Лабораторная работа № 1

Тема: Построение одноранговой сети.

Цель лабораторной работы: создать одноранговую сеть с использованием маршрутизатора, коммутатора и нескольких компьютеров, настроить базовые параметры сети.

Эталонная модель OSI (Open Systems Interconnection) представляет собой абстрактную иерархическую структуру, разработанную для стандартизации процесса сетевого взаимодействия. Она состоит из семи уровней:

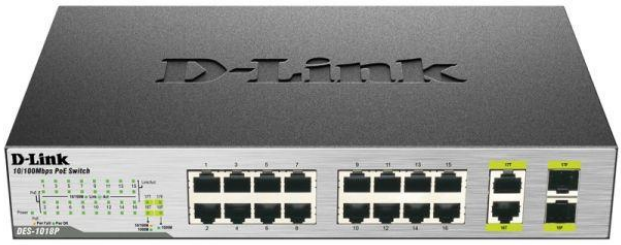
1.Физический уровень (Physical Layer): определяет аппаратные характеристики передачи данных через физические среды, такие как кабели, разъемы, сигналы.

Основные функции: Передача битов по физической среде.

Протоколы: Ethernet, Bluetooth, Wi-Fi.

Устройства: Кабели, концентраторы, повторители.

2.Канальный уровень (Data Link Layer): осуществляет организацию данных в кадры, обеспечивает управление доступом к среде (MAC-подуровень), исправление ошибок.



Основные функции: Обеспечение надежной передачи кадров в локальной сети.

Протоколы: Ethernet, PPP, CDP.

Устройства: Коммутаторы, мосты, сетевые адаптеры.

Назначение коммутатора в том, чтобы объединять множество разных устройств (компьютеров, принтеров, серверов, МФУ и прочих) в одну общую локальную сеть, позволяя её пользователям обмениваться информацией.

Чтобы принять решение об пересылке фрейма, коммутатор использует таблицу коммутации.

3.Сетевой уровень (Network Layer): определяет логическую адресацию устройств (IP-адреса), управляет маршрутизацией и обеспечивает доставку данных от отправителя к получателю.

Основные функции: Маршрутизация пакетов в глобальной сети.

Протоколы: IP, ICMP, OSPF.

Устройства: Маршрутизаторы, многофункциональные устройства (multilayer switches).

4.Транспортный уровень (Transport Layer): обеспечивает надежную доставку данных, управление потоком, сегментацию и сборку сообщений. Примеры протоколов: TCP, UDP.
Основные функции: Обеспечение надежной и упорядоченной доставки данных.
Протоколы: TCP, UDP.

5.Сеансовый уровень (Session Layer): осуществляет управление сеансами связи, синхронизацию данных и восстановление после сбоев.
Основные функции: Управление сеансами связи между приложениями.
Протоколы: NetBIOS, RPC.

6.Представительский уровень (Presentation Layer): занимается преобразованием данных в формат, понятный приложениям, обеспечивает кодирование и сжатие данных.
Основные функции: Преобразование данных в удобный для передачи формат.
Протоколы: SSL.

7.Прикладной уровень (Application Layer): Предоставляет интерфейс для взаимодействия между прикладными программами и сетью, включая функции, такие как электронная почта, передача файлов и доступ к базам данных.
Основные функции: Предоставление интерфейса для взаимодействия с прикладными программами.
Протоколы: HTTP, FTP, SMTP.

Эта модель обеспечивает стандартизированный подход к построению сетевых протоколов, позволяя разработчикам создавать совместимые системы, поддерживающие множество различных приложений и устройств.

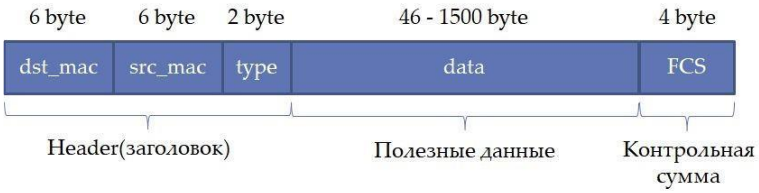
п·о·р	Основные протоколы TCP/IP по уровням модели OSI [скрыть]
Прикладной	BGP • HTTP • DHCP • IRC • SNMP • DNS • NNTP • XMPP • SIP • BitTorrent • IPP • NTP • SNTP • RDP
	Электронная почта SMTP • POP3 • IMAP4
	Передача файлов FTP • TFTP • SFTP
	Удалённый доступ rlogin • Telnet
Представления	XDR • SSL
Сеансовый	ADSP • H.245 • iSNS • NetBIOS • PAP • RPC • L2TP • PPTP • RTCP • SMPP • SCP • SSH • ZIP • SDP
Транспортный	TCP • UDP • SCTP • DCCP • RUDP • RTP
Сетевой	IPv4 • IPv6 • IPsec • ICMP • IGMP • ARP • RARP • RIP2 • OSPF
Канальный	Ethernet • PPPoE • PPP • L2F • 802.11 Wi-Fi • 802.16 WiMax • Token ring • ARCNET • FDDI • HDLC • SLIP • ATM • DTM • X.25 • Frame relay • SMDS • STP
Физический	Ethernet • RS-232 • EIA-422 • RS-449 • RS-485

Стек TCP/IP — это набор протоколов, используемых для связи и передачи данных в компьютерных сетях. Он был разработан в конце 1960-х и стал основой интернета и современных сетей.

Стек TCP/IP состоит из четырех уровней:

1.Канальный (Network Access Layer): Этот уровень определяет физическое подключение к сети и передачу данных по нему. Он включает в себя такие протоколы, как Ethernet, IEEE 802.11, WLAN, SLIP, Token Ring, ATM и MPLS и другие.

Формат Ethernet-фрейма:



2.Сетевой (Internet Layer): Этот уровень отвечает за маршрутизацию данных в сети. Он использует протокол IP (Internet Protocol), который назначает уникальные IP-адреса устройствам и обеспечивает доставку пакетов данных от отправителя к получателю по сети. Протоколы: IP + вспомогательные протоколы, вроде ICMP и IGMP.

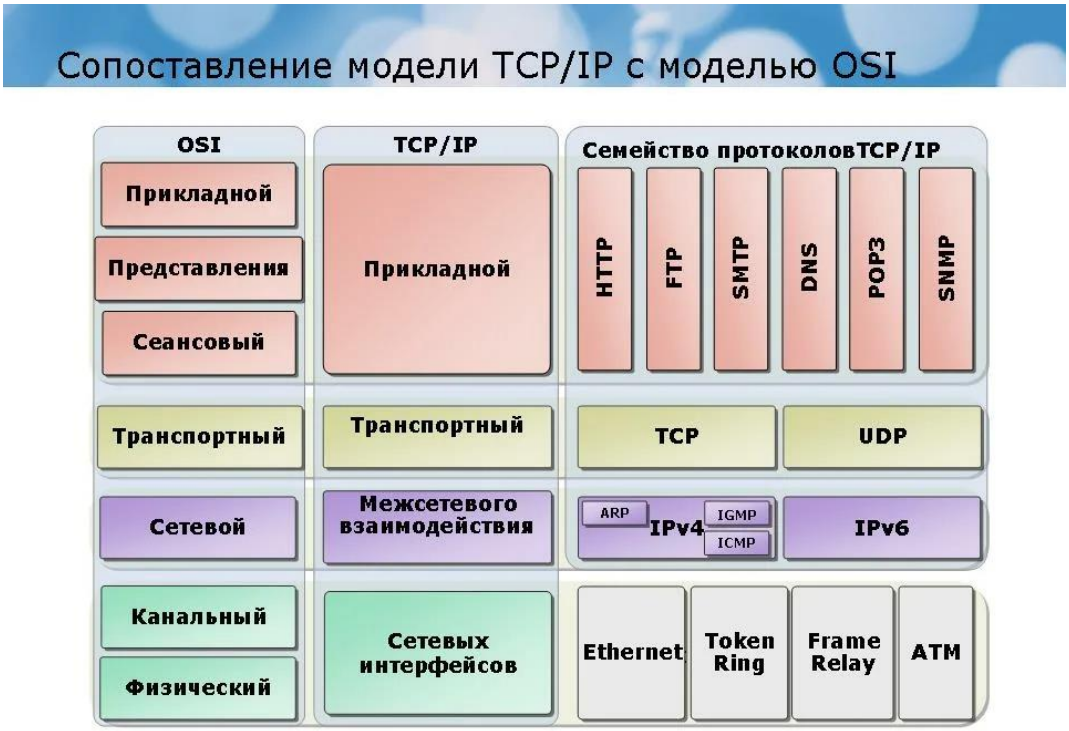
Формат IP-пакета:

3.Транспортный уровень (Transport Layer): На этом уровне обеспечивается надежная доставка данных между устройствами. Самыми известными протоколами на этом уровне являются TCP (Transmission Control Protocol) и UDP (User Datagram Protocol). TCP обеспечивает надежную и упорядоченную доставку данных с подтверждениями, в то время как UDP обеспечивает более быструю, но ненадежную доставку без подтверждений.

Формат TCP-сегмента:

Формат UDP-сегмента:

4.Прикладной уровень (Application Layer): Этот уровень предоставляет интерфейс для приложений и сервисов, использующих сеть. На этом уровне работают протоколы, такие как HTTP (Hypertext Transfer Protocol) для передачи веб-страниц, SMTP (Simple Mail Transfer Protocol) для отправки электронной почты, FTP (File Transfer Protocol) для передачи файлов и многие другие.

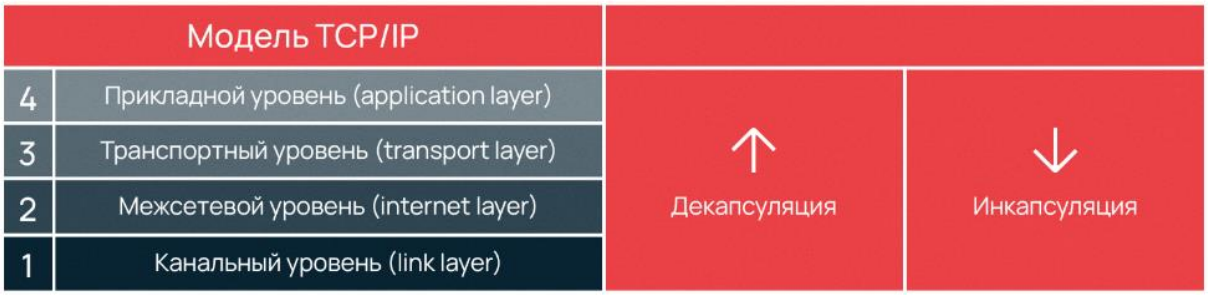


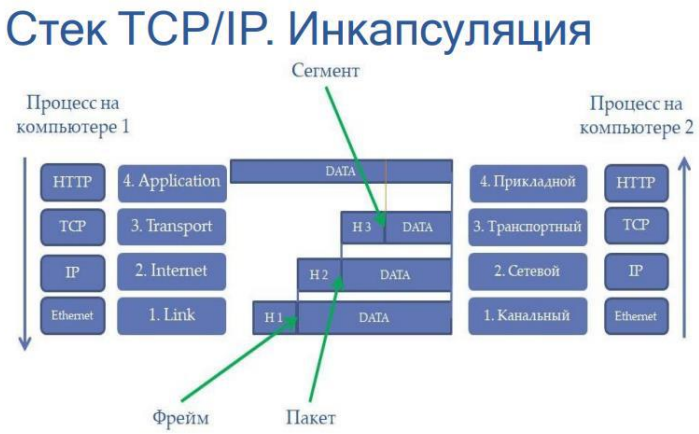
Инкапсуляция - деинкапсуляция данных

Инкапсуляция данных - это процесс, в котором некоторая дополнительная информация добавляется к элементу данных, чтобы добавить к нему некоторые функции. В нашей сети мы используем модель OSI или TCP/IP, и в этих моделях передача данных происходит через различные уровни. Инкапсуляция данных добавляет к данным информацию протокола, чтобы передача данных могла происходить надлежащим образом. Эта информация может быть добавлена в заголовок (header) или в конец (footer или trailer) данных.

Данные инкапсулируются на стороне отправителя, начиная с уровня приложения и заканчивая физическим уровнем. Каждый уровень берет инкапсулированные данные из предыдущего слоя и добавляет некоторую дополнительную информацию для их инкапсуляции и некоторые другие функции с данными. Эти функции могут включать в себя последовательность данных, контроль и обнаружение ошибок, управление потоком, контроль перегрузки, информацию о маршрутизации и так далее.

Деинкапсуляция данных - это процесс, обратный инкапсуляции данных. Инкапсулированная информация удаляется из полученных данных для получения исходных данных. Этот процесс происходит на стороне получателя. Данные деинкапсулируются на том же уровне на стороне получателя, что и инкапсулированный уровень на стороне отправителя. Добавленная информация заголовка и футера удаляется из данных в этом процессе.





Протокол Ethernet

Ethernet - это стандартный протокол канального уровня (Data Link Layer) модели OSI, который определяет метод передачи данных в локальной сети. Этот протокол широко используется для соединения устройств внутри офисов, домов и центров обработки данных.

Основные характеристики протокола Ethernet:

Кадры данных (Frames): Данные в сети Ethernet передаются в виде кадров, которые содержат заголовок и конечный разделитель (FCS - Frame Check Sequence) для обеспечения целостности данных.

MAC-адресация: Каждое устройство в сети Ethernet имеет уникальный физический адрес, известный как MAC-адрес (Media Access Control). MAC-адрес используется для идентификации устройств в локальной сети.

Контроль доступа к среде передачи (CSMA/CD): Ethernet использует метод CSMA/CD (Carrier Sense Multiple Access with Collision Detection) для контроля доступа к среде передачи данных. Этот метод позволяет устройствам конфликтовать за доступ к среде передачи и обнаруживать коллизии в случае их возникновения.

Скорости передачи данных: Стандарты Ethernet поддерживают различные скорости передачи данных, такие как 10 Mbps (Ethernet), 100 Mbps (Fast Ethernet), 1 Gbps (Gigabit Ethernet), 10 Gbps (10 Gigabit Ethernet), и так далее.

Топология сети: Ethernet поддерживает различные топологии сети, включая звезду, кольцо, и шину. Однако, в современных сетях наиболее распространенной является звездообразная топология с использованием коммутаторов.

Поверх Ethernet могут работать различные протоколы сетевого уровня, такие как IP, IPv6, IPX и др.

Коммутаторы и хабы: Для передачи данных Ethernet использует устройства, такие как коммутаторы и хабы. Коммутаторы работают на более высоком уровне и обеспечивают более эффективное управление трафиком, в то время как хабы просто усиливают сигналы и ретранслируют их всем устройствам в сегменте сети.

Протокол ARP (Address Resolution Protocol)

Протокол ARP (Address Resolution Protocol) является частью стека протоколов TCP/IP и используется для сопоставления IP-адресов с физическими (MAC) адресами в локальной сети. Основная задача ARP - определение MAC-адреса устройства по его IP-адресу, что необходимо для корректной передачи данных в локальной сети.

Процесс работы протокола ARP выглядит следующим образом:

Запрос ARP (ARP Request):

Когда устройство (например, компьютер или маршрутизатор) хочет отправить пакет данных другому устройству в локальной сети, но знает только его IP-адрес, оно отправляет широковещательный ARP-запрос в сеть с просьбой указать MAC-адрес для соответствующего IP-адреса.

Ответ ARP (ARP Reply):

Устройство, которому адресован запрос (по известному IP-адресу), отвечает, предоставляя свой MAC-адрес.

Кеширование (Caching):

После получения ответа, отправитель кеширует полученную пару IP-адрес/MAC-адрес, чтобы избежать повторных запросов при общении с тем же устройством в ближайшем будущем. Кэш ARP помогает ускорить процесс обмена данными в локальной сети.

Протокол ARP является частью канального уровня (Data Link Layer) модели OSI и работает напрямую поверх различных технологий сети, таких как Ethernet. ARP-запросы и ответы обычно передаются внутри кадра данных сетевого уровня.

Протокол ICMP (Internet Control Message Protocol)

Протокол ICMP представляет собой часть семейства протоколов TCP/IP и используется для обмена контрольными сообщениями и диагностической информацией между устройствами в сети. Он обеспечивает средства для проверки доступности сетевых узлов, обработки ошибок и определения маршрутов.

Вот ключевые аспекты протокола ICMP:

Контрольные сообщения (ICMP Messages): ICMP предназначен для отправки различных контрольных сообщений между устройствами в сети. Например, сообщение "Echo Request" используется при выполнении команды ping для проверки доступности удаленного узла.

Ping (Echo Request и Echo Reply): Одним из наиболее распространенных применений ICMP является утилита ping, которая использует сообщения "Echo Request" и "Echo Reply" для проверки связи с удаленными узлами. При отправке Echo Request удаленное устройство должно ответить сообщением Echo Reply, подтверждая свою доступность.

Обработка ошибок и определение маршрутов: ICMP также используется для передачи сообщений об ошибках, таких как "Destination Unreachable" или "Time Exceeded". Эти сообщения помогают определить, почему пакеты не могут быть доставлены или почему истекло время на маршруте.

Traceroute: Утилита traceroute также использует ICMP для определения маршрута, который проходит пакет данных от отправителя к получателю. Каждый узел на маршруте отвечает ICMP-сообщением, позволяя определить, через какие узлы проходит пакет.

Сетевая диагностика: ICMP широко применяется для диагностики сетевых проблем и проверки работоспособности сетевых устройств.

Важно отметить, что ICMP не является протоколом передачи данных, как TCP или UDP, а служит для обмена контрольными и диагностическими сообщениями между устройствами в сети.

Одноранговая сеть (Peer-to-Peer Network) - это тип сети, в которой каждый компьютер (или устройство) имеет равные права и может одновременно выступать в роли клиента и сервера. Каждое устройство подключено к сети и может обмениваться ресурсами (файлами, принтерами, другими устройствами) напрямую друг с другом, без центрального управления или контроля.

Одноранговые сети обычно масштабируются легко и просты в настройке, что делает их популярными для небольших домашних сетей или небольших офисных сред. Однако, они могут иметь ограничения в эффективности и масштабируемости по сравнению с более сложными сетями, такими как клиент-серверные сети.

В одноранговой сети каждое устройство может предоставлять ресурсы другим устройствам и получать доступ к ресурсам, предоставляемым другими. Кроме того, такие сети обычно менее зависимы от отказоустойчивости, поскольку отказ одного компьютера не приводит к полному отказу сети.

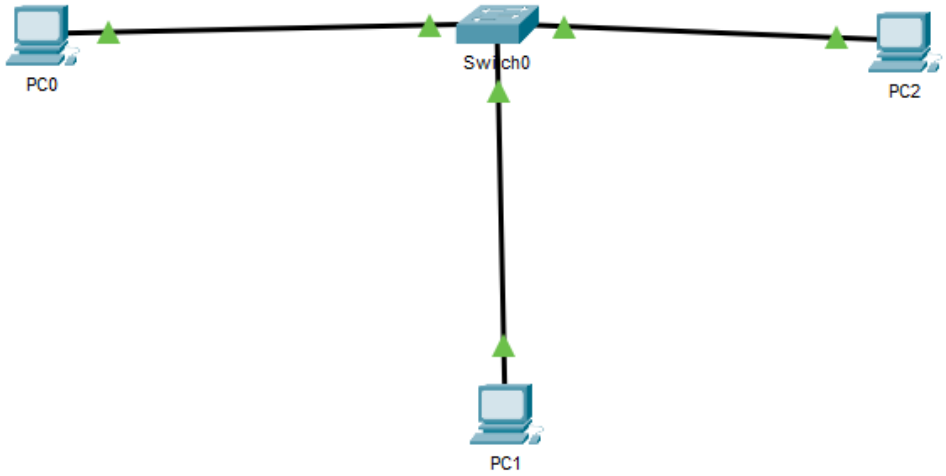
Примерами одноранговых сетей являются домашние сети, где несколько компьютеров или устройств соединены напрямую друг с другом для обмена файлами и использования общих ресурсов.

Задание:

1. Создайте логическую схему сети с 3 компьютерами и коммутатором.
   - выберите End Devices из списка в левом нижнем углу. Перетащите 3 стандартных компьютера в область составления схемы.
   - в левом нижнем углу выберите категорию устройств Switches. Добавьте коммутатор в прототип вашей сети.

- выберите в левом нижнем углу значок Connections. Выберите тип кабеля Copper Straight-Through. Щелкните первый хост (PC0) и назначьте кабель разъему FastEthernet0. Щелкните коммутатор (Switch0) и выберите любой свободный порт.

- повторите предыдущий шаг для PC1 и PC2.



2. Настройка имен хостов и IP-адресов на компьютерах

- щелкните PC0. Выберите вкладку конфигурации. На левой панели выберите вкладку FastEthernet и добавьте IP-адрес 192.168.1.1 и маску сети 255.255.255.0. Для PC1 и PC2 установите адреса 192.168.1.2 и 192.168.1.3 соответственно.

- проверьте связь между ПК командой **ping**.

3. Создайте сетевой трафик и понаблюдайте за потоком данных от PC-A до PC-C.

- перейдите в режим Simulation.

- нажмите «Изменить фильтр», на вкладке IPv4 выберите фильтры ARP и ICMP, остальные галочки снимите.

- щелкните изображение закрытого конверта на панели инструментов, щелкните значок PC1, затем на PC2.

- на панели моделирования нажмите Auto Capture/Play. Просмотрите путь конвертов ICMP и ARP.

- посмотрите заголовки пакетов 1..3 уровней. Найдите mac- и IP-адреса получателя и отправителя.

4. Просмотрите таблицы ARP на каждом компьютере.

- выберите инструмент «лупа» на вертикальной панели инструментов.

- щелкните PC1. Появится таблица ARP для компьютера PC-A. Просмотрите также таблицы ARP для PC-B и PC-C.

- щелкните PC-A и выберите вкладку Desktop.

- выберите Command Prompt, введите команду **arp -a** и нажмите Enter для просмотра таблицы ARP в режиме рабочего стола компьютера. Изучите таблицы ARP для компьютеров B и C.

Отчет по лабораторной работе должен содержать:
- скриншоты Cisco Packet Tracer, демонстрирующими выполнение пунктов задания;
- выводы.