Общая структура и функции сетевой операционной системы

Сетевая операционная система (Network Operating System, NOS) представляет собой специализированное программное обеспечение, которое обеспечивает управление и координацию работы компьютерной сети. Общая структура и функции сетевой операционной системы могут включать в себя следующие элементы:

Управление ресурсами: NOS управляет ресурсами сети, такими как файлы, принтеры, серверы, периферийные устройства и прочее. Он обеспечивает доступ к этим ресурсам пользователям сети в соответствии с их правами доступа.

Аутентификация и авторизация: NOS обеспечивает механизмы аутентификации пользователей и управление правами доступа к ресурсам сети. Это позволяет определить, кто имеет доступ к каким ресурсам и с какими привилегиями.

Управление пользователями и группами: Nекоторые NOS предоставляют возможность создавать пользователей и группы пользователей с различными правами доступа к ресурсам сети. Это упрощает администрирование сети и контроль доступа.

Обеспечение безопасности: NOS включает в себя механизмы для защиты сетевых ресурсов от несанкционированного доступа, такие как механизмы шифрования, брандмауэры, системы обнаружения вторжений и антивирусные средства.

Маршрутизация и коммутация: Некоторые NOS могут включать в себя функции маршрутизации и коммутации данных в сети. Это позволяет оптимизировать передачу данных в сети, управлять трафиком и обеспечивать отказоустойчивость.

Управление сетевыми службами: NOS может включать в себя различные сетевые службы, такие как службы каталогов, службы имен, службы времени и т. д.

Мониторинг и управление ресурсами: NOS предоставляет инструменты для мониторинга и управления ресурсами сети, включая отслеживание использования ресурсов, мониторинг производительности сети, резервирование ресурсов и т. д.

Поддержка сетевых протоколов: NOS поддерживает различные сетевые протоколы, такие как TCP/IP, IPX/SPX и другие, обеспечивая совместимость и взаимодействие между устройствами в сети.

Это основные функции и компоненты сетевой операционной системы. Различные NOS могут предоставлять дополнительные функции в зависимости от их конкретных требований и целей.

Одноранговый принцип организации сетей, преимущества и недостатки. Примеры. Одноранговая сеть в

модели рабочей группы Microsoft Windows.

Одноранговый принцип организации сетей (Peer-to-Peer, P2P) предполагает, что все узлы сети (или большинство из них) имеют одинаковые возможности и функции, и каждый узел может выступать как клиент, так и сервер, в зависимости от конкретной ситуации. Другими словами, нет централизованного сервера, который управляет всеми ресурсами и запросами в сети.

Преимущества одноранговой сети:

Простота настройки: В одноранговой сети нет необходимости в сложной конфигурации централизованного сервера. Каждый компьютер может быть настроен независимо, что делает установку и настройку сети более простой.

Масштабируемость: Поскольку каждый компьютер в одноранговой сети может выступать в роли сервера, сеть может легко масштабироваться путем добавления новых компьютеров без необходимости в дополнительном оборудовании.

Отказоустойчивость: Отсутствие единой точки отказа повышает надежность сети. Если один компьютер выходит из строя, другие компьютеры в сети могут продолжать работу.

Недостатки одноранговой сети:

Ограниченные ресурсы: Поскольку каждый компьютер в сети предоставляет свои ресурсы, такие как файлы или принтеры, доступ к ресурсам может быть ограниченным в зависимости от доступности и активности других компьютеров в сети.

Безопасность: В одноранговой сети более сложно управлять безопасностью, так как каждый компьютер может иметь доступ к ресурсам других компьютеров. Это может повысить риск несанкционированного доступа к данным.

Пример одноранговой сети в модели рабочей группы Microsoft Windows:

В операционных системах семейства Windows, таких как Windows 10 или Windows 11, рабочая группа (Workgroup) является примером одноранговой сети. В рабочей группе каждый компьютер может иметь доступ к ресурсам других компьютеров в сети, и ресурсы могут быть общими для всех участников рабочей группы. Например, компьютеры в рабочей группе могут обмениваться файлами и принтерами без необходимости в централизованном сервере для управления доступом и ресурсами.

Принцип организации сетей с выделенным сервером, преимущества и недостатки. Примеры. Сети масштаба

рабочей группы, кампуса, корпорации.

Принцип организации сетей с выделенным сервером предполагает централизацию управления и ресурсов сети через один или несколько выделенных серверов. Это может включать в себя сервера файлов, серверы баз данных, серверы приложений и т. д. Принцип с выделенным сервером широко используется в сетях различных масштабов, таких как рабочие группы, кампусы и корпорации.

Преимущества принципа с выделенным сервером:

Централизованное управление: Централизованный сервер упрощает администрирование сети, так как администратор может настроить и контролировать ресурсы сети из одного места.

Улучшенная безопасность: Централизованное хранение данных и управление доступом позволяют более эффективно обеспечивать безопасность сети, включая управление правами доступа и мониторинг активности пользователей.

Более эффективное использование ресурсов: Централизация ресурсов позволяет более эффективно использовать их, так как они могут быть распределены между пользователями сети по необходимости.

Более простая масштабируемость: Добавление новых узлов или расширение сети проще реализовать при использовании централизованного сервера, так как его можно настроить для поддержки увеличенной нагрузки.

Недостатки принципа с выделенным сервером:

Одна точка отказа: Если центральный сервер выходит из строя, это может привести к недоступности ресурсов сети для всех или для некоторых пользователей.

Необходимость более сложной инфраструктуры: Централизованные серверы требуют дополнительного оборудования и ресурсов для обеспечения их работы, что может увеличить сложность сетевой инфраструктуры и затраты на обслуживание.

Примеры использования принципа с выделенным сервером в различных масштабах сети:

Рабочая группа: В небольших сетях, например, в домашних сетях или небольших офисах, может быть выделенный сервер для общих файлов, принтеров и резервного копирования данных.

Кампус: В образовательных учреждениях или больших офисах могут использоваться централизованные серверы для управления учебными материалами, электронными ресурсами, электронной почтой и другими сервисами.

Корпорация: В крупных корпоративных сетях централизованные серверы могут предоставлять широкий спектр сервисов, включая серверы файлов, баз данных, электронной почты, веб-серверы и другие.

Эталонная семиуровневая модель OSI, ее роль и общие принципы организации. Функции уровней. 5.Сетевая

модель IEEE Project 802. Методы реализации канального уровня.

Эталонная семиуровневая модель OSI (Open Systems Interconnection):

Роль и общие принципы организации:

Разработана Международной организацией по стандартизации (ISO) для обеспечения взаимодействия различных компьютерных систем и сетей.

Разделяет процесс передачи данных между устройствами на семь последовательных уровней, каждый из которых отвечает за определенные функции и аспекты передачи данных.

Основные принципы: разделение функциональности на отдельные уровни, стандартизация интерфейсов между уровнями, обеспечение модульности и расширяемости сетевых систем.

Функции уровней:

Физический уровень (Physical Layer): Отвечает за физические аспекты передачи данных по среде передачи, такие как сигналы, проводы, радиоволны и прочее.

Канальный уровень (Data Link Layer): Обеспечивает безошибочную передачу данных между устройствами на одной локальной сети, контролируя доступ к среде передачи и обнаруживая и исправляя ошибки передачи данных.

Сетевой уровень (Network Layer): Отвечает за маршрутизацию и пересылку данных через несколько сегментов сети, управление трафиком и обеспечение адресации узлов.

Транспортный уровень (Transport Layer): Обеспечивает эффективную и надежную передачу данных между конечными точками, включая контроль потока данных, разделение и сборку сообщений и обработку ошибок.

Сеансовый уровень (Session Layer): Устанавливает, поддерживает и завершает соединения между устройствами, а также управляет сеансами передачи данных.

Представительный уровень (Presentation Layer): Отвечает за кодирование, сжатие, шифрование и декодирование данных, обеспечивая совместимость и понимание данных между различными системами.

Прикладной уровень (Application Layer): Предоставляет интерфейс для взаимодействия с пользователем и приложениями, а также обеспечивает доступ к сетевым сервисам и ресурсам.

Сетевая модель IEEE Project 802:

Ряд стандартов, разработанных IEEE (Институт инженеров по электротехнике и электронике) для организации и управления локальными сетями.

Основывается на подуровнях канального уровня модели OSI и определяет протоколы и стандарты для реализации сетевых технологий, таких как Ethernet, Wi-Fi и Token Ring.

Примеры протоколов канального уровня:

Ethernet: Стандарты 802.3 определяют методы доступа к среде передачи данных, формат кадров, скорости передачи и другие аспекты Ethernet.

Wi-Fi: Стандарты 802.11 определяют протоколы и спецификации для беспроводных локальных сетей Wi-Fi, включая методы модуляции, безопасность и управление каналами.

Методы реализации канального уровня:

Использование физических сред передачи данных, таких как медные кабели, оптоволокно, радиоволны и инфракрасное излучение.

Протоколы, определяющие методы доступа к среде передачи данных, контроль кадров, обнаружение и исправление ошибок, а также другие аспекты обмена данными между устройствами в сети.

Реализация сетевых устройств, таких как коммутаторы, маршрутизаторы и точки доступа, которые обеспечивают передачу данных в соответствии с протоколами канального уровня.

Понятие стека коммуникационных протоколов, соотношение протоколов и интерфейсов. Преоб- разование

данных при прохождении по стеку и способы адресации

Стек коммуникационных протоколов представляет собой иерархическую структуру протоколов, которые работают вместе для обеспечения передачи данных между устройствами в компьютерной сети. Этот стек состоит из различных уровней, каждый из которых отвечает за определенные аспекты коммуникации. Каждый уровень стека предоставляет интерфейсы для более высокоуровневых и низкоуровневых протоколов.

Соотношение протоколов и интерфейсов:

Физический уровень (Physical Layer): Этот уровень определяет физические характеристики передачи данных по среде передачи, такие как электрические сигналы или световые лучи. Протоколы на этом уровне работают с конкретными технологиями передачи данных, например, Ethernet или Wi-Fi. Интерфейсы этого уровня определяют физическое подключение устройств к среде передачи, например, разъемы Ethernet или антенны Wi-Fi.

Канальный уровень (Data Link Layer): Задачей этого уровня является обеспечение надежной передачи данных между соседними устройствами в сети. Протоколы на этом уровне, такие как Ethernet или Wi-Fi MAC (Media Access Control), обеспечивают контроль доступа к среде передачи и обнаружение ошибок. Интерфейсы канального уровня предоставляют методы доступа к среде передачи для устройств.

Сетевой уровень (Network Layer): Этот уровень обеспечивает маршрутизацию и пересылку данных через несколько сегментов сети. Протоколы на этом уровне, такие как IP (Internet Protocol), управляют адресацией и маршрутизацией данных. Интерфейсы сетевого уровня определяют адресацию узлов и маршруты для передачи данных в сети.

Транспортный уровень (Transport Layer): Задача этого уровня - обеспечить эффективную и надежную передачу данных между конечными точками. Протоколы на этом уровне, такие как TCP (Transmission Control Protocol) и UDP (User Datagram Protocol), обеспечивают контроль потока данных, разделение и сборку сообщений, а также обработку ошибок. Интерфейсы транспортного уровня определяют точки назначения для доставки данных и обеспечивают управление потоком данных.

Преобразование данных при прохождении по стеку:

Данные преобразуются на каждом уровне стека протоколов для обеспечения передачи и обработки в соответствии с требованиями протоколов этого уровня. Например, на физическом уровне данные могут преобразовываться в электрические сигналы или световые импульсы, а на транспортном уровне могут добавляться информация о портах отправителя и получателя.

Способы адресации:

Каждый уровень стека имеет свои собственные методы адресации, которые обеспечивают уникальную идентификацию устройств или сегментов сети на этом уровне. Например, на физическом уровне используются MAC-адреса, на сетевом - IP-адреса, а на транспортном - портовые номера.

Общая характеристика промышленных стеков протоколов. Специфика реализаций стеков прото- колов

NetBEUI, IPX/SPX, AppleTalk.

Промышленные стеки протоколов представляют собой наборы коммуникационных протоколов, разработанные для использования в промышленных средах, таких как производственные предприятия, автоматизированные системы управления и другие отрасли. Эти стеки протоколов часто оптимизированы для специфических требований и особенностей промышленных сетей, таких как высокая надежность, минимальные задержки и пропускная способность.

Специфика реализаций стеков протоколов NetBEUI, IPX/SPX и AppleTalk:

NetBEUI (NetBIOS Extended User Interface):

Характеристика: NetBEUI - это протокол, который обеспечивает надежную и эффективную передачу данных в локальных сетях, основанных на технологии Microsoft Windows.

Специфика реализации: NetBEUI работает на канальном уровне стека протоколов и основан на NetBIOS (Network Basic Input/Output System), который предоставляет приложениям доступ к сетевым службам.

Применение: Часто использовался в сетях Windows в прошлом, но в настоящее время он менее распространен из-за ограничений на расширение и недостаточной поддержки современных сетевых технологий.

IPX/SPX (Internetwork Packet Exchange/Sequenced Packet Exchange):

Характеристика: IPX/SPX - это набор протоколов, разработанных Novell для сетей NetWare, который предоставляет протоколы канального уровня и транспортного уровня.

Специфика реализации: IPX (Internetwork Packet Exchange) работает на сетевом уровне и обеспечивает маршрутизацию и пересылку данных, а SPX (Sequenced Packet Exchange) - на транспортном уровне и обеспечивает надежную доставку данных между устройствами.

Применение: IPX/SPX широко использовался в сетях NetWare, но в настоящее время уступил место более современным протоколам, таким как TCP/IP.

AppleTalk:

Характеристика: AppleTalk - это протокол, разработанный Apple для обеспечения сетевого взаимодействия между устройствами в сетях Macintosh.

Специфика реализации: AppleTalk включает в себя несколько протоколов, таких как AppleTalk Data Stream Protocol (ADSP) для транспортного уровня и AppleTalk Address Resolution Protocol (AARP) для сетевого уровня.

Применение: AppleTalk был популярным протоколом в сетях Macintosh в прошлом, но в настоящее время он устарел и был заменен более современными протоколами, такими как TCP/IP.