**РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ**

**Факультет физико-математических и естественных наук**

**Кафедра теории вероятностей и кибербезопасности**

**ОТЧЁТ**

**ПО ЛАБОРАТОРНОЙ РАБОТЕ №1**

*дисциплина: Администрирование локальных сетей*

Студент: Скандарова Полина Юрьевна

Студ. билет № 1132221815

Группа: НПИбд-02-22

**МОСКВА**

2025 г.

**Цель работы:**

Установка инструмента моделирования конфигурации сети Cisco Packet Tracer, знакомство с его интерфейсом.

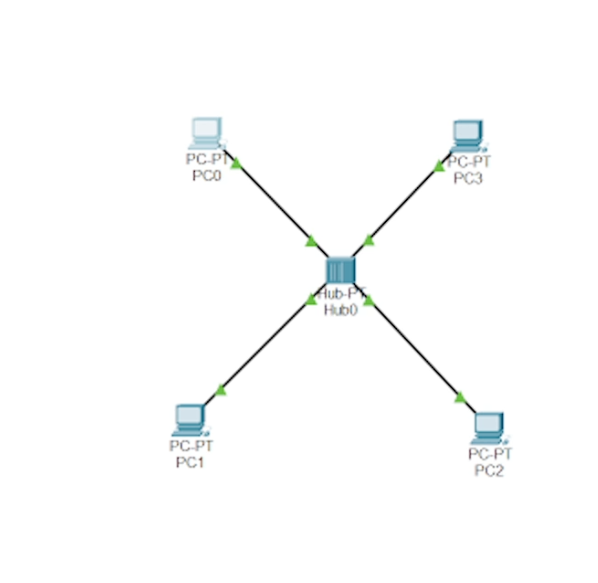
**Выполнение работы:**

Создадим новый проект с названием lab\_PT-01.pkt (Рис. 1.1):



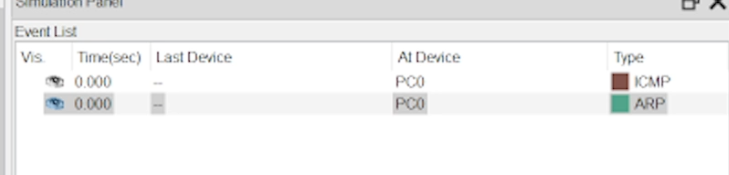
**Рис. 1.1.** Создание нового проекта.

В рабочем пространстве разместим концентратор (Hub-PT) и четыре оконечных устройства PC. Соединим оконечные устройства с концентратором прямым кабелем (рис. 1.2). Щёлкнув последовательно на каждом оконечном устройстве, зададим статические IP-адреса 192.168.1.11, 192.168.1.12, 192.168.1.13, 192.168.1.14 с маской подсети 255.255.255.0.



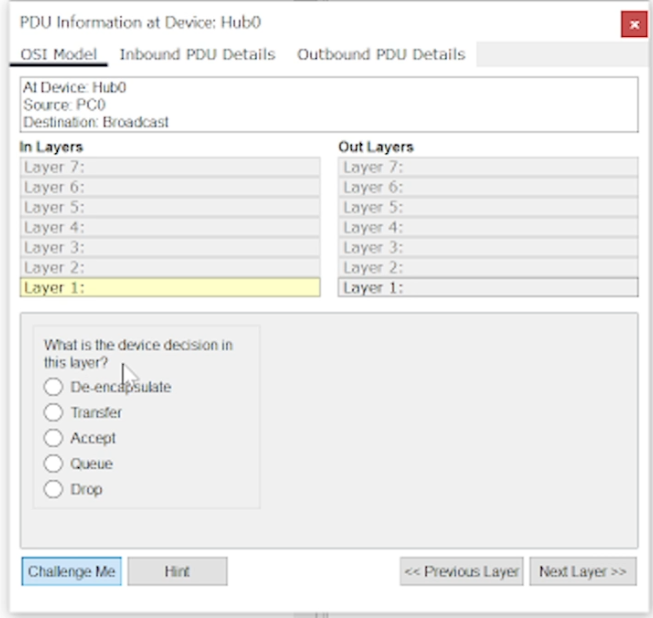
**Рис. 1.2.** Модуль простой сети с концентратором.

В основном окне проекта перейдём из режима реального времени (Realtime) в режим моделирования (Simulation). Выберем на панели инструментов мышкой «Add Simple PDU (P)» и щёлкнем сначала на PC0, затем на PC2. В рабочей области должны будут появится два конверта, обозначающих пакеты, в списке событий на панели моделирования должны будут появиться два события, относящихся к пакетам ARP и ICMP соответственно (рис. 1.3). На панели моделирования нажмём кнопку «Play» и проследим за движением пакетов ARP и ICMP от устройства PC0 до устройства PC2 и обратно.



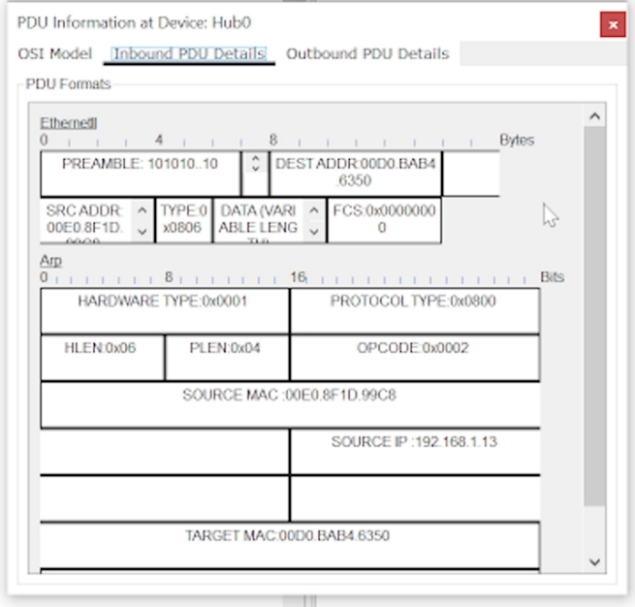
**Рис. 1.3.** События в режиме моделирования Packet Tracer.

Щёлкнув на строке события, откроем окно информации о PDU и изучим, что происходит на уровне модели OSI при перемещении пакета (рис. 1.4). Используя кнопку «Проверь себя» (Challenge Me) на вкладке OSI Model, ответим на вопросы.



**Рис. 1.4.** Информация о PDU: уровень OSI.

Откроем вкладку с информацией о PDU (рис. 1.5). Исследуем структуру пакета ICMP. Опишем структуру кадра Ethernet. Какие изменения происходят в кадре Ethernet при передвижении пакета? Какой тип имеет кадр Ethernet? Опишите структуру MAC-адресов.



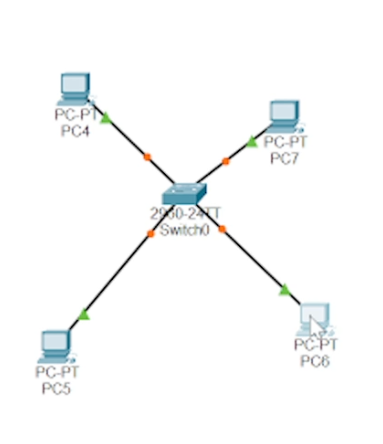
**Рис. 1.5.** Информация о PDU: форматы пакетов.

Очистим список событий, удалив сценарий моделирования. Выберем на панели инструментов мышкой «Add Simple PDU (P)» и щёлкнем сначала на PC0, затем на PC2. Снова выберем на панели инструментов мышкой «Add Simple PDU (P)» и щёлкнем сначала на PC2, затем на PC0. На панели моделирования нажмите кнопку «Play» и проследим за возникновением коллизии. В списке событий посмотрим информацию о PDU. В отчёте поясните, как отображается в заголовках пакетов информация о коллизии и почему возникла коллизия.

Перейдём в режим реального времени (Realtime). В рабочем пространстве разместим коммутатор (например Cisco 2950-24) и 4 оконечных устройства PC. Соединим оконечные устройства с коммутатором прямым кабелем.

Щёлкнув последовательно на каждом оконечном устройстве, зададим статические IP-адреса 192.168.1.21, 192.168.1.22, 192.168.1.23, 192.168.1.24 с маской подсети 255.255.255.0.

В основном окне проекта перейдём из режима реального времени (Realtime) в режим моделирования (Simulation). Выберем на панели инструментов мышкой «Add Simple PDU (P)» и щёлкнем сначала на PC4, затем на PC6. В рабочей области должны будут появится два конверта, обозначающих пакеты, в списке событий на панели моделирования должны будут появиться два события, относящихся к пакетам ARP и ICMP соответственно (рис. 1.7). На панели моделирования нажмём кнопку «Play» и проследим за движением пакетов ARP и ICMP от устройства PC4 до устройства PC6 и обратно. В отчёте поясните, есть ли различия и в чём они заключаются в событиях протокола ARP в сценарии с концентратором.

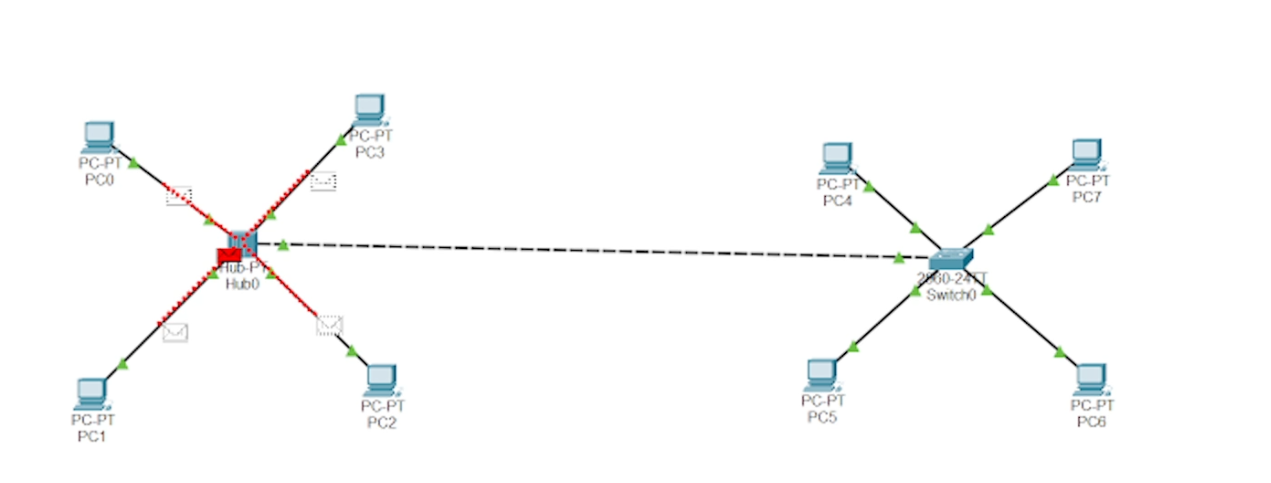


**Рис. 1.6.** Модель простой сети с коммутатором.

Исследуем структуру пакета ICMP. Опишите структуру кадра Ethernet. Какие изменения происходят в кадре Ethernet при передвижении пакета? Какой тип имеет кадр Ethernet? Опишите структуру MAC-адресов.

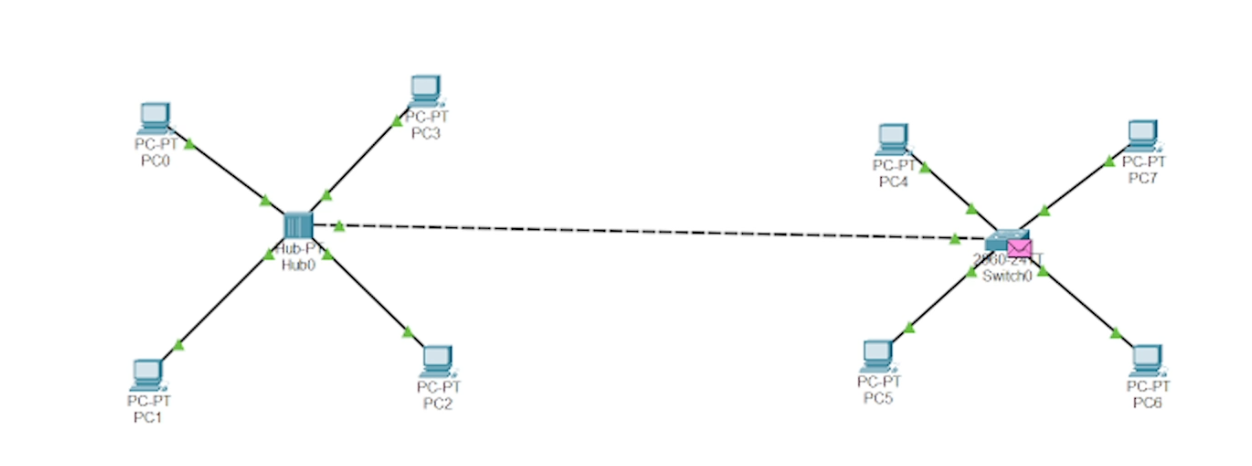
Очистим список событий, удалив сценарий моделирования. Выберем на панели инструментов мышкой «Add Simple PDU (P)» и щёлкнем сначала на PC4, затем на PC6. Снова выберем на панели инструментов мышкой «Add Simple PDU (P)» и щёлкнем сначала на PC6, затем на PC4. На панели моделирования нажмём кнопку «Play» и проследите за движением пакетов. В отчёте поясните, почему не возникает коллизия.

Перейдём в режим реального времени (Realtime). В рабочем пространстве соединим кроссовым кабелем концентратор и коммутатор. Перейдём в режим моделирования (Simulation). Очистим список событий, удалив сценарий моделирования. Выберем на панели инструментов мышкой «Add Simple PDU (P)» и щёлкните сначала на PC0, затем на PC4. Снова выберем на панели инструментов мышкой «Add Simple PDU (P)» и щёлкнем сначала на PC4, затем на PC0. На панели моделирования нажмём кнопку «Play» и проследим за движением пакетов. В отчёте поясните, почему сначала возникает коллизия (рис. 1.7), а затем пакеты успешно достигают пункта назначения.



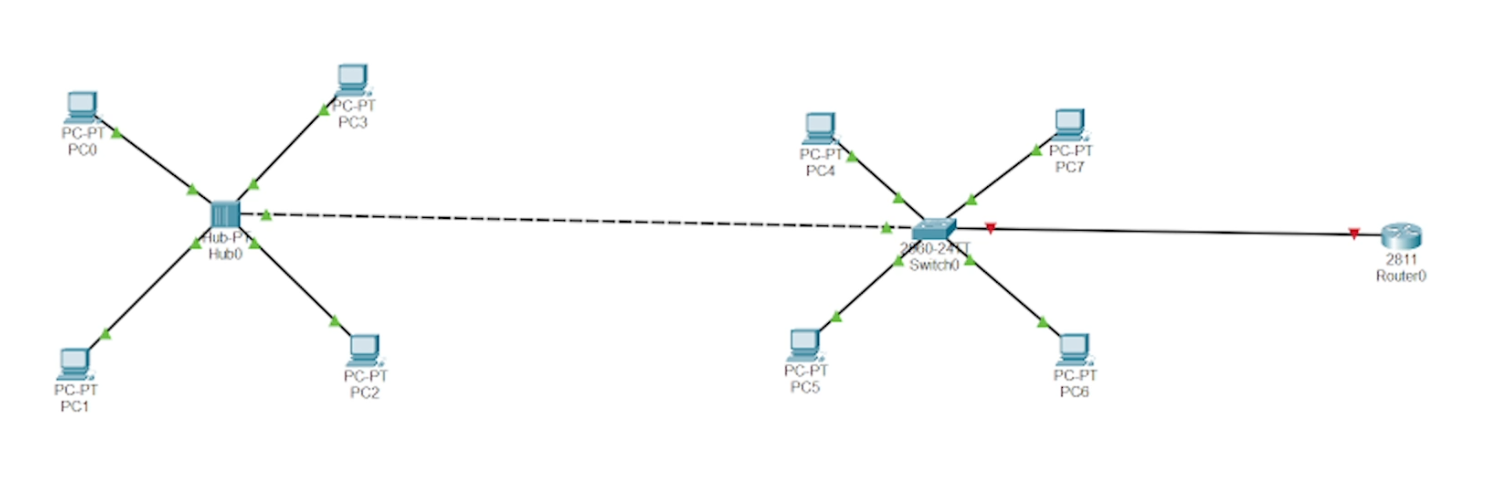
**Рис. 1.7.** Сценарий с возникновением коллизии.

Очистим список событий, удалив сценарий моделирования. На панели моделирования нажмём «Play» и в списке событий получим пакеты STP (рис. 1.8). Исследуем структуру STP. Опишите структуру кадра Ethernet в этих пакетах. Какой тип имеет кадр Ethernet? Опишите структуру MAC- адресов.

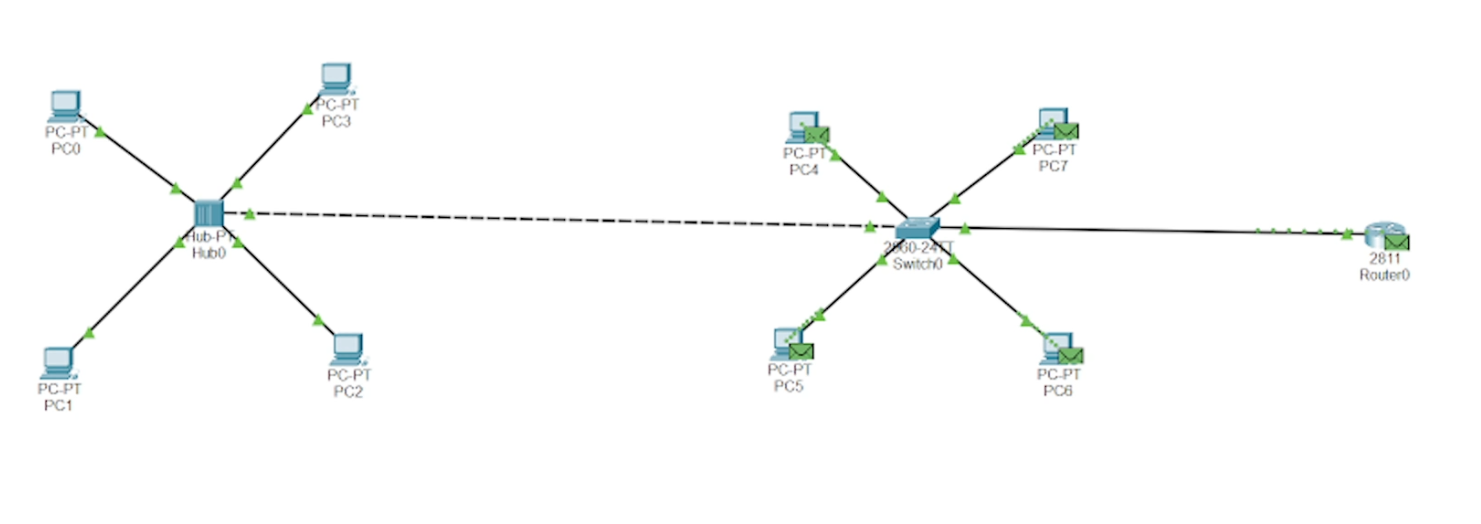


**Рис. 1.8.** Сценарий с протоколом STP.

Перейдём в режим реального времени (Realtime). В рабочем пространстве добавим маршрутизатор (например, Cisco 2811). Соединим прямым кабелем коммутатор и маршрутизатор (рис. 1.9). Щёлкнем на маршрутизаторе и на вкладке его конфигурации пропишем статический IP-адрес 192.168.1.254 с маской 255.255.255.0, активируем порт, поставив галочку «On» напротив «Port Status» (рис. 1.10).



**Рис. 1.9.** Модель простой сети с маршрутизатором.



**Рис. 1.10.** Активация порта на маршрутизаторе.

Перейдём в режим моделирования (Simulation). Очистим список событий, удалив сценарий моделирования. Выберем на панели инструментов мышкой «Add Simple PDU (P)» и щёлкнем сначала на PC3, затем на маршрутизаторе. На панели моделирования нажмём кнопку «Play» и проследим за движением пакетов ARP, ICMP, STP и CDP. Исследуем структуру пакета CDP, опишите структуру кадра Ethernet. Какой тип имеет кадр Ethernet?

**Вывод**

Установлен инструмент моделирования конфигурации сети Cisco Packet Tracer, знакомство с его интерфейсом прошло успешно.

**Контрольные вопросы**

**Ответы на контрольные вопросы:**

1. <a name=\_toc433396195></a>Дайте определение следующим понятиям: концентратор, коммутатор, маршрутизатор, шлюз (gateway). В каких случаях следует использовать тот или иной тип сетевого оборудования?

* **Концентратор (Hub): концентратор является устройством, которое принимает данные с одного устройства сети и передает их всем остальным устройствам в сети.**
* **Он работает на физическом уровне модели OSI (Open Systems Interconnection), просто усиливая сигнал и передавая его по всем портам.**
* **Концентратор не имеет интеллекта для анализа данных или управления трафиком.**
* **Обычно используется в небольших сетях или для расширения количества портов в сети.**
* **Коммутатор (Switch): коммутатор также работает на канальном уровне OSI и способен анализировать адреса MAC (Media Access Control) устройств, подключенных к нему.**
* **В отличие от концентратора, коммутатор передает данные только тому устройству, для которого они предназначены, что делает его более эффективным по сравнению с концентратором.**
* **Коммутаторы обычно используются в сетях с высокой пропускной способностью, где требуется эффективное управление трафиком и безопасностью.**
* **Маршрутизатор (Router): маршрутизатор работает на сетевом уровне OSI и способен анализировать IP-адреса устройств в сети.**
* **Он принимает решения о передаче данных между различными сетями на основе IP-адресации и информации о маршрутах.**
* **Маршрутизаторы используются для соединения различных сетей (например, локальной сети и Интернета) и обеспечения маршрутизации данных между ними.**
* **Шлюз (Gateway): шлюз - это устройство, которое соединяет различные сети с разными протоколами, форматами данных или архитектурой.**
* **В контексте сетей Шлюз часто используется как точка доступа к другой сети, например, для доступа к Интернету из локальной сети.**
* **Шлюз выполняет преобразование данных и управляет коммуникацией между разными сетями.**
* **В зависимости от конкретного применения, шлюз может быть представлен как программное или аппаратное оборудование.**
* **Выбор типа сетевого оборудования зависит от конкретных потребностей сети:**
* **Для простых сетей малого размера без особых требований к управлению трафиком можно использовать концентраторы.**
* **Для сетей среднего и большого размера, где требуется управление трафиком и безопасность, рекомендуется использовать коммутаторы.**
* **Для подключения сетей различных типов и обеспечения маршрутизации данных между ними необходимы маршрутизаторы.**
* **Шлюзы используются там, где требуется соединение сетей с разными протоколами или доступ к внешним сетям, таким как Интернет.**

1. Дайте определение следующим понятиям: ip-адрес, сетевая маска, broadcast адрес.

* **IP-адрес (Internet Protocol Address): IP-адрес - это числовая метка, присвоенная каждому устройству в компьютерной сети, использующей протокол Интернета (IP).**
* **Он используется для идентификации и адресации устройств в сети, позволяя маршрутизаторам правильно направлять пакеты данных к их назначению.**
* **IP-адрес состоит из 32 бит (для IPv4) или 128 бит (для IPv6) и представляется в виде четырех чисел, разделенных точками (для IPv4) или в виде группы шестнадцатеричных чисел, разделенных двоеточиями (для IPv6).**
* **Сетевая маска (Network Mask): сетевая маска используется для определения, какая часть IP-адреса относится к сети, а какая - к узлу в этой сети.**
* **Она представляет собой набор битов, который определяет количество битов, зарезервированных для идентификации сети, в IP-адресе.**
* **Обычно сетевая маска записывается вместе с IP-адресом, используя формат, подобный "192.168.1.0/24", где /24 указывает на количество битов, отведенных для сети.**
* **Broadcast-адрес: Broadcast-адрес - это специальный адрес в сети, который используется для отправки данных всем устройствам в этой сети.**
* **Когда устройство отправляет пакет данных на broadcast-адрес, все устройства в этой сети получают этот пакет.**
* **Broadcast-адрес для IPv4 обычно имеет значение, в котором все биты хоста установлены в 1, например, для сети 192.168.1.0 с сетевой маской /24 broadcast-адрес будет 192.168.1.255.**
* **Для IPv6 broadcast-адреса не существует, вместо этого используется multicast для доставки данных на несколько устройств.**

1. Как можно проверить доступность узла сети?

* **Ping (ICMP Echo Request): Ping - это самый распространенный способ проверки доступности узла. Это делается отправкой ICMP (Internet Control Message Protocol) Echo Request пакета на IP-адрес узла и ожиданием ответа. Если узел доступен, он отправит обратно ICMP Echo Reply пакет.**
* **Traceroute (или traceroute6 для IPv6): Этот инструмент используется для определения маршрута, который пакеты данных пройдут от отправителя до получателя. Он посылает серию пакетов с увеличивающимся TTL (Time-to-Live) и анализирует ответы для определения промежуточных узлов. Это позволяет выявить места, где возникают проблемы в маршрутизации.**
* **Проверка порта (Port Scan): Если вам нужно не только убедиться, что узел отвечает на пинг, но и проверить, работает ли на нем конкретное сетевое приложение, вы можете выполнить сканирование портов. Существуют различные инструменты, такие как Nmap, которые позволяют сканировать порты на удаленном узле и определить, какие порты открыты и доступны для подключения.**
* **Использование специализированных сетевых инструментов: Существует множество специализированных инструментов для управления сетями, которые предоставляют информацию о доступности узлов, их статусе и производительности. Это могут быть мониторинговые системы, такие как Zabbix, Nagios, Prometheus, или программное обеспечение от производителей сетевого оборудования.**
* **Использование интерфейсов управления сетевым оборудованием: Многие сетевые устройства предоставляют интерфейсы управления или CLI (Command Line Interface), через которые можно проверить доступность узлов в сети, например, используя команды ping или traceroute на маршрутизаторе.**
* **Выбор метода зависит от конкретных требований и характеристик вашей сетевой инфраструктуры.**