запросы от других машин в сети, отсылать то, что было запрошено, а также выполнять некоторые вспомогательные и административные функции.

Любой узел данной сети не дает гарантии своей постоянной работы в режиме on-line. Он может подключаться к сети и выходить из нее в любой момент времени, вынуждая подключенных клиентов искать узел, предлагающий аналогичный сетевой ресурс или сервис.

При достижении определённого критического размера сети наступает такой момент, когда в сети могут дублироваться функции и некоторые виды ресурсов, что приводит к путанице при определении исполнителя запроса.

Помимо чистых P2P-сетей, существуют так называемые гибридные сети, в которых существует по крайней мере один сервер, используемый для координации работы (в сетях Bittorrent, eDonkey) или для предоставления информации о существующих машинах сети, а также их статусе: on-line, off-line и т. д. (например, в сети ICQ).

Сейчас одноранговые сети условно разделяют на следующие два подмножества: *пиринговые файлообменные сети* и *пиринговые сети распределённых вычислений*.

Сети *клиент-сервер* (*Client/Server*) – это сетевая архитектура, в которой устройства являются либо клиентами, либо серверами на постоянной основе.

Клиентом (*front end*) является запрашивающая машина (обычно ПК), сервером (*back end*) – машина, которая отвечает на запрос. Оба термина (клиент и сервер) могут применяться как к физическим устройствам, так и к программному обеспечению.

Сети *с выделенным сервером* (*Client/Server network*) – сети, в которых сетевые устройства централизованы и управляются одним или несколькими серверами. Индивидуальные рабочие станции или клиенты должны обращаться к ресурсам сети через сервер (рисунок 8.1).

Этот принцип распространяется и на взаимодействие программ и информационных сред. Программа (среда), выполняющая предоставление соответствующего набора услуг – «сервер», а программа (среда), пользующаяся этими услугами – «клиент». Технология традиционной модели «клиент-сервер» модернизируется и совершенствуется.

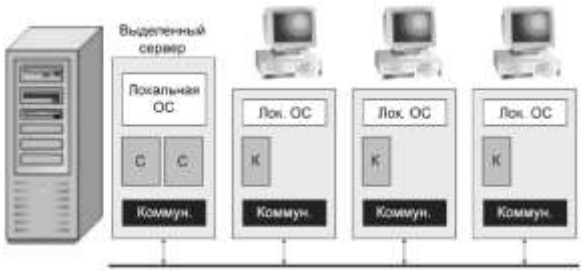


Рисунок 8.1 – Работа в сети с выделенным сервером

Аналогично вариантам организации управления компонентами сети, так же можно разделить и сетевые модели: разбиение сети на рабочие группы; построение сети на базе доменной архитектуры; группировка сетевых устройств по другим признакам.

Сетевая модель обслуживания пользователей в первую очередь зависит от того, какая операционная система установлена на каждом из узлов сети, а также, какая операционная система управляет сетевыми потоками.

Построение крупной сети на основе единственной сетевой платформы (моногенная сеть) – это большая редкость. Обычным состоянием для любой вычислительной сети средних и крупных размеров является сосуществование различных стандартов и базовых технологий.

Внедрение новых технологий, таких как Fast Ethernet или Gigabit Ethernet, не означает, что из сети мгновенно вытесняются их предшественники, например, 10-Мегабитный Ethernet, ATM, Token Ring или FDDI, так как в эти технологии были сделаны огромные капиталовложения. Поэтому трудно рассчитывать на вытеснение в обозримом будущем всех технологий в пользу какой-либо одной.

Под *гетерогенностью* (неоднородностью) сети понимают несовместимость двух узлов, принадлежащих к одной сети, либо к смежным сегментам сети по одному или нескольким логическим признакам:

- формату кадра сети;
- способу шифрования;
- типу операционной системы;
- используемой модели безопасности и пр.

Гетерогенность является непременным атрибутом любой сложной и крупномасштабной сети, поскольку нельзя удовлетворить потребности тысяч пользователей с помощью однотипных программных и аппаратных средств. В такой сети обязательно будут использоваться различные типы компьютеров – от мэйнфреймов до персоналок, несколько типов операционных систем и множество различных приложений.

Например, при объединении в сеть нескольких архитектурных поколений и платформ вычислительной техники «букет» операционных систем в пределах одной сети может достигать 10–15 единиц.

Самым распространенным средством объединения разнородных транспортных технологий является использование единого сетевого протокола во всех узлах корпоративной сети. Единый сетевой протокол работает поверх протоколов базовых технологий и является тем общим стержнем, который их объединяет. Именно на основе общего сетевого протокола маршрутизаторы осуществляют передачу данных между сетями, даже в случае очень существенных различий между их базовыми сетевыми технологиями.

При нарушении условия единства протоколов для обмена информацией требуется применение посредника, чтобы организовать обмен на прикладном, представительском, сеансовом, транспортном, а иногда и сетевом уровне (согласно модели ISO) между участниками соединения.

Для пользователя, как правило, гетерогенность сетевого обмена данными является прозрачным. В современных сетях этого чаще всего добиваются совместимостью на уровне форматов используемых документов: графические форматы, видео, аудио и прочее. В частности, это обеспечивается строгим выпонением регламента представительского уровня L6 ISO/OSI. Но до 2008 года пользователям нередко приходилось обеспечивать промежуточную трансляцию данных для возможности получения доступа на мобильных устройствах.

Построение *программных экосистем* – актуальный тренд на рынке ИТ. Программная привязка потребителя к программным решениям, которые контролирует производитель операционной системы, теоретически должна обеспечить бессбойную работу кода на стороне пользователя. По своей сути современные экосистемы - разновидность монополии, которая создает для пользователя возможность удовлетворить свои потребности в рамках единой платформы.

Примеры таких экосистем: Samsung, Huawei, Amazon, Microsoft, Google, Apple.

В большинстве этих экосистем часть данных сеанса работы пользователя хранится и анализируется на стороне вендора-владельца экосистемы. В некоторых случаях пользователь

может быть лишен права пользования программным обеспечением экоссистемы без предварительного уведомления. Например, 22 января 2020 года компания Samsung начала активно блокировать работу Smart TV на своих телевизорах, якобы не предназначенных производителем для эксплуатации на территории России. Применённые меры ударили, в первую очередь, по конечным потребителям продукции, а не по импортёрам. Устройства легально приобретались на территории сопредельных государств, но компания не обеспечила надлежащего фильтра регистрации продаваемых конечному потребителю устройств и получила репутационные потери.

Перераспределение ролей между серверами и клиентами по реализации функции вычисления на стороне сервера приведено на рисунке 8.2.

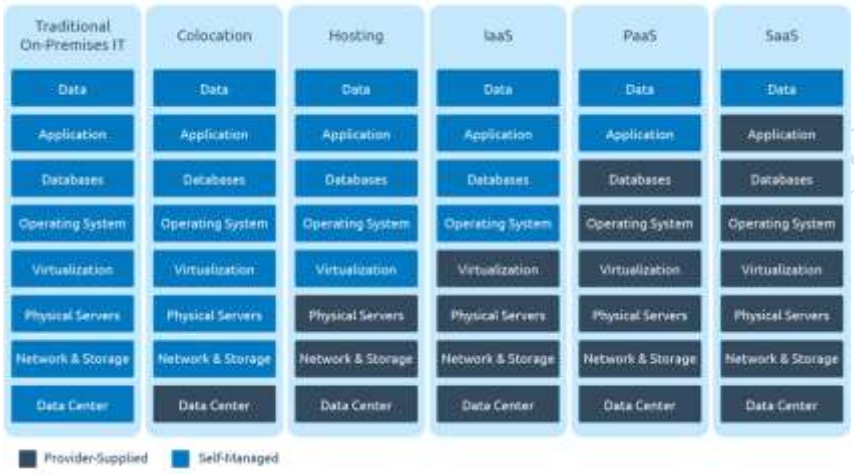


Рисунок 8.2 – Реализация сервиса удаленного обслуживания

На рисунке: On-Premises IT – традиционная клиент-серверная модель взаимодействия в LAN предприятия; Colocation – размещение оборудования предприятия в центре обработки данных ISP; Hosting – публикация данных предприятия ресурсами ISP; IaaS - инфраструктура как сервис; PaaS - платформа как сервис; SaaS – программное обеспечение как сервис.

В современном маркетинге сетевых сервисов используется подход *XaaS (Всё Как Сервис, Anything-as-a-service)*. Под него подпадают все услуги, которые оказываются через интернет и с применением облачных вычислений. Например: *база данных как сервис (DBaaS); хранилище как сервис (Storage-as-a-Service); десктоп как сервис (DaaS); коммуникации как сервис (CaaS); мониторинг как сервис (MaaS)* и даже *тестовый сервис кибератак (MaaS)*.

8.2 Операционные системы сетевых устройств

Сетевая операционная система (Network operating system) – это операционная система, которая обеспечивает обработку, хранение и передачу данных в информационной сети. Главными задачами сетевой операционной системы являются разделение ресурсов сети (например, дисковые пространства) и администрирование сети.

Операционные системы сетевых устройств – это специализированный набр программных модулей, котрые обеспечиваю продвижение PDU уровней L1-L7 через сетевые среды с максимально доступной скоростью. Поскольку такие операционные системы работают на проприетарных узкоспециализированных аппаратных платформах, то и код этих операционных систем, зачастую, проприетарный.

Например, Cisco IOS - это монолитная операционная система, работающая непосредственно на оборудовании, в то время как IOS XE представляет собой комбинацию ядра Linux и (монолитного) приложения (IOSd), который работает поверх этого ядра. С другой стороны, IOS XR основан на QNX (начиная с версии 5.0 он также основан на Linux), где приложение IOSd было разделено на множество различных приложений.

В то время как IOS XE (IOSd) и IOS используют один и тот же код, IOS XR - это совершенно другая кодовая база. Поскольку в IOS XE IOSd работает как приложение поверх

Linux, появляется возможность запускать различные приложения на оборудовании, хорошим примером этого является запуск Wireshark на коммутаторе. Другой пример - контейнеры открытых служб Cisco IOS XE.

Для объединения сетевых устройств в группы, управляемые по принципу P2P, либо архитектур «клиент-сервер» в рамках развития SNMP реализован подход разделения опеционной системы сетевого устройства на слои независимых функций (рисунок 8.3). Конечное сетевое устройство может выполнять функции слоя локально, либо делегировать контроллеру группы. Например, Link Layer Discovery Protocol (LLDP) - протокол канального уровня, позволяющий сетевому оборудованию оповещать смежные сетевые устройства, о своём существовании, передавать ему свои парметры, получать от него аналогичные сведения и команды управления.

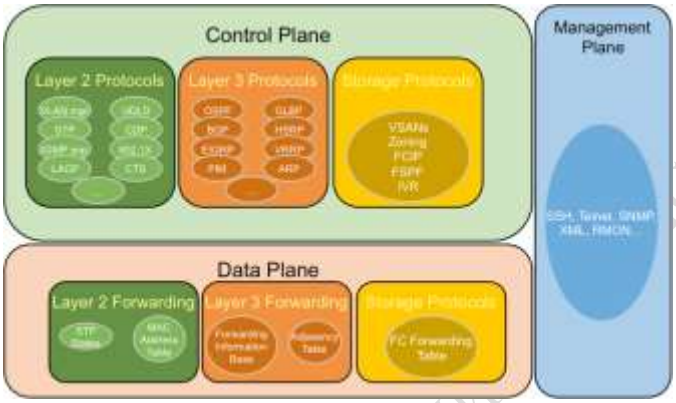


Рисунок 8.3 – Три слоя реализации функций ОС сетевого устройства

Способы доступа к операционной системе сетевого устройства (рисунок 8.4):

- консоль *(console)* - физический порт управления стандарта RS-232, используемый для доступа к устройству для обслуживания, например для выполнения начальных конфигураций;
- протокол Telnet - устанавливает небезопасное удаленное подключение CLI к устройству по сети. Данные для аутентификации пользователя, пароли и команды передаются по сети в виде простого текста. Способ отправки данных: через консоль или IP-соединение;
- Secure Shell (*SSH*) - метод, позволяющий удаленно установить защищенное подключение CLI через виртуальный интерфейс по сети. Способ отправки данных: через IP-соединение;
- веб-интерфейс – способ управления сетевым устройством средствами графического GUI. Способ отправки данных: HTTP, HTTPS;
- проприетарные программные модули удаленного управления (например, WinBOX) и системы автоматизации удаленного оборудования посредством API операционных систем сетевых устройств. Способ отправки данных: HTTPS, SOAP, REST, JSON.

Рисунок 8.4 – GUI Cisco C1000-24FP-4X-L

API - это программное обеспечение, которое позволяет другим приложениям получать доступ к его данным или услугам. Это набор правил, описывающих, как одно приложение может взаимодействовать с другим, и инструкции, позволяющие этому взаимодействию происходить. Пользователь отправляет запрос API на сервер, запрашивая конкретную информацию, и получает в ответ API от сервера вместе с запрошенной информацией.

Операционные системы сетевых устройств поддерживаются производителем экосистемы и должны получать обновления. Распространена модель обслуживания на базе подписочных сервисов.

Поддержка устаревших сетевых сервисов операционной системой сервера может создать технологическую уязвимость в сети предприятия. Примером может служить протокол Server Message Block (SMB), клиент-серверный протокол обмена файлами 1983 года. Серверы могут предоставлять свои ресурсы клиентам в сети.

В отличие от обмена файлами по протоколу FTP, клиенты устанавливают долговременное подключение к серверам. После установки соединения пользователь может получить доступ к ресурсам на сервере аналогично доступу к ресурсам на локальном хосте (рисунок 8.5).

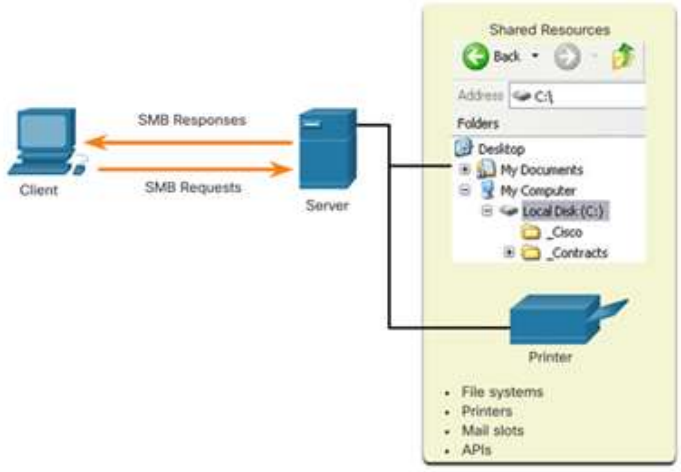


Рисунок 8.5 – Работа протокола SMB

В настоящее время SMB связан главным образом с операционными системами Microsoft Windows, где используется для реализации «Сети Microsoft Windows» (Microsoft Windows Network) и «Совместного использования файлов и принтеров» (File and Printer Sharing). Наиболее известные уязвимости в результате использования данного протокола CVE-2017-0144 EtneralBlue-Remote-Code-Execution и CVE-2022-30190 Microsoft Support Diagnostic Tool Vulnerability.

8.3 Обеспечение информационной безопасности

Реализованное решение по информационной безопасности не является гарантией предприятия от потери или «утечки» информации в компьютерных сетях и системах. Способы защиты информации и других ресурсов постоянно меняются, как меняется наше общество и технологии. Если рассматривать защиту информации в историческом разрезе, то можно выделить следующие ее виды:

- физическую безопасность;
- защиту информации в процессе передачи;
- защиту излучения;
- защиту компьютера;
- защиту сети;
- защиту информации.

Для всесторонней защиты информационных ресурсов требуется комплекс различных средств защиты, таких как:

- антивирусное программное обеспечение;
- системы управления доступом;
- межсетевые экраны (firewall);
- смарт-карты;
- биометрия;
- системы обнаружения вторжения IPS/IDS;
- управление политиками безопасности;
- шифрование и др.

Отдельной функцией контроля сети, связанной с профилактикой потенциального роста паразитного трафика, является организация работы антивирусной системы. Например, когда вирус типа «червь» (worm) поражает операционную систему, он начинает искать пути для распространения. С этой целью он рассылает по сети служебные запросы от имени системы. В сети большого масштаба такой паразитный трафик может быть значительным. Автономную систему можно защитить локальным брандмауэром, действующим совместно с антивирусным монитором, но блокировать паразитный трафик от зараженных систем без централизованной политики безопасности – практически невозможно.

В действующих вычислительных сетях хорошо зарекомендовали себя следующие антивирусные решения: Dr.Web Enterprise Suite, ESET Enterprise Security (NOD32), Kaspersky Open Space Security, McAfee Total Protection for Endpoint, Symantec AntiVirus и некоторые другие.

Еще одной важной частью системы контроля в вычислительных сетях являются системы биллинга – детализированный авторизованный учет сетевого трафика по типу запроса и объему сервиса.

Существуют комплексные решения биллинга и антивирусной защиты. Например: Kaspersky Gate Antivirus / Traffic Inspector или Panda Gate Antivirus / Traffic Inspector.

Типовой вариант схемы размещения контрольных средств в сети может выглядеть следующим образом (рисунок 8.6).

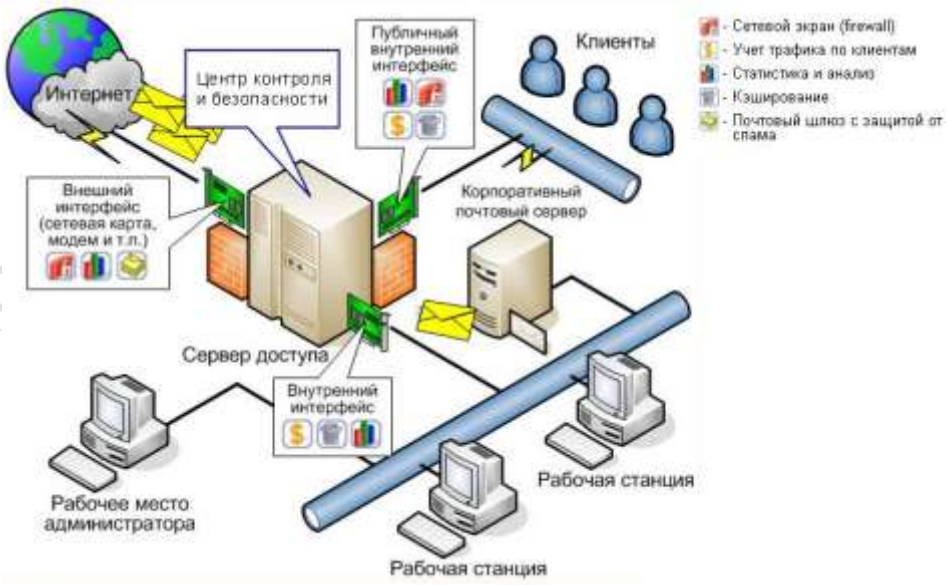


Рисунок 8.6 – Работа системы контроля сетевого трафика

При выборе программных средств сетевого контроля важно учитывать, что любое средство контроля и управления само является источником порождения дополнительного трафика и нагрузки на вычислительные мощности серверов сети. Учитывая данный факт,

необходимо найти точку баланса настроек текущей версии защитных систем, либо лучший вариант соотношения качества/цены при покупки альтернативной системы.

Во время функционирования компьютерных сетей и систем часто возникают различные проблемы. Некоторые – по чьей-то оплошности, а некоторые являются результатом злоумышленных действий. В любом случае при этом наносится ущерб. Поэтому можно назвать такие события атаками, независимо от причин их возникновения. Существуют четыре основные категории атак:

- атаки доступа;
- атаки модификации;
- атаки на отказ в обслуживании;
- атаки на отказ от обязательств.

В свою очередь, каждая категория атак делится на множество различных видов. Все эти атаки связаны с различными хакерскими методами. К этим методам относятся: социальный инжиниринг; централизованные и распределенные DoS-атаки; прослушивание коммутируемых сетей; перенаправление трафика; имитация IP-адреса; вредоносные программы («Вирусы», «Троянские кони», «Черви»).

Без понимания угроз безопасности по отношению к информационным активам организации может быть использовано либо слишком много, либо слишком мало ресурсов, или они не будут использоваться должным образом.

В сетевых операционных системах при управлении сетевыми ресурсами должна быть реализована модель системы безопасности с разграничением прав доступа на разных уровнях. В том числе: полный доступ для всех пользователей на все виды действий; ограничения на уровне пользователей; ограничения на уровне узлов сети; ограничения на уровне анализа содержимого запросов; полный запрет для всех пользователей на все виды действий.

Управление доступом к сетевым ресурсам может быть реализовано: на уровне пользователей; на уровне ресурсов; на уровне физического доступа (локальный узел).

Если доступ к сетевым ресурсам регламентируется на уровне пользователей – это означает, что пользователь сможет получить доступ к объектам системы только после того, как он будет аутентифицирован и авторизован. В процессе аутентификации система удостоверяет личность пользователя (идентифицирует его) на основании факта знания пароля либо наличия биометрических характеристик, соответствующих его учетной записи. Авторизация подразумевает назначение пользователю прав доступа к объектам системы, на основании его членства в различных группах.

Примером реализации доступа на уровне пользователей является совместное использование файлов, т. е. предоставление файлов, находящихся на компьютере, в общий доступ так, что другие пользователи могут получить к ним доступ.

Если доступ к сетевым ресурсам регламентируется на уровне оборудования – это означает, что система аутентификации использует уникальные характеристики оборудования (например, MAC-адрес).

Если доступ к сетевым ресурсам регламентируется на уровне физического доступа – это означает, что подключение пользователей осуществляется на время организации сеанса сетевого обмена. Запрет физического доступа означает невозможность подключения к сети.

Примером организации такого доступа являются сети с коммутируемыми каналами связи. На практике в локальных сетях ограничение физического доступа применяется и как штрафная санкция, и как средство защиты от внешних воздействий.

Сетевые операционные системы могут оперировать одновременно несколькими сетевыми политиками и сложными видами прав доступа. Например, согласно сетевой политике Microsoft, виды прав доступа к файловой системе могут быть такие, как указано на рисунке 8.7.

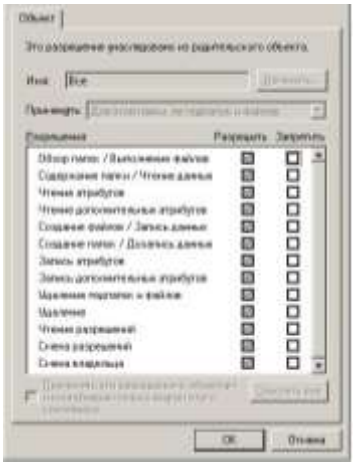


Рисунок 8.7 — Виды назначаемых прав в Windows 2000

В файловой системе NTFS у пользователя (владельца) есть возможность индивидуально назначать права доступа созданным папкам и файлам.

Пользователь, который состоит одновременно в нескольких группах, получает доступ ко всем видам ресурсов, разрешенных для каждой из групп пользователей. Но одновременно на него распространяются и запреты каждой из групп.

Успешная работа пользователя в таком случае зависит от того, насколько правильно разработана сетевая политика системным администратором и насколько корректно она применяется. Для автоматизации управления сетевой политикой используются различные скриптовые конструкции. В этом случае на вход программного скрипта подается перечень объектов, к которым его необходимо применить.

8.4 Моделирование и виртуализация сетевых структур

Перед тем как внедрять сетевое решение в программной части или при замене оборудования, удобнее апробировать его работу в среде программного симулятора.

Один из лидеров в области телекоммуникационных технологий Cisco Systems предлагает использовать программные системы моделирования сетевых структур. Системы моделирования компьютерных сетей, разработанные специалистами данной компании, позволяют быстро сконструировать сеть, настроить программную часть имитационной модели, увидеть, какие процессы происходят в созданной сети и правильно ли она функционирует. Cisco System Inc предлагает использовать бесплатный программный пакет Packet Tracer (рисунок 8.8) для *симулирования* работы сети, построенной по сетевым технологиям Cisco в рамках программы Cisco Networking Academy.

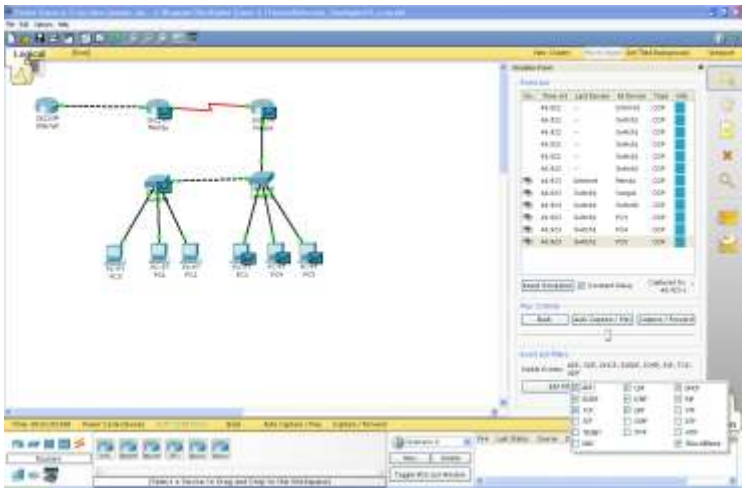


Рисунок 8.8 – Рабочее окно программы Packet Tracer

Медиатор Packet Tracer (система отслеживания пакетов) позволяет имитировать функции сетей любого размера и тем самым расширяет возможности обкатки сети на модели. Как показала практика использования данного продукта, минусом является весьма ограниченный список моделей коммутаторов и маршрутизаторов фирмы Cisco, а также отсутствие поддержки многих функций реального оборудования.

Еще одна программная система моделирования сетевых структур – *Boson Network simulator* – имеет расширенные возможности по сравнению с Packet Tracer. Данная программа позволяет получить практические знания по работе с сетевыми устройствами, начиная от обычных управляемых свичей и заканчивая маршрутизаторами и сетевыми экранами. В поставку включена утилита для моделирования сети. В ней можно смоделировать любой тип сети или выбрать готовый образец.

Еще один программный эмулятор маршрутизаторов Cisco – *Dynamips* (рисунок 8.9) разработанный Christophe Fillot работает на большинстве Linux-систем, Mac OS X и Windows, при этом позволяет эмулировать аппаратную часть маршрутизаторов, непосредственно загружая и взаимодействуя с реальными образами Cisco IOS.

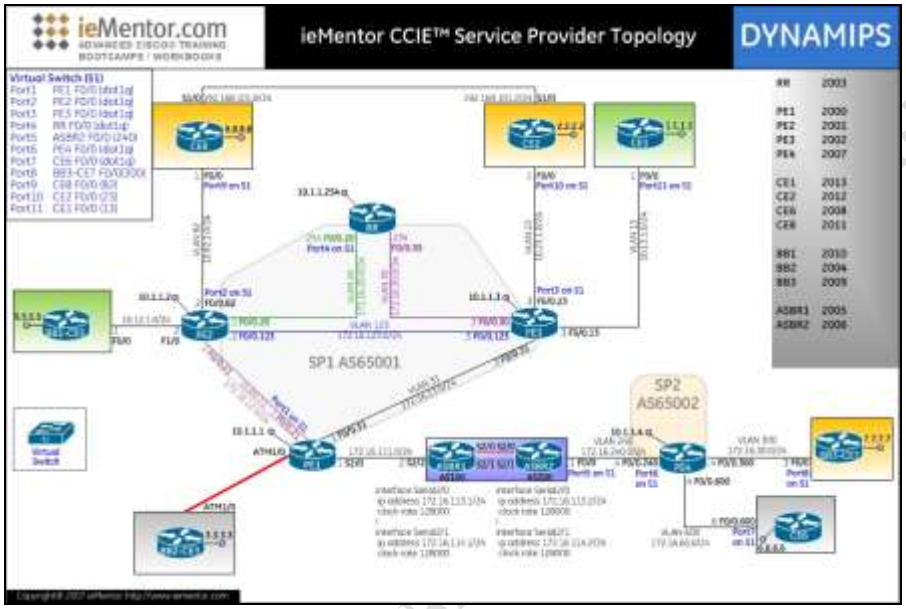


Рисунок 8.9 – Работа в среде программы Dynamips

Все же, как показывает практика, реальное оборудование никакая программа моделирования не может заменить.

Ограничение на применение программ-эмуляторов:

− эмуляция работы операционной системы сетевого устройства требует значительных вычислительных ресурсов, а в рамках одной модели должно взаимодействовать несколько устройств;

− библиотеки моделей сетевых устройств не поставляются;

− виртуальное оборудование не дает эффекта полноценной поддержки всех модулей и функций реальных устройств.

Компании-производители сетевых устройств учли опыт перевода сетевых устройств в виртуальную среду, учитывая формат представления услуг XaaS и потребность компаний арендаторов в услугах вирутальных центров обработки данных *системы моделирования сетевых сред* перешли в класс *систем эмуляции сетевых узлов и структур*.

Примеры программных продуктов этого класса представлены на рисунках 8.10-8.12.

В качестве операционных систем в этих системах эмуляции используются полноценный код, который может работать как на штатном оборудовании сетевого устройства, так и в средах виртуализации HyperV, ESXi, Proxmox.

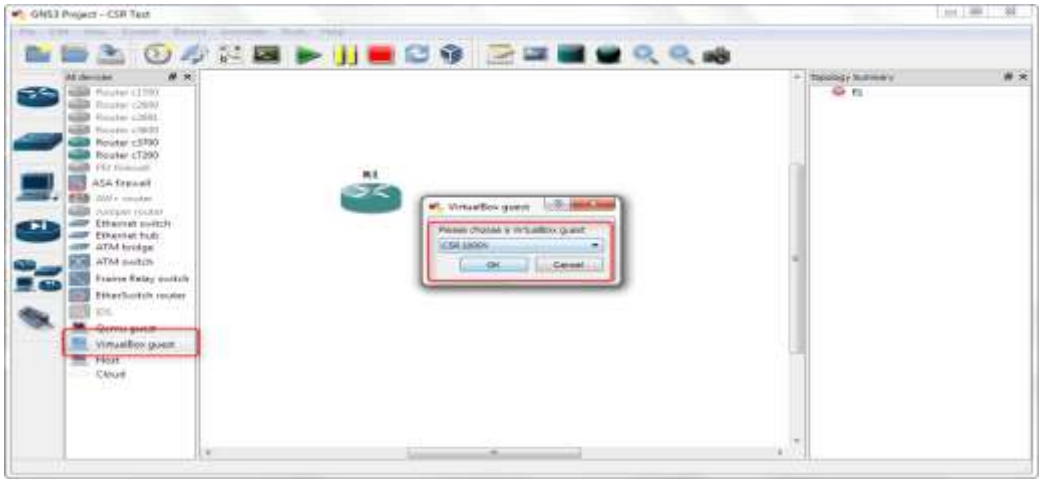


Рисунок 8.10 – Graphical Network Simulator (GNS3)

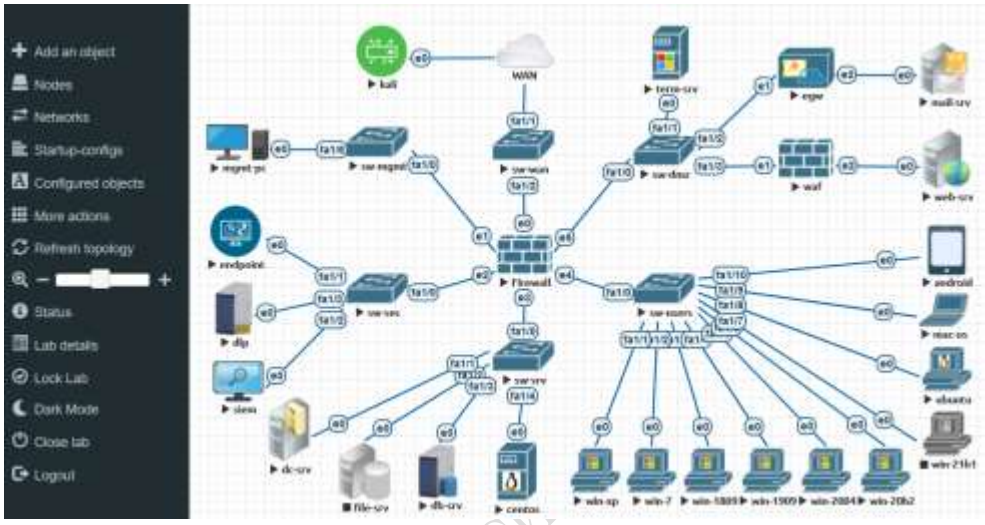


Рисунок 8.11 – Emulated Virtual Environment Next Generation (EVE-NG)

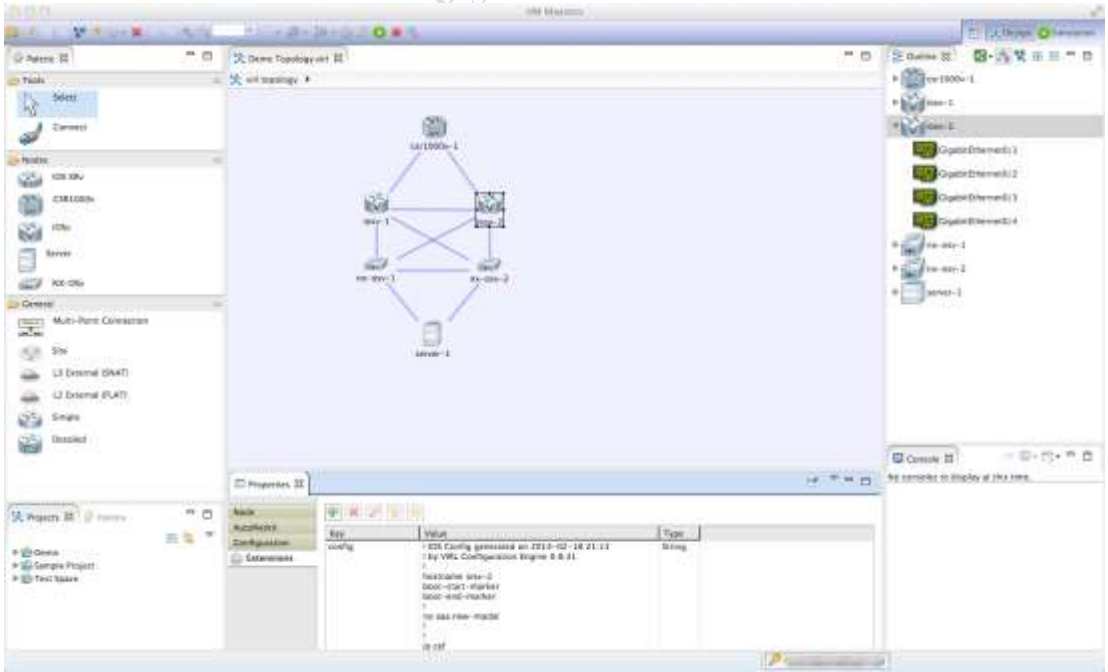


Рисунок 8.12 – Cisco Modeling Labs (CML)

3 Пример презентационного материала для проведения занятия

VTP, расширенные сети VLAN и DTP

Концепция и принципы работы VTP

- Протокол VTP помогает сетевому администратору управлять сетями VLAN на коммутаторе, который настраивается в режиме сервера VTP.
- VTP хранит конфигурации сетей VLAN в базе данных, называемой **vlan.dat**.
- Коммутатор можно настроить в одном из трех режимов VTP:
  - Сервер
  - Клиент
  - Прозрачный
- VTP включает в себя три типа объявлений:
  - Общие сведения
  - Запрос объявления
  - Подробные объявления

Компонент VTP	Определение
Домен VTP	• Состоит из одного или нескольких соединенных между собой коммутаторов. • Все коммутаторы в домене обмениваются конфигурациями VLAN с помощью объявлений VTP. • Коммутаторы из разных доменов VTP сообщениями VTP не обмениваются. • Граница домена проходит по маршрутизатору или коммутатору уровня 3.
Объявления VTP	• Каждый коммутатор в домене VTP периодически отправляет глобальные объявления с конфигурацией из каждого порта транка на зарезервированный групповой адрес. • Соседние коммутаторы получают эти объявления и при необходимости обновляют свою конфигурацию VTP и сети VLAN.
Режимы VTP	Коммутатор можно настроить в одном из трех режимов VTP: серверном, клиентском или прозрачном.
Пароль VTP	Для коммутаторов в домене VTP можно также задать пароль.

VTP, расширенные сети VLAN и DTP

Концепция и принципы работы VTP

Объявления VTP

В протоколе VTP имеется три типа объявлений:

- **Сводные объявления** – уведомляют соседние коммутаторы о доменном имени VTP и о номере версии конфигурации.
- **Запрос объявления** – направляется в ответ на сообщение сводного объявления, когда сводное объявление содержит более высокий номер версии конфигурации, чем текущее значение.
- **Объявления подмножеств** – содержат сведения о сетях VLAN, в том числе обо всех изменениях.

По умолчанию коммутаторы Cisco рассылают сводные объявления каждые пять минут.

Режимы VTP	Коммутатор можно настроить в одном из трех режимов VTP: серверном, клиентском или прозрачном.
Пароль VTP	Для коммутаторов в домене VTP можно также задать пароль.

VTP, расширенные сети VLAN и DTP

Настройка VTP

- Настройка VTP состоит из 5 шагов:
  1. Настройка сервера VTP.
  2. Настройка доменного имени и пароля VTP.
  3. Настройка клиентов VTP.
  4. Настройка сетей VLAN на сервере VTP.
  5. Проверка получения клиентами VTP новой информации о сети VLAN.

```
S2# show vlan brief

VLAN Name                    Status     Ports
---- --------------------- --------- -------------------------------
1    default                 active     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
10   SALES                   active
20   MARKETING               active
30   ACCOUNTING              active
1002 fddi-default            act/unsup
1003 token-ring-default      act/unsup
1004 fddinet-default         act/unsup
1005 trnet-default           act/unsup
S2#
```

VTP, расширенные сети VLAN и DTP

Настройка VTP

- Настройка VTP состоит из 5 шагов:
  1. Настройка сервера VTP.
  2. Настройка доменного имени и пароля VTP.
  3. Настройка клиентов VTP.
  4. Настройка сетей VLAN на сервере VTP.
  5. Проверка получения клиентами VTP новой информации о сети VLAN.

Настройка VTP на коммутаторах Cisco

Настройка VTP версии 2

Имя VTP-домена (от 1 до 32 символов):

```
sw(config)# vtp domain <domain-name>
```

Настройка пароля, который будет использоваться для аутентификации в VTP-домене (от 1 до 32 символов):

```
sw(config)# vtp password <password>
```

Настройка второй версии протокола VTP:

```
sw(config)# vtp version 2
```

Настройка режима VTP:

```
sw(config)# vtp mode <client | server | transparent>
```

VTP, расширенные сети VLAN и DTP

Расширенные сети VLAN

- Сети VLAN обычного диапазона определяются идентификатором VLAN от 1 до 1005.
- Определяются идентификатором VLAN от 1006 до 4094.
- Протокол VTP не распознаёт сети VLAN расширенного диапазона.

Создание сети VLAN

- Помимо ввода одиночного идентификатора VLAN, можно ввести ряд идентификаторов VLAN, разделенных запятыми, или диапазон идентификаторов VLAN, разделенный дефисом.

Команды коммутатора Cisco под управлением ОС IOS	
Войдите в режим глобальной настройки.	`S1# configure terminal`
Создайте сеть VLAN с допустимым номером идентификатора.	`S1 (config) # vlan` *идентификатор-VLAN*
Укажите уникальное имя для идентификации сети VLAN.	`S1 (config - vlan) # name` *имя-VLAN*
Вернитесь в привилегированный режим.	`S1 (config - vlan) # end`

VTP, расширенные сети VLAN и DTP

Расширенные сети VLAN (продолжение)

Назначение портов сетям VLAN

- Следующий шаг после создания сети VLAN — назначение портов сетям VLAN.

Команды коммутатора Cisco под управлением ОС IOS	
Войдите в режим глобальной настройки.	`S1# configure terminal`
Войдите в режим конфигурации интерфейса.	`S1 (config) # interface` *идентификатор_интерфейса*
Переведите порт в режим доступа.	`S1 (config - if) # switchport mode access`
Назначьте порт сети VLAN.	`S1 (config - if) # switchport access vlan` *идентификатор_VLAN*
Вернитесь в привилегированный режим.	`S1 (config - if) # end`

Проверка информации о сети VLAN

- Конфигурации сетей VLAN можно проверять с помощью команд Cisco IOS **show**.

Настройка расширенных сетей VLAN

- Чтобы настроить расширенную сеть VLAN на коммутаторе 2960, его необходимо установить в прозрачный режим VTP.

VTP, расширенные сети VLAN и DTP

Защищено | https://www.cisco.com/c/en/us/support/docs/switches/catalyst-2940-series-switches

and Location section for more information.

3.
Back up the existing vlan.dat file.

```
Cat6K-IOS#copy const_nvram:vlan.dat bootflash:vlan.dat
Destination filename [vlan.dat]?
976 bytes copied in 0.516 secs (1891 bytes/sec)


Cat6K-IOS#show bootflash:
-#- ED ----type---- --crc--- -seek-- nlen -length- ---------date/time--------- n
ame
1   .. image        C32839CA  2349AC   30  1788204 May 31 2006 18:15:50 +00:00 c
6msfc2-boot-mz.121-13.E17.bin
2   .. unknown      1D1450E8  234DFC    8      976 Dec 01 2008 01:43:18 +00:00 v
lan.dat

13414916 bytes available (1789436 bytes used)
```

4.
Remove the vlan.dat file from NVRAM.

```
Cat6K-IOS#delete const_nvram:vlan.dat

Delete filename [vlan.dat]?
Delete const_nvram:vlan.dat? [confirm]


Cat6K-IOS#dir const_nvram:
Directory of const_nvram:/
    1  -rw-           0                    <no date>  vlan.dat
129004 bytes total (129004 bytes free)
Cat6K-IOS#
```

5.
Reload the switch.

```
Cat6K-IOS#reload
Proceed with reload? [confirm]
```

```
00000000:  BADB100D 00000002 02044343 4E410000    :[.. .... ..CC NA..
00000010:  00000000 00000000 00000000 00000000    .... .... .... ....
00000020:  00000000 00000000 00000000 00000007    .... .... .... ....
00000030:  0A00000B 00000001 39333033 31333034    .... .... 9303 1304
00000040:  32373438 10D32D21 98ED3502 13681E2D    2748 .S-! .m5. .h.-
00000050:  B1497B40 05636973 636F0000 00000000    1I{@ .cis co.. ....
00000060:  00000000 00000000 00000000 00000000    .... .... .... ....
00000070:  00000000 00000000 00000000 00000000    .... .... .... ....
00000080:  00000000 00000000 00000000 00000000    .... .... .... ....
00000090:  00000000 00000009 02020131 047228D4    .... .... ...1 .r(T
000000A0:  07646566 61756C74 00000000 00000000    .def ault .... ....
000000B0:  00000000 00000000 00000000 00000000    .... .... .... ....
000000C0:  00000101 05DC0001 000186A1 00000000    .... .\.. ...! ....
000000D0:  00000000 00000000 00000000 08564C41    .... .... .... .VLA
000000E0:  4E303030 32000000 00000000 00000000    N000 2... .... ....
000000F0:  00000000 00000000 00000000 00000101    .... .... .... ....
00000100:  05DC0002 000186A2 00000000 00000000    .\.. ..." .... ....
00000110:  00000000 00000000 08564C41 4E303030    .... .... .VLA N000
00000120:  33000000 00000000 00000000 00000000    3... .... .... ....
00000130:  00000000 00000000 00000101 05DC0003    .... .... .... .\..
00000140:  000186A3 00000000 00000000 00000000    ...# .... .... ....
00000150:  00000000 08564C41 4E303030 34000000    .... .VLA N000 4...
```

<snip>

Начальная настройка параметров коммутатора.

Восстановление после сбоя системы

Полезные примеры:

switch: **cat flash:/config.text** – отображает содержимое текстовых файлов

switch: **copy flash:test1.text flash:test4.text** – копирование

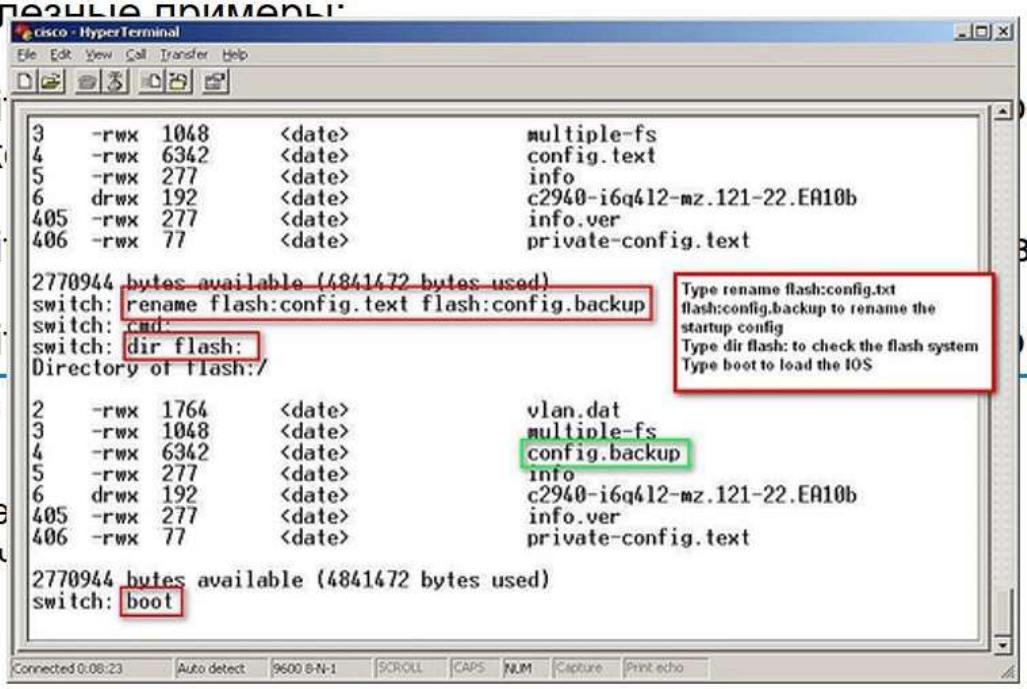
switch: **mkdir flash:Saved_Configs** – создание каталогов

3. Системный индикатор мигнет желтым, а затем загорится зеленым цветом. Отпустите кнопку Mode (Режим).

- В эмуляторе терминала на ПК появится запрос **`switch:`** от начального загрузчика.

Начальная настройка параметров коммутатора.

Восстановление после сбоя системы



Начальная настройка параметров коммутатора.

Восстановление после сбоя системы

Полезные примеры:

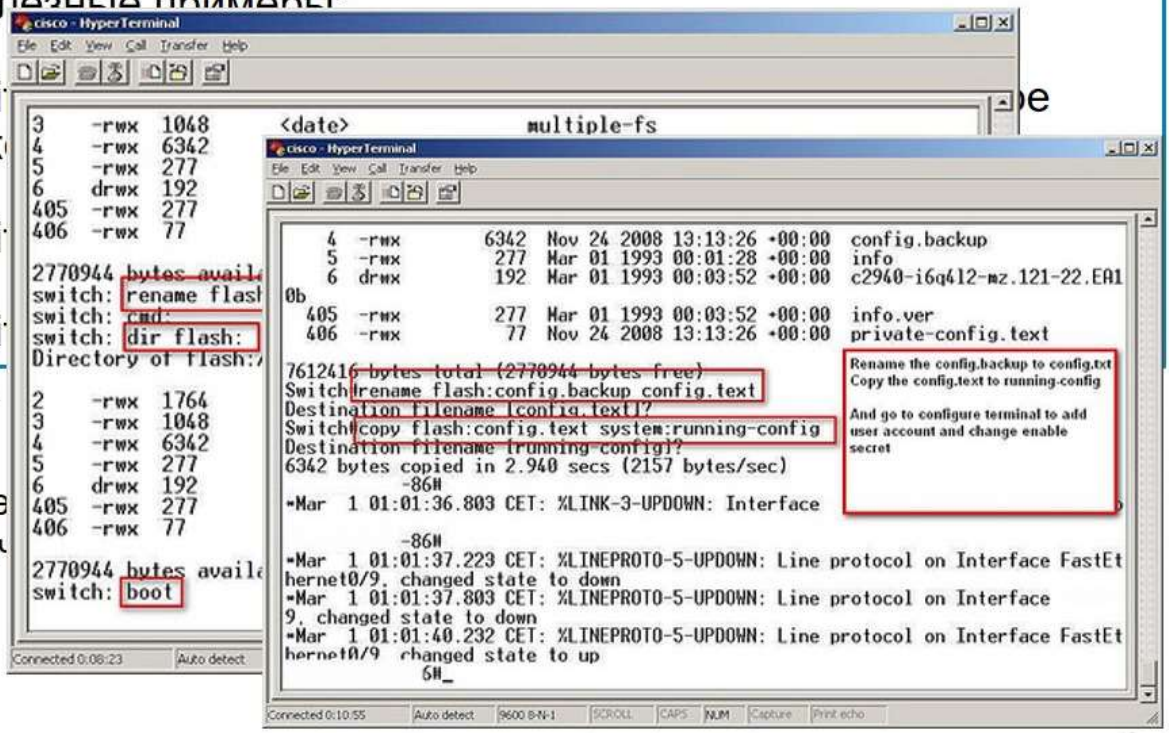
swi … е
тек…

swi…

swi…

3.

- В э…
на…



Настройка GVRP в Cisco

GVRP в Cisco можно настраивать только в COS.

Включение:

```
set gvrp enable
```

Просмотр настроек:

```
show gvrp configuration
```

Другие настройки [1].

Настройка GVRP в ProCurve

Настройки по умолчанию

Включение GVRP на коммутаторе:

```
ProCurve(config)# gvrp
```

GARP VLAN Registration Protocol (GVRP) — свободный протокол, предназначенный для создания, удаления и переименования VLANo в на сетевых устройствах и описанный в стандарте 802.1Q.

Передавать информацию о том, какой порт находится в каком VLANe, он не может.

GARP расшифровывается как Generic Attribute Registration Protocol.

Сейчас уже заменён на MVRP, Multiple VLAN Registration Protocol, свободный протокол, описанный в расширении 802.1ak к стандарту 802.1Q (802.1Q-2005).

The IEEE 802.1ak MRP provides improved resource utilization and bandwidth conservation. With the 802.1ak MRP attribute encoding scheme, MVRP sends only one protocol data unit (PDU) that includes the state of all 4094 VLANs on a port.

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface** *type number*	Configure an interface and enters interface configuration mode. The range for the *number* argument is from 1 to 253.
Step 3	switch(config-if)# **feature mvrp**	Enables MVRP on all trunk ports. If MVRP is not successfully enabled on the port, the port is put in the errdisabled state. Enter the **shutdown** and **no shutdown** commands to clear the errdisabled state. **Note** You must use the **no mrvp** command to explicitly disable MVRP on trunk ports that are connected to devices that do not support MVRP .

Registration Protocol, свободный протокол, описанный в расширении 802.1ak к стандарту 802.1Q (802.1Q-2005).

The IEEE 802.1ak MRP provides improved resource utilization and bandwidth conservation. With the 802.1ak MRP attribute encoding scheme, MVRP sends only one protocol data unit (PDU) that includes the state of all 4094 VLANs on a port.

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **[no] interface** *type number*	Configure an interface and enters interface configuration mode. The range for the *number* argument is from 1 to 253.
Step 3	switch(config-if)# **mvrp registration** {**normal** | **fixed** | **forbidden**}	(Optional) Configure an interface and enters interface configuration mode. Sets the registrars in a Multiple Registration Protocol (MRP) Attribute Declaration (MAD) instance associated with an interface. • Use the **normal** keyword to specify that the registrar respond normally to incoming MVRP messages. Normal is the default registrar state. • Use the **fixed** keyword to specify that the registrar ignore all incoming MVRP messages (remain in the IN state). VLANs are not pruned. • Use the **forbidden** keyword to specify that the registrar ignore all incoming MVRP messages (remain in the EMPTY (MT) state) and prune VLANs. **Note** You can use the **no mvrp registration** command to return the registrar to the default value (normal).
Step 4	switch(config-if)# **mvrp timer** {{**join** | **leave** | **join-leave**} *timer-value* | **periodic**}	(Optional) Sets the period timers that are used in MVRP on a given interface. • Use the **join** keyword to specify the time interval between two transmit opportunities that are applied to the Applicant State Machine (ASMs). The range is from 20 to 1,000,000 centiseconds. The default value is 20. • Use the **leave** keyword to specify the duration time before a registrar is moved to EMPTY (MT) state from leave-all (LV) state. The range is from 60 to 1,000,000 centiseconds. The default is 60. • Use the **join-leave** keyword to specify the time it takes for a LeaveAll timer to expire . The range is from 10,000 to 1,000,000 centiseconds. The default is 10,000. • Use the **periodic** keyword to set the timer value to a fixed value of 100 centiseconds. **Note** You can use the **no mvrp timer** command to remove the configured timer values.

Registration Protocol, свободный протокол, описанный в расширении 802.1ak к стандарту 802.1Q (802.1Q-2005).

VTP, расширенные сети VLAN и DTP

Динамический протокол транкинга (DTP)

- DTP
  - DTP управляет транковым согласованием только в случае, если порт соседнего коммутатора настроен в режиме транка, который поддерживает DTP.
  - Отключите протокол DTP на интерфейсах коммутатора Cisco, который подключен к устройствам, не поддерживающим DTP.
  - Чтобы включить транкинг от коммутатора Cisco к устройству, не поддерживающему DTP, используйте команды режима настройки интерфейса **switchport mode trunk** и **switchport nonegotiate**.
- Существуют 5 команд для поддержки различных режимов транкинга:
  - **switchport mode access**
  - **switchport mode dynamic auto**
  - **switchport mode dynamic desirable**
  - **switchport mode trunk**
  - **switchport nonegotiate**

	Dynamic Auto	Dynamic Desirable	Trunk	Доступ
Dynamic Auto	Access	Trunk	Trunk	Доступ
Dynamic Desirable	Trunk	Trunk	Trunk	Доступ
Trunk	Trunk	Trunk	Trunk	Ограниченные возможности подключения
Доступ	Доступ	Доступ	Ограниченные возможности подключения	Доступ

Поиск и устранение неполадок в нескольких сетях VLAN

Проблемы конфигурации между сетями VLAN

- Чтобы удалить сеть VLAN, используйте команду режима глобальной настройки **no vlan** *vlan-id*.
- Если для коммутационного порта не настроена верная сеть VLAN, настроенные в этой сети устройства не могут подключаться к интерфейсу маршрутизатора.
- В настройках коммутатора могут присутствовать проблемы, поэтому рекомендуется использовать специальные команды для проверки конфигурации и определения неполадок.

```
S1# show interfaces FastEthernet 0/4 switchport
Name: Fa0/4
Switchport: Enabled
Administrative Mode: static access
Operational Mode: up
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
<output omitted>
S1#
```

Проблемы конфигурации между сетями VLAN (продолжение)

- Неполадки в работе интерфейса
  - Одной из самых распространённых ошибок при включении маршрутизации между VLAN на маршрутизаторе является подключение физического интерфейса маршрутизатора к неверному порту коммутатора.
- Проверка настроек маршрутизатора
  - Основная проблема с методом router-on-a-stick заключается в неверном назначении подинтерфейсу идентификатора VLAN.
  - Для устранения такого типа неполадок могут быть полезны команды **show interfaces** и **show running-config**.

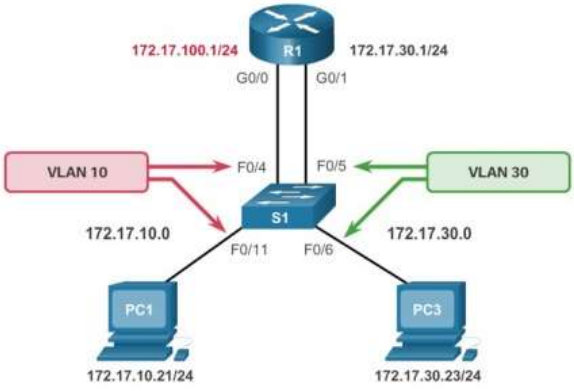
```
R1# show interfaces

<output omitted>

GigabitEthernet0/0.10 is up,line protocol is down (disabled)
 Encapsulation 802.1Q Virtual Lan,Vlan ID 100
 ARP type :ARPA,ARP Timeout 04:00:00,
 Last clearing of "show interface" counters never
```


Проблемы IP-адресации

- IP-адреса и маски подсети
  - Для работы маршрутизации между VLAN маршрутизатор должен быть подключён ко всем VLAN через физические интерфейсы или подинтерфейсы.

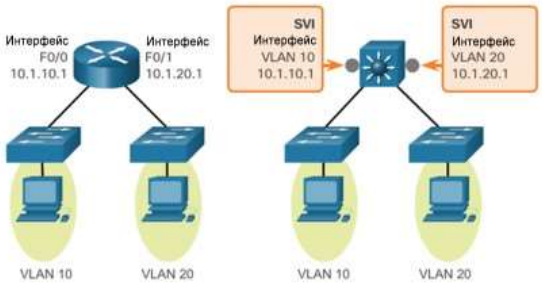


  - Каждому интерфейсу или подинтерфейсу необходимо назначить IP-адрес, соответствующий подсети, к которой он подключён.
  - Используйте команды **show running-config** и **show ip interface** для проверки IP-адреса и масок подсетей.

Коммутация 3-го уровня

Работа и настройка коммутации 3-го уровня

- Коммутация 3-го уровня
  - В современных корпоративных сетях используются многоуровневые коммутаторы для достижения высоких скоростей обработки пакетов с использованием аппаратной коммутации.
  - Многоуровневые коммутаторы Catalyst поддерживают следующие типы интерфейсов 3-го уровня:
    - Маршрутизируемый порт
    - Виртуальный интерфейс коммутатора (SVI)

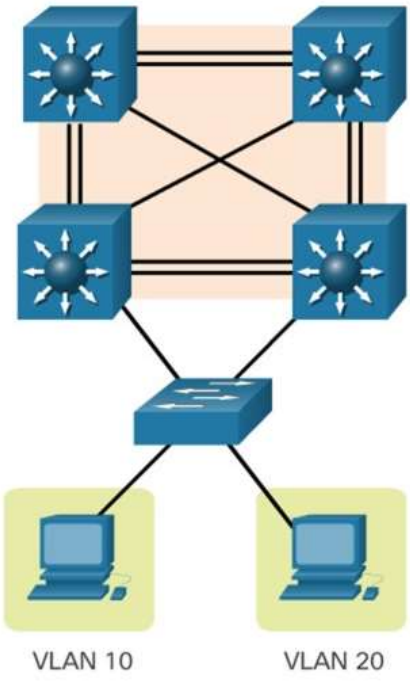


- Маршрутизация между сетями VLAN и интерфейсы SVI
  - Маршрутизацию можно перенести на основной уровень и уровень распределения (а иногда даже на уровень доступа) без ущерба производительности сети.
  - Интерфейс SVI можно создать для любой сети VLAN, существующей на коммутаторе.
  - Интерфейсы SVI создаются при первом входе в режим интерфейсной настройки сети VLAN для определенного VLAN SVI.

Коммутация 3-го уровня

Работа и настройка коммутации 3-го уровня (продолжение)

- Маршрутизация между VLAN через маршрутизируемые порты
  - Маршрутизируемый порт — это физический корт, который действует аналогично интерфейсу на маршрутизаторе.
  - Маршрутизируемый порт не связан с конкретной сетью VLAN.
  - Маршрутизируемые порты на коммутаторе Cisco IOS не поддерживают подчиненные интерфейсы.
  - Маршрутизируемые порты используются для каналов «точка-точка».
  - Для настройки маршрутизируемых портов следует использовать режим интерфейсной настройки **no switchport** на соответствующих портах.



4 ВОПРОСЫ ДЛЯ САМОКОНТРОЛЯ

1 Дайте определение информационной сети и сети обработки данных.
2 Приведите примеры классификаций компьютерных сетей.
3 Дайте определение локальной вычислительной сети.
4 Приведите пример примерного жизненного цикла локальной сети.
5 Дайте определение городской сети (Site/Metropolitan Area Net-work – SAN/MAN).
6 Дайте определение глобальной вычислительной сети (Glob-al/World Area Network - GAN/WAN).
7 Проведите сравнение свойств глобальных вычислительных сетей с локальными вычислительными сетями.
8 Что такое частные сети (Private Network – PN)?
9 Приведите примеры классификации частных сетей.
10 Что такое корпоративная сеть (Enterprise Wide Networks – EWN)?
11 Какими характеристиками обладает корпоративная сеть?
12 Какова главная задача корпоративной сети?
13 Как и на основе какого подхода строятся типовые структуры корпоративных сетей?
14 Сформулируйте определение домашней сети (Home Network – HN).
15 Какие функции выполняет домашняя сеть с точки зрения провайдера и пользователя?
16 Какими факторами обусловлен быстрый рост домашних сетей в последнее время?
17 Зачем нужны модели представления сетевых объектов и устройств?
18 Опишите теоретические модели, оказавшие влияние на сетевые технологии.
19 Какое место в описании компьютерных сетей занимает проект IEEE 802.x?
20 Каковы функции физического уровня модели OSI?
21 Каковы функции канального уровня модели OSI?
22 Каковы функции сетевого уровня модели OSI?
23 Каковы функции транспортного уровня модели OSI?
24 Каковы функции сеансового уровня модели OSI?
25 Каковы функции представительского уровня модели OSI?
26 Каковы функции прикладного уровня модели OSI?
27 Какие альтернативные модели описания компьютерных сетей вы знаете?
28 Каков порядок разработки сетевых стандартов и какие организации в этом участвуют?
29 Как реализуется сетевая архитектура в структуре современных операционных систем?
30 Что такое MAC и каковы его функции?
31 Что такое LLC и каковы его функции?
32 Дайте определение понятия протокола.
33 Какие типы протоколов существуют?
34 Приведите соответствие типов протоколов модели OSI.
35 Какие устройства реализуют протоколы канального уровня?
36 Какие стеки протоколов вы знаете?
37 Опишите схему структуры «клиент – сервер».
38 Какие протоколы файлового обмена вы знаете?
39 Какие почтовые протоколы вы знаете?
40 Назовите протоколы удаленного контроля и управления.
41 Определите понятие топология сети.
42 В чем разница между физической структурой сети и логической структурой сети?
43 Какие виды топологий применяют при проектировании компьютерных сетей?
44 Каковы свойства сетей, построенных по топологии «шина»?
45 Каковы свойства сетей, построенных по топологии «кольцо»?
46 Каковы свойства сетей, построенных по топологии «звезда»?
47 Каковы свойства сетей, построенных по топологии «ячейка»?
48 Каковы свойства сетей с комбинированными топологиями?
49 Изобразите схематично некоторые примеры смешанных топологий.

50 Какие альтернативные сетевые структуры вы можете назвать и описать?
51 Как вычислить среднее число шагов между узлами в топологии сети?
52 Что такое иерархическая топология?
53 Что такое сетеобразующая топология?
54 Какие кабельные системы применяются в различных сетевых топологиях?
55 Можно ли сравнивать надежностные характеристики сетей, построенных по различным топологиям?
56 Дайте определение среды передачи данных.
57 В каких режимах может работать среда передачи данных?
58 Каким образом можно соединить компьютеры в сеть?
59 Какие характеристики имеет коаксиальный кабель?
60 Какие существуют типы «витых пар»?
61 Назовите основные категории «витой пары» и их характеристики.
62 Объясните физический смысл волновода.
63 Опишите физические явления, протекающие в оптоволоконном кабеле.
64 Дайте понятие мультиплексирования каналов.
65 Опишите возможные коммуникации структурированных кабельных систем.
66 Каким образом осуществляется декорирование кабельных систем?
67 Приведите основные виды беспроводных сетей.
68 Раскройте понятие «затухание сигнала».
69 Как происходит одновременная передача информационных сигналов во многомодовом оптоволокне?
70 Как организуется очередность приема и передачи информации в сетевой среде?
71 На каком уровне модели OSI действуют методы доступа к среде?
72 Какие методы доступа к среде чаще всего применяются в компьютерных сетях?
73 Как можно ограничить доступ к среде передачи на физическом уровне модели OSI?
74 Каковы свойства сети, построенной с использованием маркерного доступа к сети?
75 Каковы свойства сети, построенной с использованием метода доступа к сети CSMA/CD?
76 Каковы свойства сети, построенной с использованием метода доступа к сети CSMA/CA?
77 Каковы свойства сети, построенной с использованием метода доступа к сети по приоритету запроса?
78 Какие ошибки передачи данных обусловлены выбором метода доступа к среде?
79 Что такое коллизия?
80 Что происходит в сети после возникновения коллизии?
81 Какие методы борьбы с коллизиями применяют в современных сетях?
82 Как объединяются сети с различным методом доступа к среде?
83 Какие виды активного оборудования сетей вы знаете? Перечислите их.
84 Что относится к дополнительным и комбинированным сетевым устройствам?
85 Проведите соответствие функций коммуникационного оборудования уровням модели OSI.
86 Что скрывается за понятием односегментная шина?
87 Дайте определение сетевого адаптера или сетевой карты (netcard).
88 Какими параметрами обладают современные сетевые адаптеры?
89 Приведите классификацию сетевых адаптеров.
90 Как осуществляется настройка сетевого адаптера?
91 Опишите функции и принцип работы сетевого устройства «повторитель» (repeater).
92 Опишите функции и принцип работы сетевого устройства «коммутатор» (switch).
93 Опишите функции и принцип работы сетевого устройства «мост» (bridge).
94 Опишите функции и принцип работы сетевого устройства «трансивер».
95 Опишите функции и принцип работы сетевого устройства «маршрутизатор» (router).
96 Опишите функции и принцип работы сетевого устройства «шлюз».
97 Что такое сетевые технологии и зачем они применяются?
98 Приведите примеры беспроводных сетевых технологий.
99 Каковы современные стандарты скоростей сетевого обмена?
100 Какие перспективы роста скоростей передачи данных?
101 Как оценить эффективность использования сетевой технологией среды передачи данных?

102Возможно ли увеличение скоростных характеристик сети без изменения структуры кабельной системы?
103Какие способы существуют для объединения сетевых технологий в рамках одной сети?
104Какие ошибки могут возникать при передаче данных в различных сетевых технологиях?
105Какие способы для повышения надежности передачи данных применяются в различных сетевых технологиях?
106Зачем нужна адресация в компьютерных сетях?
107Какие примеры подходов к решению задачи распределения адресов вы знаете?
108Что такое размер адресного пространства?
109Каковы свойства системы адресации на уровне MAC?
110Каковы свойства системы адресации в IP-сетях?
111Что такое классы адресации?
112Что такое бесклассовая адресация?
113Какие бывают специальные адреса в IP-сетях?
114В чем суть процесса «агрегирование адреса»?
115Какие типы адресов применяются в системе адресации IP v.6?
116Каковы перспективы применения и развития современных систем адресации?
117Какие ошибки в сети возникают по причине нарушений требований системы адресации?
118Как организовать широковещательную рассылку в различных системах адресации?
119Как производится управление компонентами сети?
120Как организовано управление в одноранговых сетях?
121Как организовано управление в сетях на основе сервера?
122Как объясняется термин – гетерогенность сети?
123Как организовать управление в гетерогенных сетях?
124Как работает сеть по технологии «рабочая группа»?
125Как работает сеть по технологии «дерево доменов»?
126Как работает сеть по технологии «Active Directory»?
127Зачем применяются методы разграничения доступа?
128Какие виды разграничения доступа вы знаете?
129Как организована многопользовательская работа в одноранговых сетях?
130Как организована многопользовательская работа в сетях на основе сервера?
131Каковы требования при формировании индивидуальных паролей пользователей?
132Опишите назначение и методы работы брандмауэров.
133Назначение командного режима и технология его применения.
134Каковы методы организации сетевой печати?
135Какие средства защиты информации вы знаете?
136Какие четыре основные категории атак вы знаете?
137Назначение резервного копирования данных.
138Что представляет собой компьютерная программа?
139На какие виды можно разделить программное обеспечение?
140Для чего применяются операционные оболочки?
141Что такое «тонкий клиент»?
142Опишите место Web-OS в современном вычислительном процессе.
143Как работает серверная операционная система?
144Приведите примеры операционных систем для сетевых клиентов.
145Перечислите функции сервера в сетевой среде.
146Для чего предназначены браузеры?
147Как организован доступ к информации в Интернет и Интранет?
148Дайте определения следующим понятиям: Web-сервер, база данных, поисковая система.
149Для чего применяются базы данных в сетевых средах?
150Как найти нужные данные в сети?
151Что представляют собой системы обмена сообщениями?
152Назовите наиболее популярные технологии обмена сообщениями и их свойства.

5 ЗАДАНИЯ К ЛАБОРАТОРНЫМ РАБОТАМ

Лабораторная работа №1 Командный режим управления сетевыми ресурсами
Задание: Документация и демонстрация работы с сетевыми ресурсами и устройствами в командном режиме.

Лабораторная работа №2 Управление сетевым оборудованием в режиме CLI в среде Packet Tracer
Задание: В предложенной преподавателем схеме с помощью команд определить:
- тип подключенного устройства
- модель подключенного устройства
- число активных/пассивных портов
- вывести на экран конфигурационный файл

Лабораторная работа №3 Динамические протоколы маршрутизации в сетях IPv6
Задание: Настроенная модель PT для комбинации роутеров из 12 устройств.

Лабораторная работа №4 Контроль параметров беспроводных соединений
Задание: Практическая демонстрация работы с устройствами. Оценка максимального и текущего состояния канала связи. Обоснование снижения производительности.

Лабораторная работа №5 Управление реальным сетевым оборудованием в режиме CLI
Задание: Под управлением преподавателя осуществить ввод первичных настроек сетевого устройства. Сброс их на начальный уровень. Установку и сброс сетевого пароля.

Лабораторная работа №6 Разработка структурного проекта ЛВС
Задание: Формулировка задания на проведение проектных работ. Схема (кампуса) помещений объекта. Структурные подразделения. Структура связей. Подробный перечень пользовательского и управляющего ПО, участвующего в сетевом обмене. Функциональная схема взаимодействия информационных потоков внутри сети.

Лабораторная работа №7 Разработка схемы размещения оборудования внутри помещений и кабельной схемы проектируемой сети
Задание: Оптимальная схема организации информационной сети. Описание способа разрешения потенциально проблемных точек с помощью возможностей современного сетевого оборудования. Схема кабельной системы с промерами длины и указанием расстояния от кабеля до ближайших источников электромагнитных помех.

Лабораторная работа №8 Планирование структуры адресов и построение модели сетевого взаимодействия в среде Packet Tracer
Задание: Функциональная схема сети в формате .pkt. Таблица адресов. Реализация DHCP-сервиса и протоколов маршрутизации.

Лабораторная работа №9 Выбор и оценка активного и пассивного сетевого оборудования для реализации проекта ЛВС
Задание: Обоснование выбора сетевого оборудования. Составление комплексной оценки (сметной стоимости) оборудования проекта.

Лабораторная работа №10 Оценка соответствия разработанного проекта санитарным нормам и техники безопасности

Задание: Перечень действующих норм (с указанием цитируемых законодательных норм). Доработанная схема размещения оборудования внутри помещений, соответствующая требованиям техники безопасности и охраны труда с письменным обоснованием

Лабораторная работа №11 Построение бесшовного беспроводного сегмента сети

Задание: Построение схемы беспроводного покрытия сети. Выбор оборудования. Построение схемы обслуживания абонентов.

Лабораторная работа №12 Выбор и оценка системного программного обеспечения для реализации проекта ЛВС

Задание: Обоснование выбора компонентов программного обеспечения. Составление комплексной оценки (сметной стоимости) ПО проекта.

Лабораторная работа №13 Поиск неполадок в моделях сетевых архитектур

Задание: Решение задачи в формате .pka

Лабораторная работа №14 Восстановление кабельной структуры сегмента сети 802.3 Ethernet.

Задание: Работа по восстановлению комплектующих кабельной сети

6 ТЕСТОВЫЕ ЗАДАНИЯ (примеры)

Определите отличия между устройствами ввода/вывода и модулем памяти.

Выберите по крайней мере один ответ:

- ☐ модуль памяти имеет в адресном пространстве системы много адресов (до нескольких десятков миллионов), а устройство ввода/вывода обычно имеет немного адресов (обычно до десяти), а иногда и всего один адрес
- ☐ модули памяти системы обмениваются информацией только с магистралью и процессором, а устройства ввода/вывода взаимодействуют еще и с внешними устройствами, цифровыми или аналоговыми.
- ☐ модули памяти более разнообразны, чем устройства ввода/вывода
- ☐ структура модуля памяти содержит схему селектора адреса, схему управления для обработки стробов обмена и буферы данных, чего нет в структуре устройств ввода/вывода
- ☐ устройства ввода/вывода обмениваются информацией с магистралью по другим принципам (отличные от принципов обмена информации памяти)

Дополните определение нужным словом: ... - это теоретическое описание принципов работы набора сетевых протоколов, взаимодействующие друг с другом.

Выберите один ответ.

- ○ Сетевая модель
- ○ Структурная модель
- ○ Двухранговая модель
- ○ Одноранговая модель

Во время выполнения программы обработки прерывания может поступить новый запрос на прерывание. Как он будет обрабатываться?

Выберите один ответ.

- ○ прерывания будут обрабатываться по очереди (быстрее обработается то прерывание, запрос на которое поступил раньше)
- ○ основной программой будет считаться прерванная программа обработки предыдущего прерывания
- ○ обработка будет осуществляться параллельно с предыдущим прерыванием

Какой тип принтера использует мелкодисперстный порошок и имеет нагревательный элемент на выходе?

Выберите один ответ.

- ○ Термопринтер
- ○ Фотопринтер
- ○ Струйный
- ○ Лазерный

Укажите причину, по которой стандарт IEEE 802.11n позволяет организовать более высокую скорость передачи данных чем 802.11g?

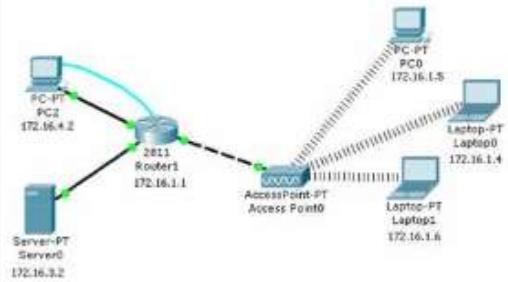
Выберите один ответ.

- ○ сетевые адаптеры и точки доступа используют более одной антенны
- ○ используется другая частота для передачи данных
- ○ используется режим с полосой частот шириной 40 МГц и технология MIMO

Зачем публиковать в информационном пространстве компании список часто задаваемых вопросов FAQ?

Выберите один ответ.

- ○ чтобы сократить число запросов к службе поддержки
- ○ чтобы службе поддержке было где посмотреть решение проблемы
- ○ чтобы сэкономить время, затрачиваемое пользователем на техническое обслуживание



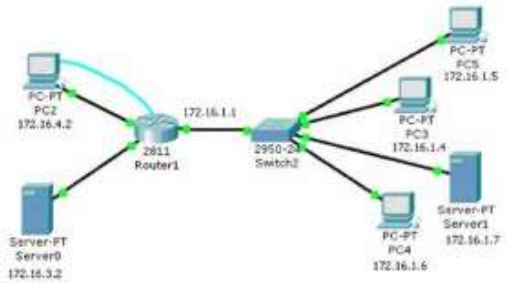
Количество доменов коллизии в сети?

Ответ:

Зачем маркировать кабельные соединения и настенные розетки?

Выберите один ответ.

- маркировка кабельных систем одно из требований стандарта Ethernet
- маркировка кабельных систем позволяет определить пользователю свое место в сети
- маркировка кабельных систем сокращает время, необходимое на проведение регламентных работ по обслуживанию сетей



Способ подключения в сеть клиентских станций.

Выберите один ответ.

- Оптоволокно
- Wi-Fi
- Serial cable
- UTP
- Коаксиальный

10101010 10001010 01010101 00001010

Переведите адрес из двоичной формы представления в десятичную форму записи - X.X.X.X.

Ответ:

Дополните определение нужным словом: сеть - это ... независимых компьютеров, связанных друг с другом с целью совместного использования.

Выберите один ответ.

- Обьединение
- Структура
- Система

Что из нижеперечисленного является устройством вывода?

Выберите один ответ.

- Мышь
- Монитор
- Трекбол
- Клавиатура

Какая файловая система применяется на гибких магнитных дисках?

Выберите один ответ.

- NTFS
- FAT32
- FAT12
- FAT16

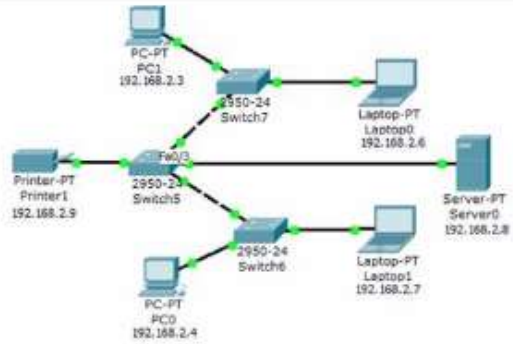
Зачем маркировать кабельные соединения и настенные розетки?

Выберите один ответ.

- маркировка кабельных систем сокращает время, необходимое на проведение регламентных работ по обслуживанию сетей
- маркировка кабельных систем одно из требований стандарта Ethernet
- маркировка кабельных систем позволяет определить пользователю свое место в сети

Выберите один ответ.

- BNC
- RJ-45
- ST
- Serial
- RJ-11
- 110 тип



Укажите тип кабельного соединения между узлами switch5 и switch6.

Выберите один ответ.

- Patch-cord
- Cross-over
- Roll-over

Метод IP-адресации, позволяющий гибко управлять пространством IP-адресов.

Выберите один ответ.

- Классовая адресация
- Бесклассовая адресация
- Особые IP-адреса
- Локальные адреса

Посмотрите на изображение. Укажите тип соединительного разъема.

Выберите один ответ.

- ST
- 110 тип
- Serial
- BNC
- RJ-11
- RJ-45

Учреждение образования
«Гомельский государственный университет имени Франциска Скорины»

УТВЕРЖДАЮ
Ректор
ГГУ имени Ф. Скорины

_____ С.А. Хахомов
_____
(дата утверждения)
Регистрационный № УД-_____/ уч.

Модуль «Компьютерные сети»:
АППАРАТНО-ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ СЕТЕЙ

Учебная программа учреждения высшего образования по учебной дисциплине для специальности

1-53 01 02 Автоматизированные системы обработки информации

2022 г.

Учебная программа составлена на основе образовательного стандарта ОСВО 1-53 01 02-2021 г. и учебного плана ГГУ имени Ф.Скорины регистрационный № I 53-1-21/УП, дата утверждения 31.05.2021.

СОСТАВИТЕЛЬ:
А.В.Воруев, доцент кафедры АСОИ

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой автоматизированных систем обработки информации
(протокол № 9 от 19.04.2022)

Научно-методическим советом Учреждения образования «ГГУ имени Ф.Скорины»
(протокол № 4 от 17.05.2022)

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Изучение дисциплины компонента учреждения высшего образования «Аппаратно-программное обеспечение сетей» модуля «Компьютерные сети» предусмотрено учебным планом подготовки специалистов специальности 1-53 01 02 – «Автоматизированные системы обработки информации».

Актуальность изучения дисциплины обусловлена высокой скоростью обновления технологической линейки электронных вычислительных систем и машин, а также смежных систем организации вычислительного процесса.

Целью дисциплины является ознакомление студентов с методами распределенного хранения и распределенной обработки информации, способам администрирования доступа к информации и основным методам кодирования информации, используемых в современных локальных и глобальных вычислительных сетях.

Задачами дисциплины «Аппаратно-программное обеспечение сетей» модуля «Компьютерные сети» являются:

- усвоение принципов проектирования и обслуживания современных сетей;
- усвоение принципов работы современного сетевого оборудования;
- овладение навыками построения сбалансированных сетевых структур, проведения анализа существующих сетей, обнаружения и исправления накопившихся нарушений предъявляемых требований;
- получение практических навыков по управлению распространенными типами сетевых устройств;
- формирование умений и навыков работы в современных сетевых средах.

В результате изучения дисциплины обучаемый должен:

знать:

– основные понятия, методы доступа и стандарты в области сетевых технологий;

– принципы построения современных компьютерных сетей;

– аппаратные средства вычислительных систем и сетей;

– программные средства вычислительных систем и сетей;

– функции сетевых операционных систем;

– базовые спецификации и параметры компьютерных сетей;

– основы сетевой безопасности;

– принципы обеспечения сетевой безопасности;

уметь:

– осваивать и внедрять современные сетевые технологии;

– использовать функции операционных систем по установке серверов и клиентов, созданию рабочих групп и доменов, управлению правами доступа;

– конфигурировать сети, инсталлировать и настраивать сетевое программное обеспечение;

– осуществлять администрирование компьютерной сети;

– обеспечивать защиту сети.

владеть:

– навыками по установке серверов и клиентов;

– навыками администрирования локальных сетей;

– навыками поиска неисправностей сетевого оборудования.

– методами и средствами машинного обучения;

После изучения дисциплины студент должен обладать следующими видами компетенций:

СК-17 Строить и конфигурировать информационные сети.

Дисциплина компонента учреждения высшего образования «Аппаратно-программное обеспечение сетей» изучается студентами 2 курса дневной, заочной и дистанционной форм обучения специальности 1-53 01 02 - «Автоматизированные системы обработки информации».

Дневная форма обучения: всего часов по плану – 240 (6 зач. ед.); аудиторное количество часов – 124, из них: лекции – 64, лабораторные занятия – 60.

Форма отчётности – экзамены в 3,4 семестре.

Заочная форма обучения: всего часов по плану – 240 (6 зач. ед.), аудиторное количество часов – 30, из них: лекции – 16, лабораторные занятия – 14.

Форма отчётности – контрольные работы и экзамены в 4,5 семестрах.

Заочная сокращенная дистанционная форма обучения: всего часов по плану – 240 (6 зач. ед.), аудиторное количество часов – 20, из них: лекции – 10, лабораторные занятия – 10.

Форма отчётности – контрольные работы и экзамены в 4,5 семестрах.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Раздел 1 Организация вычислительного процесса в сетевой среде

Тема 1.1 Концепция цифровой сети

Информационные сети включали системы для передачи сигналов, сообщений, данных и других видов информации. Распределенные и унифицированные вычислительные системы относились к сетям обработки данных. Но, поскольку распределенная обработка требует использования механизмов обмена информацией, эта грань постепенно стирается, и на данный момент все компьютерные сети являются как информационными, так и вычислительными. Поэтому часто используется более общий термин "цифровые сети". Цифровые сети можно рассматривать с разных точек зрения: для запущенной программы сеть представляет собой сложную систему маршрутов для передачи данных и ресурсов для их обработки; для пользователя компьютерная сеть - это инструмент для доступа к сетевым ресурсам; для менеджера сеть - это средство управления производственными процессами; для сетевого дизайнера это набор стандартов и требований, которые необходимо соблюдать во время реализации проекта.

Тема 1.2 Виртуализация сетевых узлов и сегментов сети

Виртуализация сетевых узлов использует преимущества незанятых ресурсов и объединяет количество необходимых серверов и сетевых устройств. Это также позволяет нескольким операционным системам существовать на одной аппаратной платформе. Кроме того, становится возможным сбалансировать нагрузку. Нет никакой концептуальной разницы между запуском сетевого узла и запуском виртуальной машины. Сетевые подключения могут быть виртуализированы на уровне программных связей между операционными средами на уровне гипервизора.

Многоуровневая веб-архитектура, тонкий клиент и ультратонкий клиент являются примерами модели централизованного обслуживания.

Ультратонкий клиент (терминал) может отображать только растровое изображение и передавать информацию с устройств ввода на сервер. Тонкие клиенты - это устройства, способные поддерживать оконную систему (например, X-Window). На следующем уровне расположены Java-станции, которые сочетают в себе интерфейс веб-браузера с возможностью загрузки и запуска Java-апплетов и автономных Java-приложений. Перераспределение клиентских функций в любой из рассмотренных архитектур увеличивает сетевой трафик и нагрузку на ресурсы сервера. Решение этой проблемы было найдено в использовании специализированных устройств для типичных сетевых сервисов и подходе этих устройств к клиентам.

Тема 1.3 Программно определяемая сетевая архитектура

Предполагается, что при решении практических задач количество IoT-устройств и объем их трафика превышают ресурсные возможности каналов

связи на пути: сетевой периметр - облачный сервер. При этом количество этих устройств динамически изменяется как в большую, так и в меньшую сторону в зависимости от потребностей решаемой задачи. Следовательно, настройки устройств сетевого подключения должны динамически изменяться, что позволяет объединять подмножества IoT-устройств в единый сегмент сети или удалять их из этого сегмента. Чтобы сеть обладала этими свойствами, используется программно-определяемая сетевая архитектура.

Туманные вычисления являются частью инфраструктуры распределенных вычислений для модели сети IoT, которая определяет изолированный сегмент, расположенный ближе к периметру сети относительно устройства IoT. Это позволяет устройствам получать доступ к данным, запускать приложения и принимать немедленные решения. Данные не нужно отправлять через сетевые подключения в режиме онлайн. Предусмотрена возможность их промежуточного накопления и первичной переработки. Устройства IoT способны работать при потере сетевых соединений, что повышает отказоустойчивость. Конфиденциальные данные хранятся в границах, где они необходимы, что повышает уровень безопасности.

Тема 1.4 Определение границ облачной среды

Иерархическая архитектура службы приложений позволяет комбинировать аппаратные решения, программные интерфейсы обслуживания клиентов (приложения) и программно реализованные (виртуализированные) сетевые службы для повышения эффективности обслуживания конечного оборудования. Архитектура, состит из контроллера туманности (Плоскость управления, уровень 1) и многоуровневых узлов тумана (Плоскость управления, уровни 2, 3 и 4). Уровни работают вместе, чтобы обеспечить миграцию услуг для перераспределения трафика с поддержкой QoE. В такой архитектуре мы рассматриваем полностью подключенный и полностью туманный сценарий, где узлы тумана иерархически организованы для предоставления видеоуслуг конечным пользователям.

Раздел 2 Модели описания сетевого взаимодействия

Тема 2.1 Классификация сетевых архитектур

Компьютерные сети принято классифицировать по типам передачи данных (широковещательные, сети с передачей от узла к узлу) и по размеру (локальные, муниципальные и глобальные сети). Широковещательные сети обладают единым каналом связи, совместно используемым всеми машинами сети. Короткие сообщения, называемые в некоторых случаях пакетами, которые посылаются одной машиной, получают все машины. Поле адреса в пакете указывает, кому направляется сообщение. При получении пакета машина проверяет его адресное поле. Если пакет адресован этой машине, она его обрабатывает. Пакеты, адресованные другим машинам, игнорируются.

Сети с передачей от узла к узлу, напротив, состоят из большого количества соединенных пар машин. В сети подобного типа пакету, чтобы добраться до пункта назначения, необходимо пройти через ряд промежуточных машин. Часто при этом существует несколько возможных путей от источника до получателя, поэтому алгоритмы вычисления таких путей играют очень важную роль в сетях с передачей от узла к узлу.

Тема 2.2 Теоретические модели ISO/OSI и TCP/IP

Сетевая модель OSI (The Open Systems Interconnection model) – сетевая модель стека (магазина) сетевых протоколов OSI/ISO. Посредством данной модели различные сетевые устройства могут взаимодействовать друг с другом. Модель определяет различные уровни взаимодействия систем. Каждый уровень выполняет определённые функции при таком взаимодействии. Модель OSI была разработана в конце 1970-х годов для поддержания разнообразных методов компьютерных сетей, которые в это время конкурировали за применение в крупных национальных сетевых взаимодействиях во Франции, Великобритании и США. В 1980-х годах она стала рабочим продуктом группы взаимодействия открытых систем Международной организации по стандартизации (ISO). Модель не смогла дать полное описание сети и не получила поддержку архитекторов на заре Интернета, который впоследствии нашел отражение в менее предписывающем TCP/IP, в основном под руководством Инженерного совета Интернета (IETF).

TCP/IP – сетевая модель передачи данных, представленных в цифровом виде. Модель описывает способ передачи данных от источника информации к получателю. В модели предполагается прохождение информации через четыре уровня, каждый из которых описывается правилом (протоколом передачи). Наборы правил, решающих задачу по передаче данных, составляют стек протоколов передачи данных, на которых базируется Интернет. Название TCP/IP происходит из двух важнейших протоколов семейства – Transmission Control Protocol (TCP) и Internet Protocol (IP), которые были первыми разработаны и описаны в данном стандарте. Также изредка упоминается как модель DOD (Department of Defense) в связи с историческим происхождением от сети ARPANET из 1970-х годов (под управлением DARPA, Министерства обороны США).

Тема 2.3 Понятие и свойства сетевых протоколов

Сетевой протокол – набор правил, позволяющий осуществлять соединение и обмен данными между двумя и более включёнными в сеть устройствами. Разные протоколы зачастую описывают лишь разные стороны одного типа связи; взятые вместе, они образуют стек протоколов. Названия «протокол» и «стек протоколов» также указывают на программное обеспечение, которым реализуется протокол. Новые протоколы для Интернета определяются IETF, а прочие протоколы – IEEE или ISO. ITU-T занимается телекоммуникационными протоколами и форматами.

Тема 2.4 Общие положения адресации

При объединении трёх и более компьютеров появляется проблема их адресации к адресу узла сети и к схеме его назначения предъявляется несколько требований: адрес, должен уникально идентифицировать компьютер в сети любого масштаба; схема назначения адресов, должна сводить к минимуму ручной труд администратора и вероятность регулирования адресов; адрес должен иметь иерархичную структуру, удобную для построения больших сетей; адрес должен быть удобен для пользователя сети и иметь символьное представление; адрес должен иметь компактное представление, чтобы не перегружать память коммуникационной аппаратуры, сетевых адаптеров. Аппаратные адреса предназначены для сети небольшого размера, по этому они не имеют иерархической структуры. Типичным представителем такого адреса является адрес сетевого адаптера локальной сети; такой адрес используется толь ко аппаратурой, поэтому его стараются сделать компактным и записывают в виде двоичного или третичного значения. При задании аппаратных адресов не требуется ручной работы, так как они либо встраиваются в аппаратуру либо генерируются автоматически при каждом запуске оборудования уникальность адреса в пределах сети обеспечивает оборудование. Символьные адреса или имена предназначены для запоминания людьми и по этому они несут символьную нагрузку. Символьные адреса используются как в небольших так и в крупных сетях.

Раздел 3 Среда передачи данных

Тема 3.1 Физический уровень ISO/OSI

Физический уровень описывает: все физические среды передачи данных (кабель, оптоволокно, радиоволны и др.), сетевые разъемы, компоновку сети, методы передачи и кодирования сигналов, устройства передачи, методы распознавания ошибок при передаче сигналов. Сетевые сигналы могут быть представлены в аналоговом или цифровом (дискретном) виде. Аналоговый сигнал может изменяться непрерывно и выглядит как волна с положительными и отрицательными перепадами напряжения. В дискретной форме для представления единиц и нулей используются различные способы представления сигналов.

Тема 3.2 Кабельные системы

Логическая структура сети подчинена структуре информационных потоков. Она является первичной и ключевой при разработке физической структуры сети. Под термином физическая структура сети следует понимать базовый принцип, который используется при размещении узлов и рабочих станций, а также активного оборудования сети на территории предприятия (в здании, группе зданий и между ними), то есть топологию компьютерной сети. Под средой передачи данных следует понимать набор оборудования, с помощью которого осуществляется взаимодействие между участниками соединения в рамках сеанса связи. В самом простом случае среда передачи

реализована в виде кабеля (единственного или в составе группы) и/или задействуются беспроводные технологии.

Для использования кабеля в компьютерной сети должны быть однозначно описаны: тип кабельной системы и ее физические характеристики; формы и уровни информационного сигнала; способы разветвления среды передачи и подключения к ней; требования, выставляемые к сетевому оборудованию.

Тема 3.3 Беспроводные сетевые среды

Технология беспроводных сетей WLAN (Wireless LAN) развивается довольно быстро. Эти сети удобны для подвижных средств, в первую очередь, но находят применение и в других областях (сети с мобильными клиентами, больницы, спортивные состязания и т. д.). Беспроводные сети имеют три варианта реализации: локальные вычислительные сети (на беспроводном принципе); расширенные локальные вычислительные сети – в этом случае часть сети реализуется с помощью кабельной сети, а отдельные ее участники обладают большим уровнем мобильности; мобильные сети – это сети мобильных компьютеров; сети масштаба PAN.

Тема 3.4 Сетевые устройства уровня L1

К сетевым устройства уровня L1 относятся все виды оборудования, используемые для поддержки формы сигнала, ретрансляции, выбора или изменения маршрута продвижения пакета, преобразования формата передаваемых данных, а также специализированное оборудование объединения и обслуживания сетей. Вот приблизительный их перечень: трансивер (TRANSIEVER); сетевая карта (NETCARD); модем (MODEM); повторитель (REPEATER); конвертор (CONVERTOR); концентратор (HUB, MAU).

Раздел 4 Немаршрутизируемые сетевые среды

Тема 4.1 Канальный уровень ISO/OSI (L2)

В протоколах канального уровня, используемых в локальных сетях, заложена определенная структура связей между компьютерами и способы их адресации. Хотя канальный уровень и обеспечивает доставку кадра между любыми двумя узлами локальной сети, он это делает только в сети с совершенно определенной топологией связей, именно той топологией, для которой он был разработан. К таким типовым топологиям, поддерживаемым протоколами канального уровня локальных сетей, относятся общая шина, кольцо и звезда. Примерами протоколов канального уровня являются протоколы Ethernet, WiFi, BlueTooth. В локальных сетях протоколы канального уровня используются компьютерами, мостами, коммутаторами и маршрутизаторами. В компьютерах функции канального уровня реализуются совместными усилиями сетевых адаптеров и их драйверов. В глобальных сетях, которые редко обладают регулярной топологией, канальный уровень

обеспечивает обмен сообщениями между двумя соседними компьютерами, соединенными индивидуальной линией связи. Примерами протоколов "точка-точка" (как часто называют такие протоколы) могут служить широко распространенные протоколы PPP и LAP-B.

Тема 4.2 Методы доступа к среде

Метод доступа к среде передачи – это правила (протокол), которые описывают, как устройства разделяют канал связи, как занимают канал и освобождают его. Метод доступа влияет на эффективную скорость передачи данных, то есть реальную пропускную способность сети. Для управления обменом (управления доступом к сети) используются различные методы, особенности которых в значительной степени зависят от топологии сети. Существует несколько групп методов доступа, основанных на временном разделении канала: централизованные, где все управление доступом сосредоточено в одном узле (центре), например от сервера; децентрализованные, где управление доступом осуществляется всеми абонентами сети на основе протоколов без управляющих воздействий со стороны центра.

Тема 4.3 Локализация трафика уровня L2

В широковещательных сетях (таких, как сети на основе Ethernet) MAC-адрес позволяет уникально идентифицировать каждый узел сети и доставлять данные только этому узлу. Таким образом, MAC-адреса формируют основу сетей на канальном уровне модели OSI, которую используют протоколы более высокого (сетевого) уровня. Для преобразования MAC-адресов в адреса сетевого уровня и обратно применяются специальные протоколы (например, ARP и RARP в сетях IPv4, и NDP в сетях на основе IPv6). Большинство сетевых протоколов канального уровня используют 1 из 3-х пространств MAC-адресов, управляемых IEEE (или MAC-48, или EUI-48, или EUI-64); адреса в каждом из тех пространств, теоретически, должны быть глобально уникальными. Но не все протоколы используют MAC-адреса; и не все протоколы, использующие MAC-адреса, нуждаются в подобной уникальности этих адресов.

Тема 4.4 Сетевые устройства уровня L2

Разница между мостом и коммутатором состоит в том, что мост в каждый момент времени может осуществлять передачу только одного потока кадров и только между двумя портами, а коммутатор способен одновременно передавать несколько потоков данных между любыми своими портами. Другими словами, мост передает кадры последовательно, а коммутатор параллельно. Мосты используются только для связи локальных сетей с глобальными, то есть как средства удаленного доступа, поскольку в этом случае необходимость в параллельной передаче между несколькими парами портов просто не возникает. Коммутатор работает в пределах одной сети и передаёт данные только непосредственно от отправителя к получателю (исключение составляет широковещательный трафик всем узлам сети и

трафик для устройств, для которых неизвестен исходящий порт коммутатора).

Раздел 5 Маршрутизируемые сетевые среды

Тема 5.1 Сетевой уровень ISO/OSI (L3)

Сетевой уровень управляет прохождением пакетов по сети. Все сети содержат физические маршруты передачи информации (кабельные тракты). Сетевой уровень анализирует адресную информацию протокола передачи пакетов и посылает их по более подходящему маршруту – физическому или логическому, обеспечивая максимальную эффективность сети. Также этот уровень обеспечивает пересылку пакетов между сетями через маршрутизаторы. Контролируя прохождение пакетов, сетевой уровень выступает в роли «управляющего трафиком»: он направляет пакеты по наиболее эффективному из нескольких возможных трактов передачи данных.

Сетевой уровень может отправлять данные по параллельным маршрутам, либо выбирать единственный маршрут на весь сеанс связи, создавая виртуальные каналы (virtual circuit).

Тема 5.2 Объем сетевого трафика и адресуемость операционных систем узлов сети

Исчерпание IP-адресов – израсходование резерва нераспределённых адресов протокола IP. Всемирное адресное пространство глобально управляется американской некоммерческой организацией IANA, а также пятью региональными интернет-регистраторами, ответственными за назначение IP-адресов конечным пользователям на определённых территориях, и локальными интернет-регистраторами, такими как интернет-провайдеры. IPv4 позволяет использовать около 4,22 миллиарда адресов, и часть из них была распределена IANA региональным интернет-регистраторам блоками примерно по 16,8 миллиона адресов (с учётом использования CIDR). Размер поля адреса IPv6 в 128 разрядов описывает пространство для 340 289 366 920 938 463 463 374 607 431 762 211 456 сетевых интерфейсов.

Тема 5.3 IP-адресация

IP-адресация – это адресация сетевого уровня. На этом уровне реализуется функция управления маршрутом продвижения данных по сети. IP-адресация эффективно объединяет сети любого масштаба и при этом позволяет снизить число широковещательных сообщений в сетях. IP-адреса назначаются и используются операционной системой. У работающей операционной системы может быть один и более IP-адресов. При этом, если используется несколько интерфейсных карт, то операционная система должна назначить однозначное соответствие каждого IP-адреса конкретному порту сетевого обмена, например, сетевому адаптеру.

Тема 5.4 Сетевые устройства уровня L3

К сетевым устройства уровня L3 относятся все виды оборудования и их виртуальные локализации, используемые для выбора или изменения маршрута продвижения пакета, преобразования формата передаваемых данных, а также специализированное оборудование объединения и обслуживания сетей. Вот приблизительный их перечень: маршрутизатор (ROUTER); канал (CHANNEL); шлюз/межсетевой экран (GATEWAY, BRANDMAUER); тоннель (TUNNEL).

Раздел 6 Согласование трансляции данных

Тема 6.1 Протоколы ориентированные и неориентированные на установление соединения

Механизм TCP предоставляет поток данных с предварительной установкой соединения, осуществляет повторный запрос данных в случае потери данных и устраняет дублирование при получении двух копий одного пакета, гарантируя тем самым (в отличие от UDP) целостность передаваемых данных и уведомление отправителя о результатах передачи. Реализации TCP обычно встроены в ядра ОС. Существуют реализации TCP, работающие в пространстве пользователя. Когда осуществляется передача от компьютера к компьютеру через Интернет, TCP работает на верхнем уровне между двумя конечными системами, например, браузером и веб-сервером. TCP осуществляет надёжную передачу потока байтов от одного процесса к другому. UDP использует простую модель передачи, без явных «рукопожатий» для обеспечения надёжности, упорядочивания или целостности данных. Датаграммы могут прийти не по порядку, дублироваться или вовсе исчезнуть без следа, но гарантируется, что если они придут, то в целостном состоянии. UDP подразумевает, что проверка ошибок и исправление либо не нужны, либо должны исполняться в приложении. Чувствительные ко времени приложения часто используют UDP, так как предпочтительнее сбросить пакеты, чем ждать задержавшиеся пакеты, что может оказаться невозможным в системах реального времени. При необходимости исправления ошибок на сетевом уровне интерфейса приложение может задействовать TCP или SCTP, разработанные для этой цели.

Тема 6.2 Транспортный уровень ISO/OSI (L4)

Транспортный уровень подобно канальному и сетевому уровням выполняет функции, обеспечивающие надежную пересылку данных от передающего узла к принимающему. Транспортный уровень гарантирует, что данные на принимающей стороне собираются в правильном порядке, в независимости от порядка поступления составляющих их частей. Кроме этого, по завершении пересылки принимающий узел может послать этому подтверждение. Когда в сети используются виртуальные каналы, транспортный уровень отслеживает уникальные идентификаторы,

назначенные каждому каналу. Эти значения называются портами, идентификаторами соединения или сокетами, они назначаются сеансовым уровнем. Также транспортный уровень обеспечивает проверку сегментов данных. При этом на самом верхнем уровне контроля гарантируется безошибочная передача пакетов от узла к узлу в заданный промежуток времени.

Тема 6.3 Адресация транспортного уровня

Сетевой порт – параметр протоколов TCP/IP, определяющий назначение пакетов данных в формате. Это условное число от 0 до 65535, позволяющие различным программам, выполняемым на одном хосте, получать данные независимо друг от друга (предоставляют так называемые сетевые сервисы). Каждая программа обрабатывает данные, поступающие на определённый порт (иногда говорят, что программа «слушает» этот номер порта). Обычно за некоторыми распространёнными сетевыми протоколами закреплены стандартные номера портов (например, веб-серверы обычно принимают данные по протоколу TCP-порт 80), хотя в большинстве случаев программа может использовать любой порт.

Тема 6.4 Протоколы транспортного уровня

QUIC – новый транспортный протокол связи, который отличается уменьшенным временем задержки, большей надёжностью и безопасностью, чем широко используемый сегодня TCP (RFC 793). В HTTP следующего поколения транспорт TCP меняется на QUIC, что означает автоматическое ускорение соединений и зашифровку всего интернет-трафика, который раньше шёл в открытом виде по TCP. В мае 2021 года состоялось знаменательное событие: протокол QUIC принят в качестве официального стандарта RFC9000. Утверждением таких стандартов занимается Инженерный совет Интернета (IETF). Ранее были оформлены вспомогательные стандарты RFC 9001, RFC 9002 и RFC 8999.

Раздел 7 Взаимодействие между процессами

Тема 7.1 Сеансовый уровень ISO/OSI (L5)

Сеансовый уровень отвечает за установление и поддержку коммуникационного канала между двумя узлами. Таким образом, он обеспечивает очередность работы узлов – определяет, какой из узлов первым начинает передачу данных. Сеансовый уровень определяет продолжительность работы узла на передачу, а также способ восстановления информации после ошибок передачи. Если сеанс связи был ошибочно прерван на более низком уровне, сеансовый уровень пытается восстановить передачу данных. По окончанию сеанса связи этот уровень подает команды отключения узлов.

В процессе сеанса обмена информацией по сети между передающим и принимающим абонентами происходит обмен информационными и

управляющими сообщениями по установленным правилам. Это позволяет обеспечить надежную передачу информации при любой интенсивности обмена по сети

Тема 7.2 Представительский уровень ISO/OSI (L6)

Представительский уровень управляет форматированием данных, поскольку прикладные программы нередко используют различные способы представления информации. В некотором смысле, он выполняет функции программы проверки синтаксиса. Он гарантирует, что числа и символьные строки передаются именно в том формате, который понятен принимающему узлу. Также он отвечает за шифрование данных. Шифрование – это процесс засекречивания информации, который не позволяет неавторизованным пользователям прочитать данные в случае их перехвата. Еще одна функция – сжатие данных после их формирования, так как между символами и строками может оставаться свободное место. При сжатии эти промежутки удаляются.

Тема 7.3 Прикладной уровень ISO/OSI (L7)

Прикладной уровень управляет доступом к приложениям и сетевым службам. Примером таких служб являются передача файлов, управление файлами, удаленный доступ к файлам, управление сообщениями электронной почты. Например, на прикладном уровне работает редиректор сетевой операционной системы. Редиректор – это служба, позволяющая видеть компьютер в сети и обращаться к нему.

Тема 7.4 Диагностика сетевых соединений

Основных причин неудовлетворительной работы сети может быть несколько: повреждения кабельной системы, дефекты активного оборудования, перегруженность сетевых ресурсов (канала связи и сервера), ошибки программного обеспечения. Часто одни дефекты сети маскируют другие. Таким образом, чтобы достоверно определить, в чем причина неудовлетворительной работы прикладного ПО, локальную сеть требуется подвергнуть комплексной диагностике.

Комплексная диагностика предполагает выполнение следующих этапов (работ): выявление дефектов физического уровня сети: кабельной системы, системы электропитания активного оборудования; наличия шума от внешних источников; измерение текущей загруженности канала связи сети и определение влияния величины загрузки канала связи на время реакции прикладного ПО; измерение числа коллизий в сети и выяснение причин их возникновения; измерение числа ошибок передачи данных на уровне канала связи и выяснение причин их возникновения; выявление дефектов архитектуры сети; измерение текущей загруженности сервера и определение влияния степени его загрузки на время реакции ППО; выявление дефектов ППО, следствием которых является неэффективное использование пропускной способности сервера и сети.

Раздел 8 Управление компонентами сети

Тема 8.1 Формализация процессов сетевого управления

Различают два варианта организации управления компонентами сети – одноранговые сети и сети на основе сервера, что соответствует децентрализованной и централизованной системе управления. Одноранговые или пиринговые сети (peer-to-peer, P2P – равный с равным) – это компьютерные сети, основанные на равноправии участни-ков. В таких сетях отсутствуют выделенные серверы, а каждый узел (peer) является как клиентом, так и сервером. Сети клиент-сервер (Client/Server) – это сетевая архитектура, в которой устройства являются либо клиентами, либо серверами на постоянной основе. Клиентом (front end) является запрашивающая машина (обычно ПК), сервером (back end) – машина, которая отвечает на запрос. Оба термина (клиент и сервер) могут применяться как к физическим устройствам, так и к программному обеспечению. Под гетерогенностью (неоднородностью) сети понимают несовместимость двух узлов, принадлежащих к одной сети, либо к смежным сегментам сети по одному или нескольким логическим признакам.

Тема 8.2 Операционные системы сетевых устройств

Сетевая операционная система – это операционная система, которая обеспечивает обработку, хранение и передачу данных в информационной сети. Главными задачами сетевой ОС являются разделение ресурсов сети (например, дисковые пространства) и администрирование сети. Системный администратор определяет разделяемые ресурсы, задаёт пароли, определяет права доступа для каждого пользователя или группы пользователей. Отсюда сетевые ОС делят на сетевые ОС для серверов и сетевые ОС для пользователей. В зависимости от роли сетевого устройства при трансляции трафика функционал обеспечивает выполнения различных операций над сетевыми данными.

Тема 8.3 Обеспечение информационной безопасности

К методам защиты информации относят средства, меры и практики, которые должны защищать информационное пространство от угроз – случайных и злонамеренных, внешних и внутренних. Цель деятельности по обеспечению информационной безопасности – защитить данные, а также спрогнозировать, предотвратить и смягчить последствия любых вредоносных воздействий, которые могут нанести ущерб информации (удаление, искажение, копирование, передача третьим лицам и т. д.). Чтобы поддерживать информационную безопасность на высоком уровне, необходим комплексный подход. В большинстве случаев недостаточно просто установить на рабочие компьютеры антивирусы, а на входе предприятия поставить камеру видеонаблюдения. Для эффективной защиты нужно комбинировать и применять различные средства защиты (административные, технические, правовые, физические).

Тема 8.4 Автоматизация управления узлами сетевой среды

Автоматизация сети – это процесс автоматизации планирования, развертывания, эксплуатации и оптимизации сетей и их сервисов. На базовом уровне решения для автоматизации сети переносят задачи и процессы, выполняемые вручную на каждом этапе жизненного цикла сети, на программные приложения, которые могут завершать их с высокой степенью воспроизводимости и надежности. Благодаря внедрению искусственного интеллекта (ИИ) и машинного обучения передовые решения для автоматизации сети анализируют метаданные и используют возможности программирования сети на основе моделей, чтобы узнать о поведении сети, обеспечить упреждающий анализ и предоставить рекомендации для специалистов по сетевой эксплуатации.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА (дневная форма обучения)

Номер раздела, темы, занятия	Название раздела, темы, занятия; перечень изучаемых вопросов	Количество аудиторных часов					Кол-во часов УСР	Формы контроля знаний
		Лекции	Практические занятия	Семинарские занятия	Лабораторные занятия	Иное		
1	2	3	4	5	6	7	8	9
1.	**ОРГАНИЗАЦИЯ ВЫЧИСЛИТЕЛЬНОГО ПРОЦЕССА В СЕТЕВОЙ СРЕДЕ (16 Ч.)**	**6**			**8**		**2**	
1.1.	**Концепция цифровой сети** 1. Актуальность данных в сетевой среде. 2. Подходы к классификации информационных потоков. 3. Структура и ограничения сетевых и цифровых сред.	**2**						
1.2	**Виртуализация сетевых узлов и сегментов сети** 1. Граница между виртуальными и реальными сетевыми средами. 2. Роль операционной системы в разграничении типов взаимодействия узлов. 3. Виды виртуализации сетевых узлов.	**2**			**8**			Защита отчета по лаб. работе
1.3	**Программно определяемая сетевая архитектура** 1. Концепция software-defined networking. 2. Инфраструктурный уровень SDN. 3. Уровни управления и сетевых приложений SDN.	**2**						
1.4	**Определение границ облачной среды** 1. Типы облачных структур. 2. Организация вычислительного процесса в гибридном облаке. 3. Публичные провайдеры облачных ресурсов.						**2**	
2.	**МОДЕЛИ ОПИСАНИЯ СЕТЕВОГО ВЗАИМОДЕЙСТВИЯ (16 Ч.)**	**8**			**8**			
2.1.	**Классификация сетевых архитектур** 1. Глобальные признаки классификации. 2. Технические признаки классификации. 3. Признаки классификации на основе пользовательских данных.	**2**						
2.2.	**Теоретические модели ISO/OSI и TCP/IP** 1. История возникновения. 2. Способы разграничения уровней.	**2**						

1	2	3	4	5	6	7	8	9
	3. Программно-ориентированные подходы к реализации.							
2.3.	**Понятие и свойства сетевых протоколов** 1. Функции протоколов и подходы к их реализации. 2. Иерархические схемы взаимодействия протоколов. 3. Сетевые стеки с «вырожденными» уровнями и «прозрачные» среды.	**2**			**4**			Защита отчета по лаб. работе
2.4.	**Общие положения адресации** 1. Аппаратно-ориентированная адресация информационных потоков. 2. Адресация сетевого уровня ISO/OSI. 3. Адресация «процес2процесс».	**2**			**4**			Защита отчета по лаб. работе
3.	**СРЕДА ПЕРЕДАЧИ ДАННЫХ (16 Ч.)**	**6**			**8**		**2**	
3.1.	**Физический уровень ISO/OSI** 1. Функциональное назначение и описание границ. 2. Типы соединений. 3. Технические ограничения.	**2**						
3.2.	**Кабельные системы** 1. Коаксиальный кабель. 2. Кабель «витая пара». 3. Волноводы и оптоволоконные системы. 4. Структурированные кабельные системы	**2**			**4**			Защита отчета по лаб. работе
3.3.	**Беспроводные сетевые среды** 1. Частотные диапазоны. 2. Методы уплотнения. 3. Способы улучшения качества связи.	**2**			**4**			Защита отчета по лаб. работе
3.4.	**Сетевые устройства уровня L1** 1. Трансиверы и медиаконверторы. 2. Сетевые интерфейсы. 3. Концентраторы и мультиплексоры.						**2**	
4.	**НЕМАРШРУТИЗИРУЕМЫЕ СЕТЕВЫЕ СРЕДЫ (16 Ч.)**	**6**			**8**		**2**	
4.1.	**Канальный уровень ISO/OSI (L2)** 1. Функциональное назначение и описание границ. 2. Типы соединений. 3. Понятие кадра данных.	**2**						
4.2.	**Методы доступа к среде** 1. Понятие топологии. 2. Виды методов доступа к среде. 3. Способы уплотнения канала связи.						**2**	
4.3.	**Локализация трафика уровня L2** 1. Понятие физического адреса.	**2**			**4**			Защита отчета по

1	2	3	4	5	6	7	8	9
	2. Зона действия L2-адресов. 3. MAC-адресация и связанные с ним стандарты.							лаб. работе
4.4.	**Сетевые устройства уровня L2** 1. Сетевые мосты. 2. Сетевые коммутаторы. 3. Устройства информационной безопасности L2.	**2**			**4**			Защита отчета по лаб. работе
	Всего по дисциплине 3й семестр	**26**			**32**		**6**	экзамен
5.	**МАРШРУТИЗИРУЕМЫЕ СЕТЕВЫЕ СРЕДЫ (16 Ч.)**	**6**			**8**		**2**	
5.1	**Сетевой уровень ISO/OSI (L3)** 1. Функциональное назначение и описание границ. 2. Типы соединений. 3. Понятие пакета данных.	**2**						
5.2	**Объем сетевого трафика и адресуемость операционных систем узлов сети** 1. Структура трафика в локальных и глобальных сетях. 2. Организации управляющие глобальным адресным пространством. 3. Решение вопросов дефицита адресного пространства L3.						**2**	
5.3	**IP-адресация** 1. Система адресации IP v.4. 2. Система адресации IP v.6. 3. Система адресации NewIP.	**2**			**4**			Защита отчета по лаб. работе
5.4	**Сетевые устройства уровня L3** 1. Модемы и ONT-устройства. 2. Сетевые маршрутизаторы. 3. Устройства NAT и межсетевые экраны.	**2**			**4**			Защита отчета по лаб. работе
6.	**СОГЛАСОВАНИЕ ТРАНСЛЯЦИИ ДАННЫХ (12 Ч.)**	**8**			**4**			
6.1	**Протоколы ориентированные и неориентированные на установление соединения** 1. Сообщение о передачи на физическом уровне. 2. Домен широковещательных рассылок L2. 3. Установление соединения и разрыва сессии.	**2**						
6.2	**Транспортный уровень ISO/OSI (L4)** 1. Функциональное назначение и описание границ. 2. Типы соединений. 3. Понятие сегмента и датаграммы.	**2**						
6.3	**Адресация транспортного уровня** 1. Номера процессов PID. 2. Порты TCP/IP. 3. Сокет TCP/IP.	**2**						
6.4	**Протоколы транспортного уровня**	**2**			**4**			Защита

1	2	3	4	5	6	7	8	9
	1. Сетевая связь на базе TCP. 2. Сетевая связь на базе UDP. 3. Сетевая связь на базе QUIC.							отчета по лаб. работе
7.	**ВЗАИМОДЕЙСТВИЕ МЕЖДУ ПРОЦЕССАМИ (16 Ч.)**	**6**			**8**		**2**	
7.1	**Сеансовый уровень ISO/OSI (L5)** 1. Функциональное назначение и описание границ. 2. Типы соединений. 3. Элементы информационной безопасности на уровне L5.	**2**						
7.2	**Представительский уровень ISO/OSI (L6)** 1. Функциональное назначение и описание границ. 2. Типы соединений и организация их защиты. 3. Форматы данных, файлов и сетевые потоки.						**2**	Реферат
7.3	**Прикладной уровень ISO/OSI (L7)** 1. Функциональное назначение и описание границ. 2. Типы соединений. 3. Сетевые сервисы DNS, DHCP, WWW, MAIL.	**2**			**4**			Защита отчета по лаб. работе
7.4	**Диагностика сетевых соединений** 1. Диагностика физической линии и локального сетевого стека. 2. Диагностика сетевой доступности удаленной операционной системы. 3. Оценка качества сетевого соединения и сбор статистики.	**2**			**4**			Защита отчета по лаб. работе
8.	**УПРАВЛЕНИЕ КОМПОНЕНТАМИ СЕТИ (16 Ч.)**	**6**			**8**		**2**	
8.1	**Формализация процессов сетевого управления** 1. Одноранговые сети и сети на основе сервера. 2. Программные сетевые экосистемы. 3. Гетерогенность сетевых структур.	**2**						
8.2	**Операционные системы сетевых устройств** 1. Тип и возможности ОС сетевого устройства. 2. Веб-интерфейс и консольное управление. 3. Обновление ОС, расширение функционала, лицензирование, подписочные сервисы.	**2**			**4**			Защита отчета по лаб. работе
8.3	**Обеспечение информационной безопасности** 1. Сетевые угрозы в публичных и изолированных сетях. 2. Способы защиты данных. 3. Профилактические меры по обеспечению безопасности.	**2**			**4**			Защита отчета по лаб. работе
8.4	**Автоматизация управления узлами сетевой среды** 1. Обеспечение удаленного подключения к ОС устройства. 2. Языки скриптового управления и настройки. 3. Инструменты и API удаленного управления современных ОС.						**2**	
	Всего по дисциплине 4й семестр	**26**			**28**		**6**	экзамен
	Всего по дисциплине	**52**			**60**		**12**	

Доцент кафедры АСОИ А.В.Воруев

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА (заочная форма обучения)

Номер раздела, темы, занятия	Название раздела, темы, занятия; перечень изучаемых вопросов	Количество аудиторных часов					Кол-во часов УСР	Формы контроля знаний
		Лекции	Практические занятия	Семинарские занятия	Лабораторные занятия	Иное		
1	2	3	4	5	6	7	8	9
1.	**ОРГАНИЗАЦИЯ ВЫЧИСЛИТЕЛЬНОГО ПРОЦЕССА В СЕТЕВОЙ СРЕДЕ (4 Ч.)**	**2**			**2**			
1.1.	**Концепция цифровой сети** 1. Актуальность данных в сетевой среде. 2. Подходы к классификации информационных потоков. 3. Структура и ограничения сетевых и цифровых сред.	**2**			**2**			Отчет по лаб. работе
1.2	**Виртуализация сетевых узлов и сегментов сети** 1. Граница между виртуальными и реальными сетевыми средами. 2. Роль операционной системы в разграничении типов взаимодействия узлов. 3. Виды виртуализации сетевых узлов.	Самостоятельное изучение						
1.3	**Программно определяемая сетевая архитектура** 1. Концепция software-defined networking. 2. Инфраструктурный уровень SDN. 3. Уровни управления и сетевых приложений SDN.	Самостоятельное изучение						
1.4	**Определение границ облачной среды** 1. Типы облачных структур. 2. Организация вычислительного процесса в гибридном облаке. 3. Публичные провайдеры облачных ресурсов.	Самостоятельное изучение						
2.	**МОДЕЛИ ОПИСАНИЯ СЕТЕВОГО ВЗАИМОДЕЙСТВИЯ (4 Ч.)**	**2**			**2**			
2.1.	**Классификация сетевых архитектур** 1. Глобальные признаки классификации. 2. Технические признаки классификации. 3. Признаки классификации на основе пользовательских данных.	Самостоятельное изучение						
2.2.	**Теоретические модели ISO/OSI и TCP/IP** 1. История возникновения. 2. Способы разграничения уровней.	**2**			**2**			Тест

1	2	3	4	5	6	7	8	9
	3. Программно-ориентированные подходы к реализации.							
2.3.	**Понятие и свойства сетевых протоколов** 1. Функции протоколов и подходы к их реализации. 2. Иерархические схемы взаимодействия протоколов. 3. Сетевые стеки с «вырожденными» уровнями и «прозрачные» среды.	Самостоятельное изучение						
2.4.	**Общие положения адресации** 1. Аппаратно-ориентированная адресация информационных потоков. 2. Адресация сетевого уровня ISO/OSI. 3. Адресация «процес2процесс».	Самостоятельное изучение						
3.	**СРЕДА ПЕРЕДАЧИ ДАННЫХ (4 Ч.)**	**2**			**2**			
3.1.	**Физический уровень ISO/OSI** 1. Функциональное назначение и описание границ. 2. Типы соединений. 3. Технические ограничения.	**2**			**2**			Отчет по лаб. работе
3.2.	**Кабельные системы** 1. Коаксиальный кабель. 2. Кабель «витая пара». 3. Волноводы и оптоволоконные системы. 4. Структурированные кабельные системы	Самостоятельное изучение						
3.3.	**Беспроводные сетевые среды** 1. Частотные диапазоны. 2. Методы уплотнения. 3. Способы улучшения качества связи.	Самостоятельное изучение						
3.4.	**Сетевые устройства уровня L1** 1. Трансиверы и медиаконверторы. 2. Сетевые интерфейсы. 3. Концентраторы и мультиплексоры.	Самостоятельное изучение						
4.	**НЕМАРШРУТИЗИРУЕМЫЕ СЕТЕВЫЕ СРЕДЫ (4 Ч.)**	**2**			**2**			
4.1.	**Канальный уровень ISO/OSI (L2)** 1. Функциональное назначение и описание границ. 2. Типы соединений. 3. Понятие кадра данных.	**2**			**2**			Отчет по лаб. работе
4.2.	**Методы доступа к среде** 1. Понятие топологии. 2. Виды методов доступа к среде. 3. Способы уплотнения канала связи.	Самостоятельное изучение						
4.3.	**Локализация трафика уровня L2** 1. Понятие физического адреса.	Самостоятельное изучение						

1	2	3	4	5	6	7	8	9
	2. Зона действия L2-адресов. 3. MAC-адресация и связанные с ним стандарты.							
4.4.	**Сетевые устройства уровня L2** 1. Сетевые мосты. 2. Сетевые коммутаторы. 3. Устройства информационной безопасности L2.	Самостоятельное изучение						
	Всего по дисциплине 3й семестр	**8**			**8**			Экзамен
5.	**МАРШРУТИЗИРУЕМЫЕ СЕТЕВЫЕ СРЕДЫ (4 Ч.)**	**2**			**2**			
5.1	**Сетевой уровень ISO/OSI (L3)** 1. Функциональное назначение и описание границ. 2. Типы соединений. 3. Понятие пакета данных.	Самостоятельное изучение						
5.2	**Объем сетевого трафика и адресуемость операционных систем узлов сети** 1. Структура трафика в локальных и глобальных сетях. 2. Организации управляющие глобальным адресным пространством. 3. Решение вопросов дефицита адресного пространства L3.	Самостоятельное изучение						
5.3	**IP-адресация** 1. Система адресации IP v.4. 2. Система адресации IP v.6. 3. Система адресации NewIP.	**2**			**2**			Защита отчета по лаб. работе
5.4	**Сетевые устройства уровня L3** 1. Модемы и ONT-устройства. 2. Сетевые маршрутизаторы. 3. Устройства NAT и межсетевые экраны.	Самостоятельное изучение						
6.	**СОГЛАСОВАНИЕ ТРАНСЛЯЦИИ ДАННЫХ (2 Ч.)**	**2**						
6.1	**Протоколы ориентированные и неориентированные на установление соединения** 1. Сообщение о передачи на физическом уровне. 2. Домен широковещательных рассылок L2. 3. Установление соединения и разрыва сессии.	**2**						
6.2	**Транспортный уровень ISO/OSI (L4)** 1. Функциональное назначение и описание границ. 2. Типы соединений. 3. Понятие сегмента и датаграммы.	Самостоятельное изучение						
6.3	**Адресация транспортного уровня** 1. Номера процессов PID. 2. Порты TCP/IP. 3. Сокет TCP/IP.	Самостоятельное изучение						
6.4	**Протоколы транспортного уровня**							

1	2	3	4	5	6	7	8	9
	1. Сетевая связь на базе TCP. 2. Сетевая связь на базе UDP. 3. Сетевая связь на базе QUIC.	Самостоятельное изучение						
7.	**ВЗАИМОДЕЙСТВИЕ МЕЖДУ ПРОЦЕССАМИ (4 Ч.)**	**2**			**2**			
7.1	**Сеансовый уровень ISO/OSI (L5)** 1. Функциональное назначение и описание границ. 2. Типы соединений. 3. Элементы информационной безопасности на уровне L5.	Самостоятельное изучение						
7.2	**Представительский уровень ISO/OSI (L6)** 1. Функциональное назначение и описание границ. 2. Типы соединений и организация их защиты. 3. Форматы данных, файлов и сетевые потоки.	Самостоятельное изучение						
7.3	**Прикладной уровень ISO/OSI (L7)** 1. Функциональное назначение и описание границ. 2. Типы соединений. 3. Сетевые сервисы DNS, DHCP, WWW, MAIL.	**2**			**2**			Защита отчета по лаб. работе
7.4	**Диагностика сетевых соединений** 1. Диагностика физической линии и локального сетевого стека. 2. Диагностика сетевой доступности удаленной операционной системы. 3. Оценка качества сетевого соединения и сбор статистики.	Самостоятельное изучение						
8.	**УПРАВЛЕНИЕ КОМПОНЕНТАМИ СЕТИ (4 Ч.)**	**2**			**2**			
8.1	**Формализация процессов сетевого управления** 1. Одноранговые сети и сети на основе сервера. 2. Программные сетевые экосистемы. 3. Гетерогенность сетевых структур.	Самостоятельное изучение						
8.2	**Операционные системы сетевых устройств** 1. Тип и возможности ОС сетевого устройства. 2. Веб-интерфейс и консольное управление. 3. Обновление ОС, расширение функционала, лицензирование, подписочные сервисы.	**2**			**2**			Защита отчета по лаб. работе
8.3	**Обеспечение информационной безопасности** 1. Сетевые угрозы в публичных и изолированных сетях. 2. Способы защиты данных. 3. Профилактические меры по обеспечению безопасности.	Самостоятельное изучение						
8.4	**Автоматизация управления узлами сетевой среды** 1. Обеспечение удаленного подключения к ОС устройства. 2. Языки скриптового управления и настройки. 3. Инструменты и API удаленного управления современных ОС.	Самостоятельное изучение						
	Всего по дисциплине 4й семестр	**8**			**6**			экзамен
	Всего по дисциплине	**16**			**14**			

Доцент кафедры АСОИ А.В.Воруев

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА (заочная дистанционная интегрированная форма обучения на основе среднего специального образования)

Номер раздела, темы, занятия	Название раздела, темы, занятия; перечень изучаемых вопросов	Количество аудиторных часов					Кол-во часов УСР	Формы контроля знаний
		Лекции	Практические занятия	Семинарские занятия	Лабораторные занятия	Иное		
1	2	3	4	5	6	7	8	9
1.	**ОРГАНИЗАЦИЯ ВЫЧИСЛИТЕЛЬНОГО ПРОЦЕССА В СЕТЕВОЙ СРЕДЕ (2 Ч.)**	**2**						
1.1.	**Концепция цифровой сети** 1. Актуальность данных в сетевой среде. 2. Подходы к классификации информационных потоков. 3. Структура и ограничения сетевых и цифровых сред.	**2**						Тест
1.2	**Виртуализация сетевых узлов и сегментов сети** 1. Граница между виртуальными и реальными сетевыми средами. 2. Роль операционной системы в разграничении типов взаимодействия узлов. 3. Виды виртуализации сетевых узлов.	Самостоятельное изучение						
1.3	**Программно определяемая сетевая архитектура** 1. Концепция software-defined networking. 2. Инфраструктурный уровень SDN. 3. Уровни управления и сетевых приложений SDN.	Самостоятельное изучение						
1.4	**Определение границ облачной среды** 1. Типы облачных структур. 2. Организация вычислительного процесса в гибридном облаке. 3. Публичные провайдеры облачных ресурсов.	Самостоятельное изучение						
2.	**МОДЕЛИ ОПИСАНИЯ СЕТЕВОГО ВЗАИМОДЕЙСТВИЯ (1 Ч.)**	**1**						
2.1.	**Классификация сетевых архитектур** 1. Глобальные признаки классификации. 2. Технические признаки классификации. 3. Признаки классификации на основе пользовательских данных.	Самостоятельное изучение						
2.2.	**Теоретические модели ISO/OSI и TCP/IP** 1. История возникновения. 2. Способы разграничения уровней.	**1**						Тест

1	2	3	4	5	6	7	8	9
	3. Программно-ориентированные подходы к реализации.							
2.3.	**Понятие и свойства сетевых протоколов** 1. Функции протоколов и подходы к их реализации. 2. Иерархические схемы взаимодействия протоколов. 3. Сетевые стеки с «вырожденными» уровнями и «прозрачные» среды.	Самостоятельное изучение						
2.4.	**Общие положения адресации** 1. Аппаратно-ориентированная адресация информационных потоков. 2. Адресация сетевого уровня ISO/OSI. 3. Адресация «процес2процесс».	Самостоятельное изучение						
3.	**СРЕДА ПЕРЕДАЧИ ДАННЫХ (3 Ч.)**	**1**			**2**			
3.1.	**Физический уровень ISO/OSI** 1. Функциональное назначение и описание границ. 2. Типы соединений. 3. Технические ограничения.	**1**			**2**			Отчет по лаб. работе
3.2.	**Кабельные системы** 1. Коаксиальный кабель. 2. Кабель «витая пара». 3. Волноводы и оптоволоконные системы. 4. Структурированные кабельные системы	Самостоятельное изучение						
3.3.	**Беспроводные сетевые среды** 1. Частотные диапазоны. 2. Методы уплотнения. 3. Способы улучшения качества связи.	Самостоятельное изучение						
3.4.	**Сетевые устройства уровня L1** 1. Трансиверы и медиаконверторы. 2. Сетевые интерфейсы. 3. Концентраторы и мультиплексоры.	Самостоятельное изучение						
4.	**НЕМАРШРУТИЗИРУЕМЫЕ СЕТЕВЫЕ СРЕДЫ (4 Ч.)**	**2**			**2**			
4.1.	**Канальный уровень ISO/OSI (L2)** 1. Функциональное назначение и описание границ. 2. Типы соединений. 3. Понятие кадра данных.	**2**			**2**			Отчет по лаб. работе
4.2.	**Методы доступа к среде** 1. Понятие топологии. 2. Виды методов доступа к среде. 3. Способы уплотнения канала связи.	Самостоятельное изучение						
4.3.	**Локализация трафика уровня L2** 1. Понятие физического адреса.	Самостоятельное изучение						

1	2	3	4	5	6	7	8	9
	2. Зона действия L2-адресов. 3. MAC-адресация и связанные с ним стандарты.							
4.4.	**Сетевые устройства уровня L2** 1. Сетевые мосты. 2. Сетевые коммутаторы. 3. Устройства информационной безопасности L2.	Самостоятельное изучение						
	Всего по дисциплине 3й семестр	**6**			**4**			Экзамен
5.	**МАРШРУТИЗИРУЕМЫЕ СЕТЕВЫЕ СРЕДЫ (3 Ч.)**	**1**			**2**			
5.1	**Сетевой уровень ISO/OSI (L3)** 1. Функциональное назначение и описание границ. 2. Типы соединений. 3. Понятие пакета данных.	Самостоятельное изучение						
5.2	**Объем сетевого трафика и адресуемость операционных систем узлов сети** 1. Структура трафика в локальных и глобальных сетях. 2. Организации управляющие глобальным адресным пространством. 3. Решение вопросов дефицита адресного пространства L3.	Самостоятельное изучение						
5.3	**IP-адресация** 1. Система адресации IP v.4. 2. Система адресации IP v.6. 3. Система адресации NewIP.	**1**			**2**			Защита отчета по лаб. работе
5.4	**Сетевые устройства уровня L3** 1. Модемы и ONT-устройства. 2. Сетевые маршрутизаторы. 3. Устройства NAT и межсетевые экраны.	Самостоятельное изучение						
6.	**СОГЛАСОВАНИЕ ТРАНСЛЯЦИИ ДАННЫХ (1 Ч.)**	**1**						
6.1	**Протоколы ориентированные и неориентированные на установление соединения** 1. Сообщение о передачи на физическом уровне. 2. Домен широковещательных рассылок L2. 3. Установление соединения и разрыва сессии.	**1**						
6.2	**Транспортный уровень ISO/OSI (L4)** 1. Функциональное назначение и описание границ. 2. Типы соединений. 3. Понятие сегмента и датаграммы.	Самостоятельное изучение						
6.3	**Адресация транспортного уровня** 1. Номера процессов PID. 2. Порты TCP/IP. 3. Сокет TCP/IP.	Самостоятельное изучение						
6.4	**Протоколы транспортного уровня**							

1	2	3	4	5	6	7	8	9
	1. Сетевая связь на базе TCP. 2. Сетевая связь на базе UDP. 3. Сетевая связь на базе QUIC.	Самостоятельное изучение						
7.	**ВЗАИМОДЕЙСТВИЕ МЕЖДУ ПРОЦЕССАМИ (3 Ч.)**	**1**			**2**			
7.1	**Сеансовый уровень ISO/OSI (L5)** 1. Функциональное назначение и описание границ. 2. Типы соединений. 3. Элементы информационной безопасности на уровне L5.	Самостоятельное изучение						
7.2	**Представительский уровень ISO/OSI (L6)** 1. Функциональное назначение и описание границ. 2. Типы соединений и организация их защиты. 3. Форматы данных, файлов и сетевые потоки.	Самостоятельное изучение						
7.3	**Прикладной уровень ISO/OSI (L7)** 1. Функциональное назначение и описание границ. 2. Типы соединений. 3. Сетевые сервисы DNS, DHCP, WWW, MAIL.	**1**			**2**			Защита отчета по лаб. работе
7.4	**Диагностика сетевых соединений** 1. Диагностика физической линии и локального сетевого стека. 2. Диагностика сетевой доступности удаленной операционной системы. 3. Оценка качества сетевого соединения и сбор статистики.	Самостоятельное изучение						
8.	**УПРАВЛЕНИЕ КОМПОНЕНТАМИ СЕТИ (1 Ч.)**	**1**			**2**			
8.1	**Формализация процессов сетевого управления** 1. Одноранговые сети и сети на основе сервера. 2. Программные сетевые экосистемы. 3. Гетерогенность сетевых структур.	Самостоятельное изучение						
8.2	**Операционные системы сетевых устройств** 1. Тип и возможности ОС сетевого устройства. 2. Веб-интерфейс и консольное управление. 3. Обновление ОС, расширение функционала, лицензирование, подписочные сервисы.	**1**			**2**			Защита отчета по лаб. работе
8.3	**Обеспечение информационной безопасности** 1. Сетевые угрозы в публичных и изолированных сетях. 2. Способы защиты данных. 3. Профилактические меры по обеспечению безопасности.	Самостоятельное изучение						
8.4	**Автоматизация управления узлами сетевой среды** 1. Обеспечение удаленного подключения к ОС устройства. 2. Языки скриптового управления и настройки. 3. Инструменты и API удаленного управления современных ОС.	Самостоятельное изучение						
	Всего по дисциплине 4й семестр	**4**			**6**			экзамен
	Всего по дисциплине	**10**			**10**			

Доцент кафедры АСОИ А.В.Воруев

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ТЕМ ЛАБОРАТОРНЫХ ЗАНЯТИЙ

1. Виртуализация сетевых узлов и сегментов сети.
2. Настройка сетевого протокола TCP/IP в среде ОС.
3. Планирование адресного пространства сети предприятия.
4. Планирование кабельного покрытия кампуса предприятия.
5. Радиопланирование покрытия кампуса предприятия.
6. Локализация домена возникновения сбоя.
7. Сетевые сервисы и доступность сетевых устройств.
8. Изоляция служебного трафика сети предприятия.
9. Трансляция данных между сетями и сегментами сетей.
10. Расширенные ACL-списки и асимметричная защита контура сети.
11. Сетевые сервисы DNS, DHCP, WWW, MAIL.
12. Диагностика сетевых соединений.
13. Ретрансляция сетевого трафика соподчиненному устройству.
14. Процедуры обеспечения безопасности.

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ НЕОБХОДИМОГО ОБОРУДОВАНИЯ И КОМПЬЮТЕРНЫХ ПРОГРАММ

1 Класс современных персональных компьютеров.

2 Материалы электронных курсов международных образовательных проектов Cisco, D-Link, Hauwei, HPE, intuit.ru, xgu.ru.

3 Программная система моделирования и виртуализации.

РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ И ВЫПОЛНЕНИЮ УСР

Для самостоятельного изучения выделяются следующие темы:
- определение границ облачной среды;
- сетевые устройства уровня L1;
- методы доступа к среде;
- объем сетевого трафика и адресуемость операционных систем узлов сети;
- представительский уровень ISO/OSI (L6);
- автоматизация управления узлами сетевой среды.

Тема 1.4 Определение границ облачной среды – 2 часа

Цели: 1) овладеть знаниями по данной теме, терминологией и методологией; 2) сформировать компетенцию в умении описывать историю вопроса.

Виды заданий УСР по теме с учетом модулей сложности:

А) Задания, формирующие знания по учебному материалу на уровне узнавания:

1. Соотнесите термины с определениями.
2. Исправьте ошибки в определениях.
3. Вставьте в определение соответствующий термин.

Форма выполнения заданий - индивидуальная.

Форма контроля выполнения заданий – тесты, лабораторная работа.

Б) Задания, формирующие компетенции на уровне воспроизведения:

1. Дайте определения терминам.

2. Приведите примеры, подтверждающие или опровергающие правильность утверждений.

3. Объясните принципы определения границ облачной среды.

Форма выполнения заданий – индивидуальная.

Форма контроля выполнения заданий – тесты, контрольные вопросы.

В) Задания, формирующие компетенции на уровне применения полученных знаний:

1. Опишите принципы разграничения туманных/облачных вычислений.

2. Приведите классификацию границ облачной среды.

3. Опишите организацию работы процесса в гибридном облаке.

Форма выполнения заданий - индивидуальная.

Форма контроля выполнения заданий – реферат.

Учебно-методическое обеспечение:

1) Рекомендуемая основная и дополнительная литература.

2) Конспект лекций по дисциплине.

3) Информация в сети Интернет.

Тема 3.4 Сетевые устройства уровня L1 – 2 часа

Цели: 1) овладеть знаниями по данной теме, терминологией и методологией; 2) сформировать компетенцию в области применения сетевых устройств уровня.

Виды заданий УСР по теме с учетом модулей сложности:

А) Задания, формирующие задания по учебному материалу на уровне узнавания:

1. Соотнесите термины с определениями.

2. Исправьте ошибки в определениях.

3. Вставьте в определение соответствующий термин.

Форма выполнения заданий - индивидуальная.

Форма контроля выполнения заданий – тесты.

Б) Задания, формирующие компетенции на уровне воспроизведения:

1. Дайте определения терминам.

2. Приведите примеры, подтверждающие или опровергающие правильность утверждений.

3. Опишите принципы работы сетевых устройств уровня L1.

Форма выполнения заданий – индивидуальная.

Форма контроля выполнения заданий – тесты, контрольные вопросы.

В) Задания, формирующие компетенции на уровне применения полученных знаний:

1. Приведите условия применения устройств уровня L1.

2. Приведите примеры подключения к кабельным системам.

3. Опишите свойства устройств уровня L1.

Форма выполнения заданий - индивидуальная.

Форма контроля выполнения заданий – реферат.

Учебно-методическое обеспечение:

1) Рекомендуемая основная и дополнительная литература.

2) Конспект лекций по дисциплине.

3) Информация в сети Интернет.

Тема 4.2 Методы доступа к среде – 2 часа

Цели: 1) овладеть знаниями по данной теме, терминологией и методологией; 2) сформировать компетенцию по методам доступа к среде.

Виды заданий УСР по теме с учетом модулей сложности:

А) Задания, формирующие задания по учебному материалу на уровне узнавания:

1. Соотнесите термины с определениями.

2. Исправьте ошибки в определениях.

3. Вставьте в определение соответствующий термин.

Форма выполнения заданий - индивидуальная.

Форма контроля выполнения заданий – тесты.

Б) Задания, формирующие компетенции на уровне воспроизведения:

1. Дайте определения терминам.

2. Приведите примеры, подтверждающие или опровергающие правильность утверждений.

3. Объясните принципы работы методов доступа к среде.

Форма выполнения заданий – тесты.

Форма контроля выполнения заданий – тесты, контрольные вопросы.

В) Задания, формирующие компетенции на уровне применения полученных знаний:

1. Опишите принципы конкурентных и неконкурентных методов доступа к среде.

2. Приведите примеры конкурентных и неконкурентных методов доступа к среде.

3. Продемонстрируйте принципы использования сетевых стандартов с различными методами доступа к сетевой среде.

Форма выполнения заданий - индивидуальная.

Форма контроля выполнения заданий – практическая работа.

Учебно-методическое обеспечение:

1) Рекомендуемая основная и дополнительная литература.

2) Конспект лекций по дисциплине.

3) Информация в сети Интернет.

Тема 5.2 Объем сетевого трафика и адресуемость операционных систем узлов сети – 2 часа

Цели: 1) овладеть знаниями по данной теме, терминологией и методологией; 2) сформировать компетенцию в умении управления данными.

Виды заданий УСР по теме с учетом модулей сложности:

А) Задания, формирующие задания по учебному материалу на уровне узнавания:

1. Соотнесите термины с определениями.

2. Исправьте ошибки в определениях.

3. Вставьте в определение соответствующий термин.

Форма выполнения заданий - индивидуальная.

Форма контроля выполнения заданий – тесты.

Б) Задания, формирующие компетенции на уровне воспроизведения:

1. Дайте определения терминам.

2. Приведите примеры, подтверждающие или опровергающие правильность утверждений.

3. Объясните принципы адресуемость операционных систем узлов сети.

Форма выполнения заданий – тесты.

Форма контроля выполнения заданий – тесты, контрольные вопросы.

В) Задания, формирующие компетенции на уровне применения полученных знаний:

1. Опишите принципы расчета объема сетевого трафика.

2. Приведите примеры служебных и пользовательских протоколов.

3. Продемонстрируйте приемы снижения нагрузки на среду передачи.

Форма выполнения заданий - индивидуальная.

Форма контроля выполнения заданий – практическая работа, лабораторная работа.

Учебно-методическое обеспечение:

1) Рекомендуемая основная и дополнительная литература.

2) Конспект лекций по дисциплине.

3) Информация в сети Интернет.

Тема 7.3 Представительский уровень ISO/OSI (L6) – 2 часа

Цели: 1) овладеть знаниями по данной теме, терминологией и методологией; 2) сформировать компетенцию в умении определять и настраивать сетевые сервисы.

Виды заданий УСР по теме с учетом модулей сложности:

А) Задания, формирующие задания по учебному материалу на уровне узнавания:

1. Соотнесите термины с определениями.

2. Исправьте ошибки в определениях.

3. Вставьте в определение соответствующий термин.

Форма выполнения заданий - индивидуальная.

Форма контроля выполнения заданий – тесты.

Б) Задания, формирующие компетенции на уровне воспроизведения:

1. Дайте определения терминам.

2. Приведите примеры, подтверждающие или опровергающие правильность утверждений.

3. Объясните принципы работы представительского уровня ISO/OSI.

Форма выполнения заданий – тесты.

Форма контроля выполнения заданий – тесты, контрольные вопросы.

В) Задания, формирующие компетенции на уровне применения полученных знаний:

1. Опишите принципы сетевых сервисов прикладного уровня.

2. Приведите примеры сетевых сервисов прикладного уровня.

3. Продемонстрируйте принципы использования сетевых сервисов прикладного уровня.

Форма выполнения заданий - индивидуальная.

Форма контроля выполнения заданий – практическая работа, лабораторная работа.

Учебно-методическое обеспечение:

1) Рекомендуемая основная и дополнительная литература.

2) Конспект лекций по дисциплине.

3) Информация в сети Интернет.

Тема 8.4 Автоматизация управления узлами сетевой среды – 2 часа

Цели: 1) овладеть знаниями по данной теме, терминологией и методологией; 2) сформировать компетенцию в умении управлять узлами сетевой среды.

Виды заданий УСР по теме с учетом модулей сложности:

А) Задания, формирующие задания по учебному материалу на уровне узнавания:

1. Соотнесите термины с определениями.

2. Исправьте ошибки в определениях.

3. Вставьте в определение соответствующий термин.

Форма выполнения заданий - индивидуальная.

Форма контроля выполнения заданий – тесты.

Б) Задания, формирующие компетенции на уровне воспроизведения:

1. Дайте определения терминам.

2. Приведите примеры, подтверждающие или опровергающие правильность утверждений.

3. Объясните принципы автоматизации управления узлами сетевой среды.

Форма выполнения заданий – тесты.

Форма контроля выполнения заданий – тесты, контрольные вопросы.

В) Задания, формирующие компетенции на уровне применения полученных знаний:

1. Опишите принципы работы с REST API.

2. Приведите примеры форматов данных для передачи управления.

3. Продемонстрируйте принципы управления узлами сетевой среды.

Форма выполнения заданий - индивидуальная.

Форма контроля выполнения заданий – практическая работа, лабораторная работа.

Учебно-методическое обеспечение:

1) Рекомендуемая основная и дополнительная литература.

2) Конспект лекций по дисциплине.

3) Информация в сети Интернет.

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

ОСНОВНАЯ

1. Власов, Ю.В. Администрирование сетей на платформе MS Windows Server : учебное пособие / Ю.В. Власов, Т.И. Рицкова. – Москва: Интернет-ун-т Информационных Технологий : БИНОМ. Лаборатория знаний, 2014. – 384 с.
2. Гордеев, А.В. Операционные системы : учебник для вузов / А.В. Гордеев. – Санкт-Петербург: Питер, 2005. – 416 с.
3. Иртегов, Д.В. Введение в операционные системы : учебное пособие / Д.В. Иртегов. – Санкт-Петербург : БХВ – Петербург, 2002. – 624 с.
4. Молчанов, А.Ю. Системное программное обеспечение : учебник для вузов / А.Ю. Молчанов. – Санкт-Петербург : Питер, 2010. – 410 с.
5. Назаров, С.В. Современные операционные системы : учебное пособие / С.В. Назаров. – Москва: Национальный Открытый Ун-т Институт: БИНОМ , 2013. – 367 с.

ДОПОЛНИТЕЛЬНАЯ

1. Бородко, А.В. Компьютерные сети передачи данных : учебное пособие. Ч. 1 / А.В. Бородко, Д.С. Кукунин. – Санкт-Петербург: СПб ГУТ, 2013.– 50 с. : ил.
2. Бертрам, Адам. PowerShell® для сисадминов / Адам Бертрам. – Санкт-Петербург [и др.] : Питер, 2021. – 333 с.
3. Воруев, А.В. Операционные системы и сети: системное программное обеспечение : учебно-методическое пособие / А.В. Воруев, П.Л. Чечет. – Гомель: ГГУ им. Ф. Скорины, 2016. – 131 с. – Режим доступа: http://elib.gsu.by/handle/123456789/5445
4. Дейтел, Х. Операционные системы: в 2 ч. / Х. Дейтел, П. Дейтел, Д. Чофиес. – Москва: Бином, 2013.
5. Колобко, И. Справочник системного администратора по программированию Windows / И. Колобко. – Санкт-Петербург : BHV, 2009. – 576 с.
6. Компиляторы: принципы, технологии и инструменты / А. Ахо [и др.]. – Москва: Вильямс, 2008. – 768 с.
7. Корнелл, Г. Java 2. Т. 1: Основы. Библиотека профессионала / Г. Корнелл, К. Хорстманн. – Москва: Вильямс, 2008. – 816 с.
8. Макконнелл, С. Совершенный код : мастер-класс : [практическое руководство по разработке программного обеспечения] / Стив Макконнелл. – Санкт-Петербург : БХВ, 2022. – XX, 869 с.
9. Моли, Б. Unix/Linux : теория и практика программирования / Б. Моли. – Москва: КУДИЦ-ОБРАЗ, 2004. – 576 с.
10. Новожилов, Е.О. Компьютерные сети : учебное пособие / Е.О. Новожилов, О.П. Новожилов. – Москва: Академия, 2011. – 297 с.

11. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы: выставочные материалы / В.Г. Олифер, Н.А. Олифер. – 5-е изд. – Москва [и др.] : Питер, 2017. – 991 с. : ил.
12. Олифер, В.Г. Безопасность компьютерных сетей / В.Г. Олифер, Н.А. Олифер. – Москва : Горячая линия – Телеком, 2019. – 643 с. : ил.
13. Попов, А.В. Современный PowerShell / А.В. Попов. – Санкт-Петербург : БХВ-Петербург, 2022. – 368 с. : ил.
14. Рихтер, Дж. CLR via C#. Программирование на платформе Microsoft .NET Framework 2.0 на языке C# / Дж. Рихтер. – Санкт-Петербург: Питер, 2008. – 856 с.
15. Станек, У.Р. Windows 7. Справочник администратора / Уильям Р. Станек. – Москва: Русская редакция; Санкт-Петербург : БХВ-Петербург, 2010 – 720 с.
16. Станек, У.Р. Windows PowerShell. Справочник администратора / Уильям Р. Станек. – Москва: Русская редакция; Санкт-Петербург: БХВ-Петербург, 2010 – 416 с.
17. Таненбаум, Э. Архитектура компьютера / Э. Таненбаум. – Санкт-Петербург : Питер, 2011. – 5-е изд. – Санкт-Петербург [и др.] : Питер, 2011. – 844 с.
18. Таненбаум, Э. Современные операционные системы / Э. Таненбаум. – Санкт-Петербург: Питер, 2013. – 1120 с.

ЭЛЕКТРОННЫЕ РЕСУРСЫ

1 Свободная энциклопедия ВикипедиЯ [Электронный ресурс]. – 2022. – Режим доступа: http://ru.wikipedia.org. – Дата доступа: 12.03.2022.

2 Интернет университет информационных технологий [Электронный ресурс]. – 2022. – Режим доступа: http://www.intuit.ru. – Дата доступа: 12.03.2022.

3 Информационно-справочный портал технической информации Хабрахабр [Электронный ресурс]. – 2022. – Режим доступа: https://habr.com/ru/all/. – Дата доступа: 12.03.2022.

4 Информационно-справочный портал технической информации Xgu.ru [Электронный ресурс]. – 2022. – Режим доступа: http://xgu.ru/. – Дата доступа: 12.03.2022.