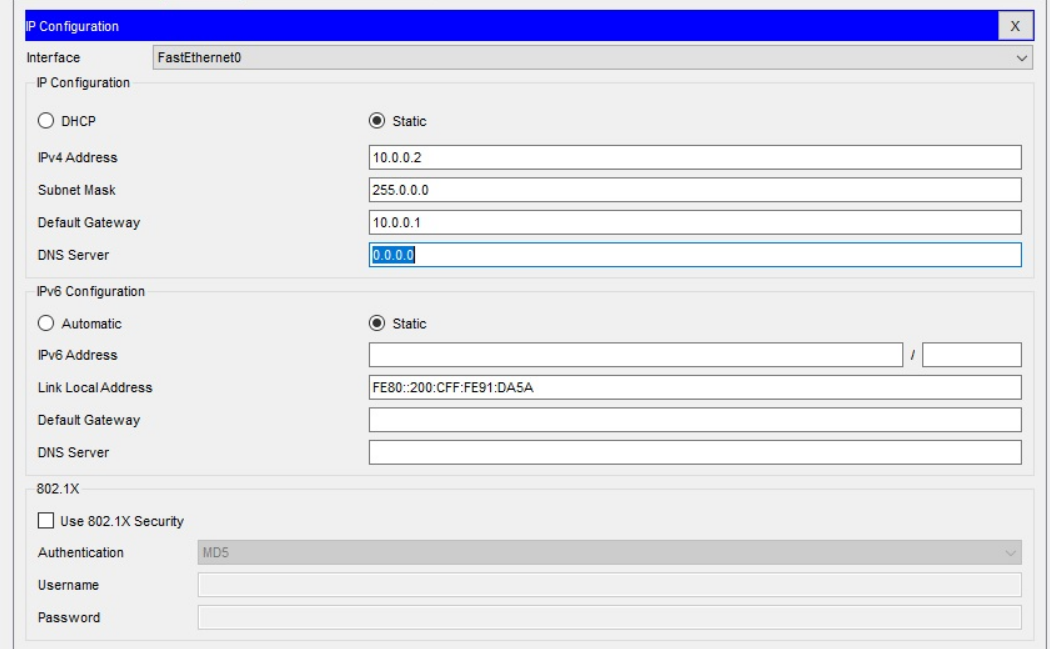
**3.1 Знакомство с интерфейсом Packet Tracer**

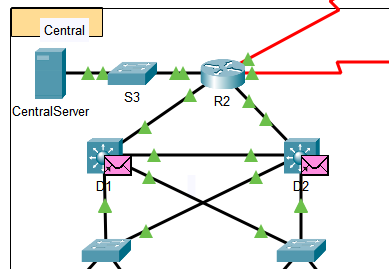
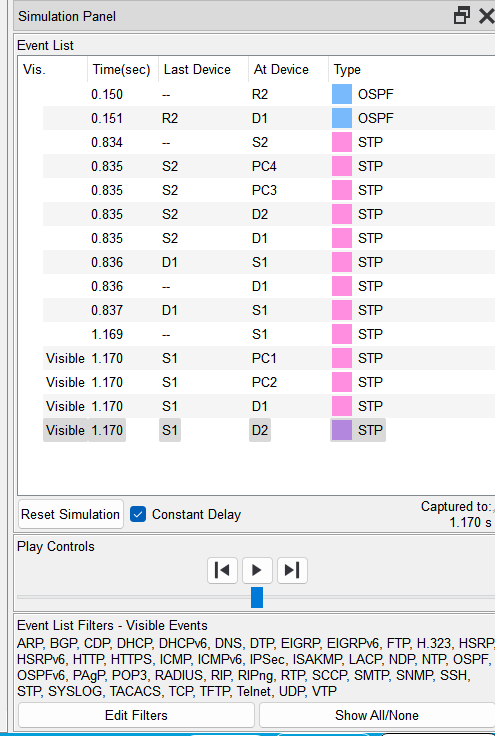
**(выполнять в Cisco Packet Tracer 6.0.1 или старше)**

   Найдите учебное пособие «Configuring Devices Using the Desktop Tab» (Настройка устройств с помощью вкладки «Desktop»). **Посмотрите первую часть учебного пособия и ответьте на следующий вопрос: какие данные можно настроить в окне «IP Configuration»?**

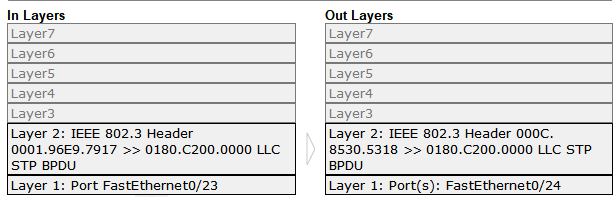


**Переключитесь между режимами реального времени и моделирования.**

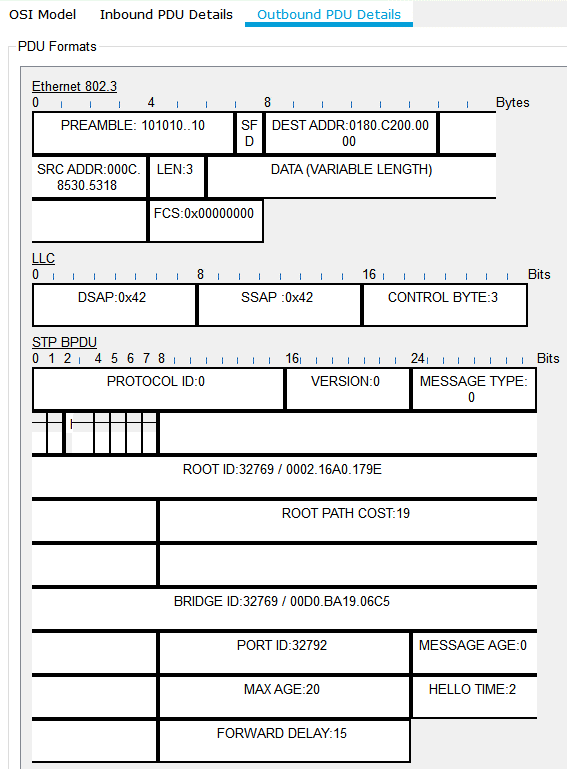
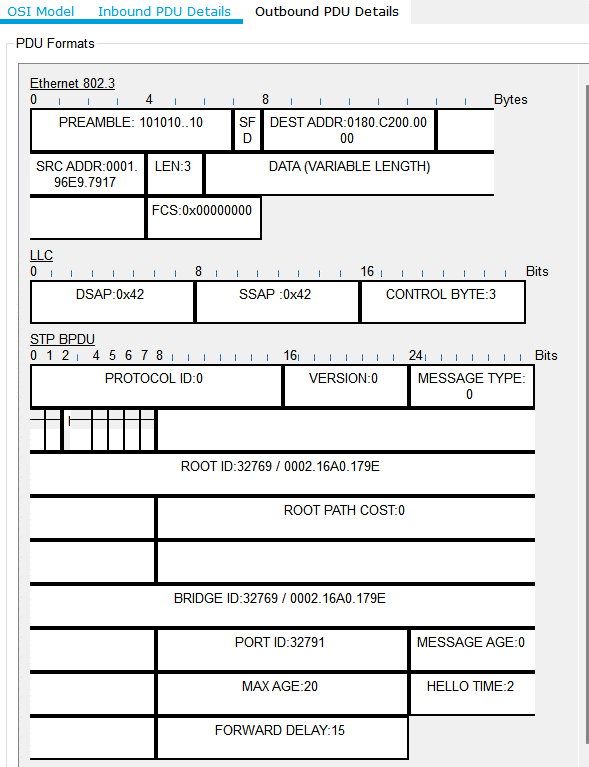
Теперь вы должны видеть пакеты данных, представленные конвертами разного цвета, которые движутся между устройствами.



- На **вкладке OSI Model** сколько уровней **In Layers** и **Out Layers** содержат информацию?

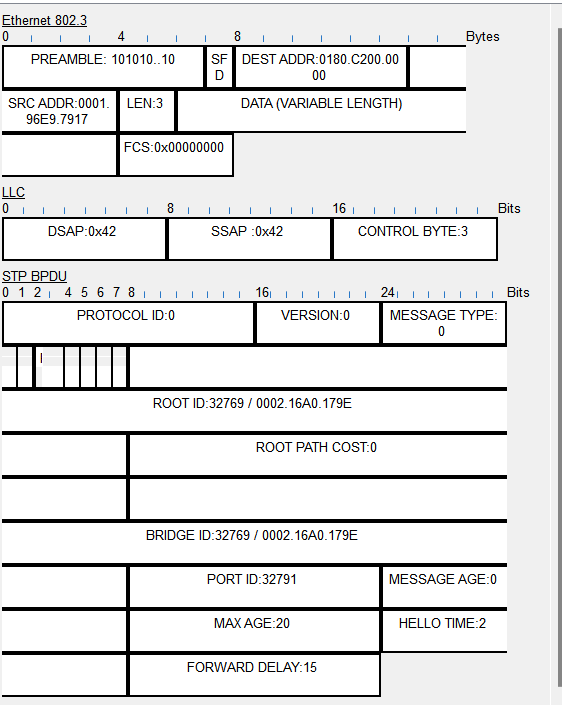


- Что является заголовками основных разделов на вкладках **Inbound PDU Details** (Сведения о входящем PDU) и **Outbound PDU Details**(Сведения об исходящем PDU)?



- Нажмите кнопку «Назад» и перейдите между вкладками **Inbound PDU Details** и **Outbound PDU Details**. Изменились ли данные? Если да, то как?

Данные не изменились.



**Изучение локальных сетей, сети WAN и сети Интернет**

**Перечислите категории промежуточных устройств**.

* Промежуточные устройства включают:
  1. Маршрутизаторы (Routers)
  2. Коммутаторы (Switches)
  3. Беспроводные устройства (Wireless Devices)
  4. Модемы (Modems)

**Не входя в облако Интернет или Интранет, перечислите количество значков в топологии, представляющих оконечные устройства (при наличии только одного входящего подключения).**

* Оконечные устройства с одним подключением:
  1. HomeDesktop (домашний настольный ПК)
  2. Home Laptop (домашний ноутбук)
  3. Струйный принтер
  4. Планшетный ПК
  5. Сервер филиала
  6. Лазерный принтер
  7. Смартфон
  8. Гостевое устройство
  9. Отдел продаж (компьютер)
  10. Бухгалтерия (компьютер)
  11. IP-телефон 0
  12. IP-телефон 1

Итого: 12 оконечных устройств.

**Если не учитывать два облака, сколько значков в топологии представляют промежуточные устройства (при наличии нескольких входящих подключений)?**

* Промежуточные устройства:
  1. R4 (маршрутизатор)
  2. S4 (коммутатор)
  3. R2 (маршрутизатор)
  4. S3 (коммутатор)
  5. S2 (коммутатор)
  6. S1 (коммутатор)
  7. Linksys (беспроводной маршрутизатор)
  8. Модем

Итого: 8 промежуточных устройств.

**Сколько промежуточных устройств являются маршрутизаторами?**

* Маршрутизаторы:
  1. R4
  2. R2
  3. Linksys

Итого: 3 маршрутизатора.

**Сколько оконечных устройств не являются настольными компьютерами?**

Оконечные устройства, не являющиеся настольными компьютерами:

* 1. Home Laptop
  2. Струйный принтер
  3. Планшетный ПК
  4. Сервер филиала
  5. Лазерный принтер
  6. Смартфон
  7. Гостевое устройство
  8. IP-телефон 0
  9. IP-телефон 1

Итого: 9 оконечных устройств, не являющихся настольными компьютерами.

**Сколько типов соединений используются в этой топологии сети?**

* Типы соединений:
  1. Проводное подключение (Ethernet) — зеленые линии.
  2. Беспроводное подключение (Wireless) — пунктирные зеленые линии.
  3. Интернет/внешнее подключение (WAN/Internet) — синие и красные линии.

Итого: 3 типа соединений.

**Почему в категории «Connections» нет значка соединения для беспроводной сети?**

Беспроводные соединения обычно автоматически управляются через устройства, такие как беспроводные маршрутизаторы и точки доступа, и не требуют отдельного физического подключения в Packet Tracer.

**В программе Packet Tracer устройство Server-PT может выступать в роли сервера. Настольные и портативные компьютеры не могут быть серверами. Справедливо ли это утверждение в реальном мире?**

Это утверждение не совсем справедливо в реальном мире. В реальных сетях настольные и портативные компьютеры могут выступать в роли серверов, хотя и не так часто, как специализированные серверные машины. В зависимости от задач и нагрузки, любой компьютер, способный обрабатывать запросы клиентов, может стать сервером. Однако специализированные серверы, такие как серверы с поддержкой серверного оборудования (с большим объемом памяти, высокопроизводительными процессорами и системами хранения данных), обычно лучше подходят для работы в режиме сервера благодаря своей надежности и мощности.

Модель «клиент-сервер» предполагает взаимодействие двух типов устройств:

- Сервер — это устройство или программа, предоставляющая услуги или ресурсы (например, файлы, приложения, базы данных) клиентам.

- Клиент — это устройство, которое отправляет запросы на сервер, чтобы получить доступ к услугам или данным, которые сервер предоставляет.

**Назовите минимум два промежуточных устройства.**

1. Маршрутизатор (Router) — передает данные между сетями, направляя трафик на основе IP-адресов.

2. Коммутатор (Switch) — управляет передачей данных внутри одной локальной сети (LAN), используя MAC-адреса для передачи данных между устройствами.

**Назовите минимум два критерия для выбора типа среды передачи данных.**

1. Пропускная способность — способность среды передачи поддерживать высокие скорости передачи данных.

2. Расстояние передачи — максимальная длина кабеля или дальность беспроводного сигнала, которую может поддерживать среда передачи без потери сигнала.

**Сравните и сопоставьте локальные и глобальные сети.**

Объясните различия между локальной и глобальной сетью. Приведите примеры каждой из сетей.

1. Локальная сеть (LAN) — это сеть, которая охватывает небольшую географическую область, например, офис, дом или школу. Она используется для соединения устройств внутри одной организации или здания. Пример: сеть внутри офиса с подключением компьютеров, серверов и принтеров.

2. Глобальная сеть (WAN) — это сеть, охватывающая большие географические расстояния, соединяя несколько локальных сетей. WAN может включать городские, региональные и международные соединения. Пример: Интернет или частная корпоративная сеть, объединяющая офисы компании в разных странах.

**Сколько глобальных сетей представлено в сети программы Packet Tracer?**

1. В представленной сети Packet Tracer показана одна глобальная сеть — это сеть Интернет (облако "Интернет").

**Сколько представлено локальных сетей?**

В топологии Packet Tracer показаны три локальные сети (LAN):

1. Home Office (домашний офис)

2. Central (центральный офис)

3. Branch (филиал).

**Интернет в этой сети Packet Tracer значительно упрощён и не отражает структуру и форму реального Интернета. Дайте краткое описание сети Интернет.**

Интернет — это глобальная сеть, соединяющая миллионы компьютеров и устройств по всему миру с использованием единого набора протоколов (TCP/IP). Интернет объединяет множество различных сетей (локальных и глобальных) через маршрутизаторы и коммутаторы, предоставляя возможность обмена данными, доступ к веб-сайтам, электронной почте, приложениям и другим услугам. Основные компоненты Интернета включают:

- Провайдеры интернет-услуг (ISP),

- Магистральные сети,

- Дата-центры и серверные фермы.

**Перечислите несколько распространённых способов подключения домашних пользователей к Интернету.**

1. DSL (Цифровая абонентская линия)

2. Кабельный Интернет

3. Оптоволоконное подключение

4. Мобильные сети 4G/5G

5. Спутниковый Интернет

**Перечислите несколько распространённых методов подключения предприятий к Интернету в вашем регионе.**

1. Оптоволоконное подключение (самый распространённый и быстрый вариант для предприятий).

2. Ethernet через MPLS (для крупных компаний с удалёнными офисами).

3. DSL или кабельное подключение (для небольших и средних предприятий).

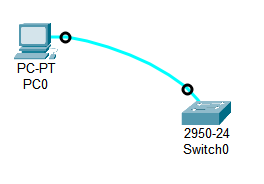
4. Мобильные сети 4G/5G (для удалённых офисов или резервного подключения).

5. Спутниковое подключение (для предприятий в удалённых районах).

**3.2. Режимы работы и структура команд интерфейса командной строки CLI.**

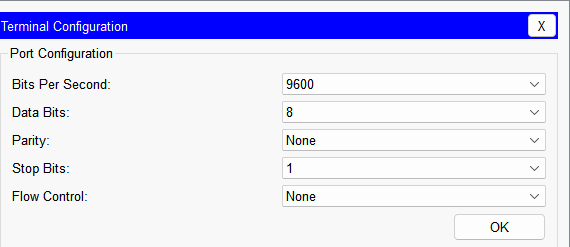
**(выполнять в Cisco Packet Tracer 6.0.1 или старше)**

1. Создайте новый файл.
2. Переключитесь на вкладку логического представления (Logical)
3. На рабочую область из нижней левой вкладки «конечные устройства» поместите ПК **(End Devices > PC-PT).** Кликнув на ПК, выберете вкладку **«Desktop»\ «IP Configuration».** Установите в качестве IP адреса 192.168.10.5, в качестве маски подсети 255. 255. 255.0, в качестве шлюза по умолчанию 192.168.10.1
4. На рабочую область из нижней левой вкладки «Коммутаторы» поместите коммутатор 2950-24 (Switches > 2950-24).
5. Подключите ПК к коммутатору с помощью консольного кабеля
6. Щёлкните значок **Connections (Соединения)** (в виде молнии) в левом нижнем углу окна Packet Tracer.
7. Выберите светло-голубой консольный кабель, щёлкнув по нему. Указатель мыши примет вид разъёма со свисающим концом кабеля.
8. Щёлкните на ПК. В окне будет показан вариант для подключения RS-232.
9. Перетащите другой конец консольного подключения к коммутатору и щёлкните коммутатор, чтобы открыть список подключений.
10. Выберите консольный порт, чтобы завершить подключение.

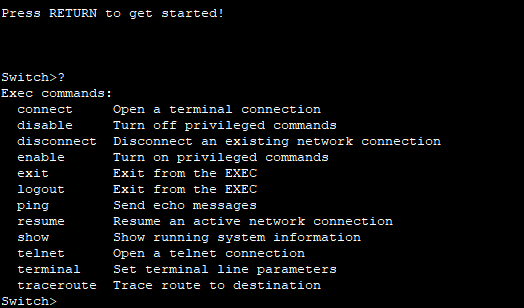


11. Установите сеанс терминальной связи с коммутатором S1

* Щёлкните на ПК и откройте вкладку **Desktop (Рабочий стол).**
* Щёлкните значок приложения **Terminal**. Проверьте правильность параметров по умолчанию, установленных для порта. Каково значение параметра в битах в секунду?



* Нажмите кнопку OK.
* В появившемся окне может быть показано несколько сообщений. В какой-либо части окна должно появиться сообщение Press RETURN to get started! (Нажмите клавишу ВВОД, чтобы начать работу). Нажмите клавишу ВВОД. Какое приглашение показано на экране?



**Изучение справки по IOS.**

В IOS доступна справка по командам в зависимости от уровня работы. В данный момент отображается приглашение, называемое Пользовательским режимом, и устройство ожидает ввода команд. Самый простой способ вызова справки — ввести вопросительный знак (?) в приглашении, чтобы получить список команд.

**S1> ?**

Какая команда начинается с буквы «c»?

**connect**

В командной строке введите **t** с вопросительным знаком в конце (?).

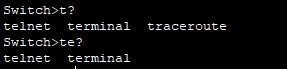
**S1> t?**

Какие отображаются команды?

В командной строке введите **te** с вопросительным знаком в конце (?).

**S1> te?**

Какие отображаются команды?



Такой тип справки называется контекстной; в ней предоставляются дополнительные сведения при расширении команд.

Войдите в привилегированный режим.

В командной строке введите вопросительный знак **(?).**

**S1> ?**

Какие из показанных данных описывают команду **enable**?

Введите en и нажмите клавишу TAB.

**S1> en<Tab>**

Что отображается после нажатия клавиши TAB?

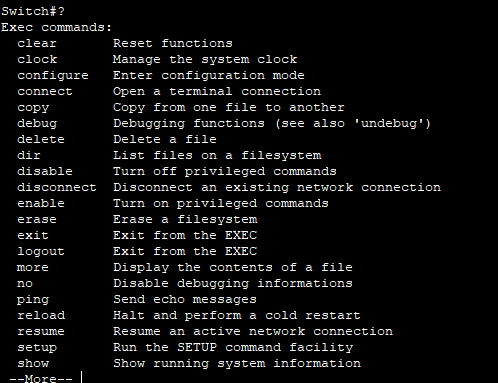
Это называется завершением команды или завершением клавишей TAB. После ввода части команды с помощью клавиши TAB можно завершить ввод этой команды. Если введённых символов достаточно для уникального определения команды (например, как в случае с командой enable), оставшаяся часть будет введена автоматически.  Что произойдёт, если ввести **te<Tab>** в командной строке?

**te вывело**

Введите команду **enable** и нажмите клавишу ВВОД. Как изменилась строка приглашения?



Введите в строке вопросительный знак (?).



**Переход в режим глобальной конфигурации.**

Одной из команд, доступных в привилегированном режиме и начинающихся с буквы «c», является **configure**. Введите команду полностью или только её часть, достаточную для завершения, клавишей TAB, а затем нажмите клавишу ВВОД.

**S1# configure**

Какое отобразилось сообщение?



Нажмите клавишу ВВОД, чтобы принять параметр по умолчанию, заключённый в квадратные скобки **[terminal].**

Как изменилась строка приглашения?



Такой режим называется режимом глобальной конфигурации. А теперь вернитесь в привилегированный режим, введя команду exit или end, либо нажав сочетание клавиш Ctrl-Z.

**Настройка часов**

Используйте команду **clock**, чтобы подробнее изучить справку и синтаксис команды. Введите **show** **clock** в привилегированном режиме.

**S1# show clock**

Какая информация отображается? Какой год отображается?



Используйте контекстную справку и команду **clock**, чтобы установить текущее время на коммутаторе. Введите команду **clock** и нажмите клавишу ВВОД.

**S1# clock<ENTER>**



IOS выдала сообщение **% Incomplete command**, которое означает, что для команды **clock** требуются дополнительные параметры. В справке можно получить дополнительные сведения о времени, если ввести после команды пробел и вопросительный знак (?).

**S1# clock ?**

Какая информация отображается?



Настройте время с помощью команды **clock**. Продолжайте изучение команды, выполняя по одному действию за один раз.

**S1# clock set ?**

Какая запрашивается информация?



Какие отобразятся сведения, если ввести только команду **clock**, не выполняя запрос справки с помощью вопросительного знака?

**incomplite**

На основе данных, запрошенных с помощью команды clock set ?, введите время 15:00, используя 24-часовой формат. Проверьте, нужны ли дополнительные параметры.

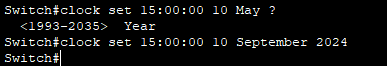
**S1# clock set 15:00:00 ?**

Выходные данные содержат запрос на получение дополнительных сведений:

**<1-31>  Day of the month**

**MONTH   Month of the year**

Попробуйте установить сегодняшнюю дату и время

****

**Изучение дополнительных сообщений команд.**

IOS выводит различные данные для неправильных или неполных команд, в чём можно было убедиться в предыдущих разделах. Продолжайте работать с командой clock, чтобы изучить дополнительные сообщения, которые могут появиться в ходе обучения работы с IOS.

Введите следующую команду и запишите сообщение:

**S1# cl**

Какие возвращены данные?



**S1# clock**

Какие возвращены данные?

**S1# clock set 25:00:00**

Какие возвращены данные?



**S1# clock set 15:00:00 32**

Какие возвращены данные?

**Invalid input**

**3.3. Установка первоначальных настроек безопасности в интерфейсе командной строки CLI**

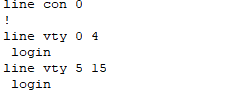
Откройте файл «2.2.3.3 Packet Tracer - Configuring Initial Switch Settings.pka» и выполните задания, представленные в файле.

**Ответьте на следующие вопросы.**

1. Сколько у маршрутизатора интерфейсов FastEthernet? --- 24

2. Сколько у маршрутизатора интерфейсов Gigabit Ethernet? --- 2

Каков диапазон значений, отображаемых в vty-линиях?



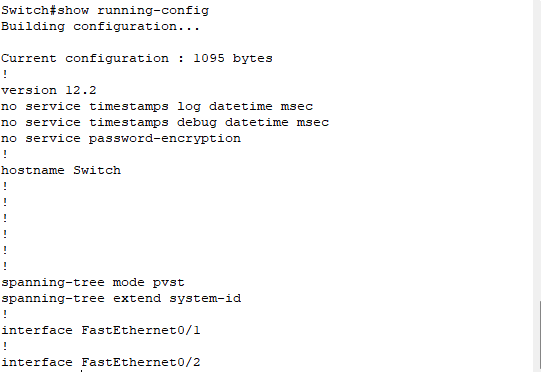
3. Какая команда отображает текущее содержимое NVRAM?

Команда для отображения текущего содержимого NVRAM на коммутаторе — это:

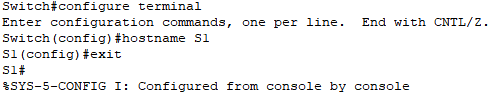
show startup-config

4. Почему коммутатор отвечает сообщением startup-config is not present?

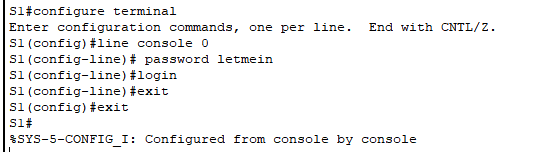
Сообщение **"startup-config is not present"** указывает на то, что в NVRAM (Non-Volatile RAM) коммутатора не сохранена стартовая конфигурация.



**Шаг 1.**   **Задайте коммутатору имя.**



**Шаг 2.**   **Защитите доступ к консоли.**



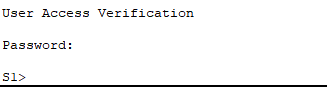
Команда **login** используется для включения аутентификации на консоли коммутатора или маршрутизатора. Без этой команды пароль, заданный с помощью команды **password**, не будет запрашиваться при подключении к консоли.

После выполнения команды:

1. **password letmein** — задается пароль для консольного доступа.
2. **login** — активирует запрос пароля при попытке доступа к консоли.

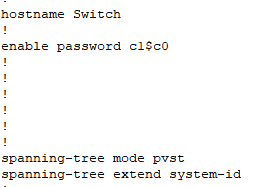
Это означает, что в следующий раз, когда кто-то попытается подключиться к консоли, система запросит ввод пароля **letmein**.

**Шаг 3.**   **Убедитесь, что доступ к консоли защищён.**



**Поверьте на слово что я это сделала**

**Шаг 4.**   **Защитите доступ в привилегированный режим.**

****

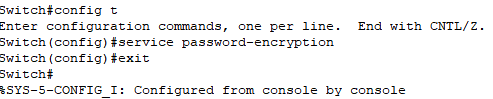
Что отображается при выводе пароля **enable secret**?

****

 Почему пароль **enable secret** отображается не так, как он был настроен? --- зашифрован

**Шаг 5.**  **Зашифруйте пароли enable и console.**

Пароли на коммутаторе могут храниться как в виде обычного текста, так и в зашифрованном виде, в зависимости от того, как они были настроены и какие команды использовались.

****

**Баннер MOTD**

В каких случаях будет отображаться этот баннер?

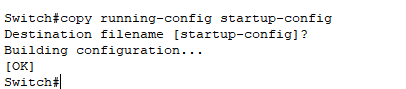
**Случаи отображения баннера:**

1. При **подключении к коммутатору через консоль**.
2. При **удалённом подключении** (например, через Telnet или SSH).
3. При **перезапуске** или перезагрузке устройства.

Для чего на всех коммутаторах настраивается баннер MOTD?

Баннер **MOTD (Message of the Day)** отображается всякий раз, когда кто-либо подключается к коммутатору через консольный порт, VTY (виртуальные терминальные линии), или по другим методам удаленного доступа (например, через Telnet или SSH). Он выводится **до** запроса ввода имени пользователя или пароля.

Сохранить в NVRAM



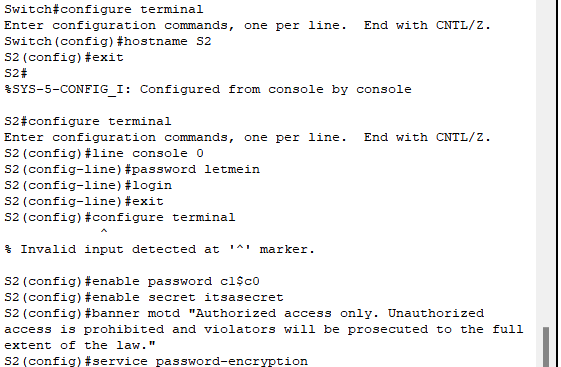
Какова самая короткая версия команды **copy running-config startup-config**? copy run start

Какая команда отображает содержимое NVRAM? show startup-config

Были ли все изменения записаны в файл?

Чтобы убедиться, что все внесённые изменения были записаны в файл конфигурации, вы можете сравнить **текущую конфигурацию** (running-config), которая находится в оперативной памяти, с **стартовой конфигурацией** (startup-config), которая хранится в NVRAM.

**Настройка коммутатора S2**



**3.4 Реализация базовой схемы подключения**

Откройте файл " 2.3.2.5 Packet Tracer - Implementing Basic Connectivity.pka " и выполните указанные задания

**Настройка основных параметров на коммутаторах S1 и S2**

Выполните следующие действия на коммутаторах S1 и S2.

**Шаг 1. Задайте коммутатору S1 имя узла.**

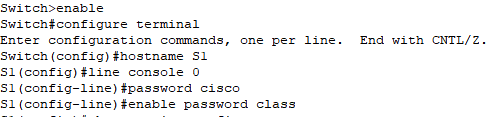
a.   Нажмите **S1** и откройте вкладку**CLI**.

b.   Введите соответствующую команду для настройки имени узла **S1**.

**Шаг 2. Настройте пароли для консоли и привилегированного режима.**

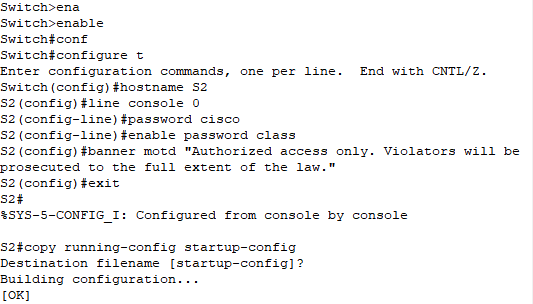
a.   В качестве пароля консоли введите **cisco**.

b.   В качестве пароля привилегированного режима введите **class**.

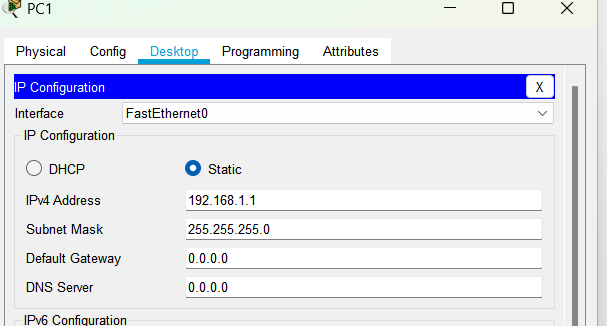


Добавила сообщение дня и сохранила nvram

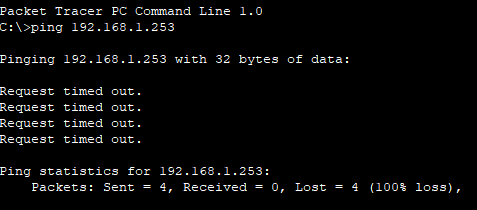
Тоже самое для второго коммутатора



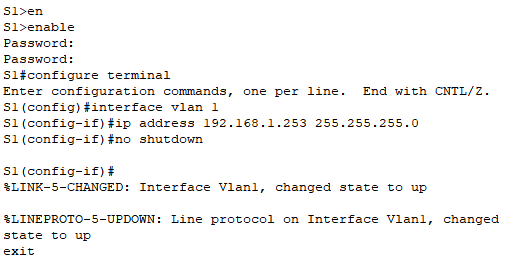
**Настройте IP-адреса на обоих ПК.**



Успешно ли был обработан эхо-запрос? Поясните свой ответ.



Настройка айпи коммутатора s1

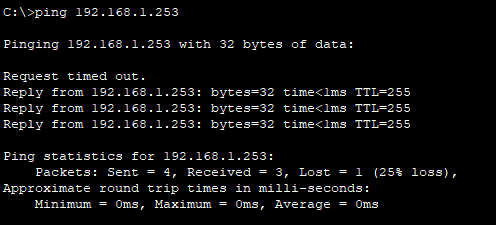


**По умолчанию интерфейсы выключены**: После создания нового интерфейса (например, на маршрутизаторе или VLAN-интерфейсе на коммутаторе) или при инициализации устройства, большинство интерфейсов находится в состоянии **shutdown** (выключены). Это делается для того, чтобы предотвратить незапланированную активность на неиспользуемых портах.

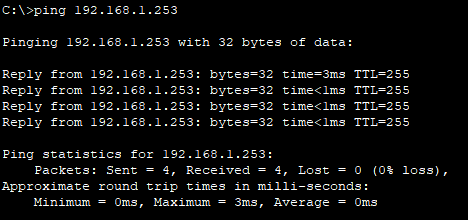
**Активация порта или интерфейса**: Чтобы интерфейс стал активным и начал передавать данные, необходимо вручную активировать его.

Настроила теперь получила пинг

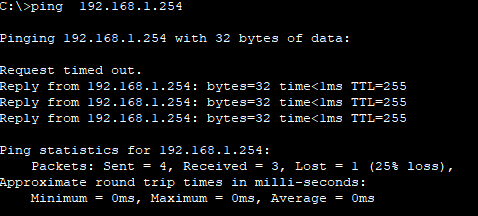
PC1



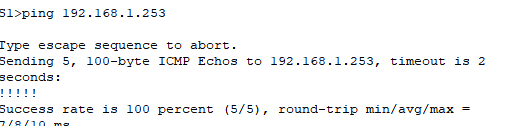
Вторая попытка



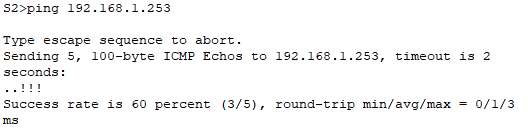
PC2



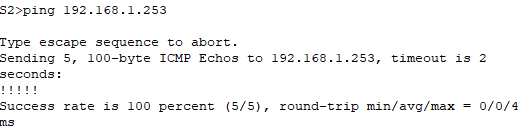
S1



S2



Вторая попытка



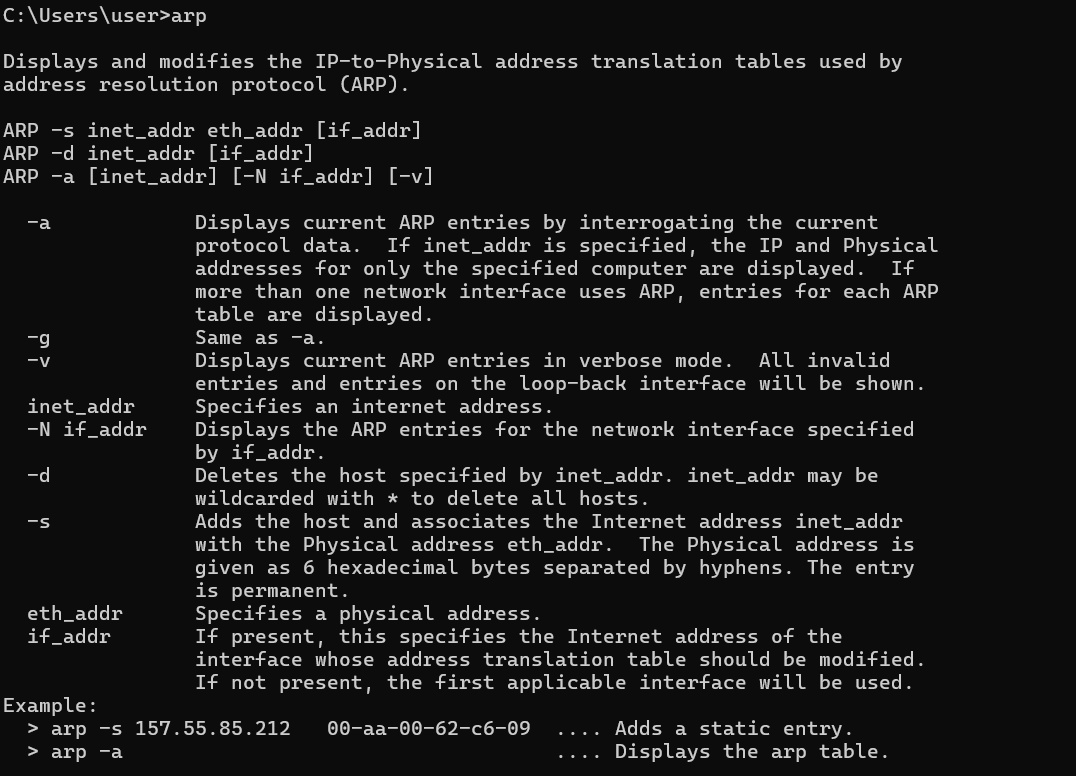
**3.5 Просмотр ARP с помощью интерфейса командной строки Windows и Wireshark**

Команда **arp** позволяет пользователю просматривать и изменять ARP-кэш в ОС Windows. Команда вводится в командную строку Windows.

**Отобразите ARP-кэш.**

1. Откройте окно командной строки на ПК-А и введите **arp**.

C:\Users\User1> **arp**



**Изучите выходные данные.**

Какая команда позволяет отобразить все записи в ARP-кэше?

**arp -a**

Какая команда позволяет удалить все записи в ARP-кэше (очистить ARP-кэш)?

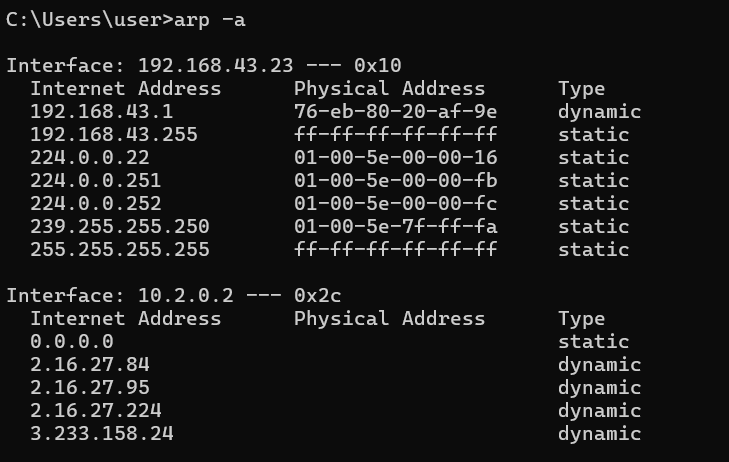
**arp -d \***

Какая команда позволяет удалить все записи в ARP-кэше для 192.168.1.11?

**arp -d 192.168.1.11**

**Введите arp -a, чтобы отобразить таблицу ARP.**

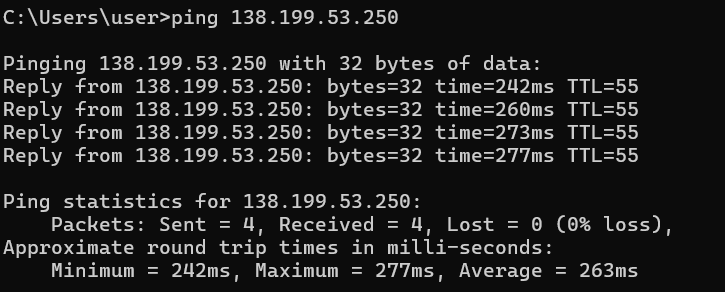
C:\Users\User1> **arp –a**



**Отправьте эхо-запрос с помощью команды ping с вашего ПК на ПК другого учащегося для динамического добавления записей в ARP-кэш.**

C:\Documents and Settings\User1> **ping IP-адрес устройства коллеги**

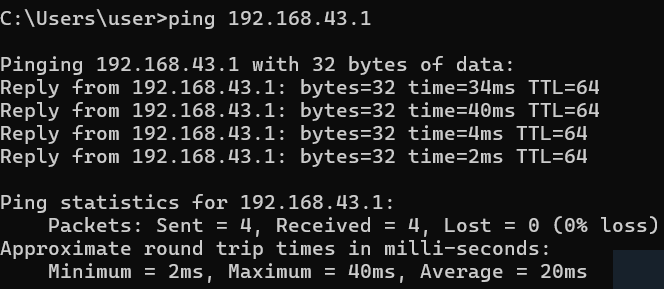
Назовите физический адрес узла с IP-адресом



**Шаг 2. Настройте записи в ARP-кэш вручную.**

Чтобы удалить записи из ARP-кэша, выполните команду **arp –d {inet- addr | \*}**. Можно удалить адреса по отдельности, указав соответствующие IP-адреса, либо стереть сразу все записи с помощью подстановочного символа **\***.

С вашего ПК отправьте эхо-запросы с помощью команды ping на все адрес другого учащегося и на адрес шлюза по умолчанию.



В окне командной строки администратора введите **arp –d \***. Эта команда удалит все записи из ARP-кэша. Убедитесь в том, что все записи из ARP-кэша удалены. Для этого в командной строке введите **arp –a**.

C:\windows\system32> **arp –d \* (почему то не сработало)**

**Часть 2. Анализ обмена сообщениями ARP с помощью программы Wireshark**

В части 2 вам предстоит изучить обмен сообщениями ARP, используя программу Wireshark для их захвата и оценки. Кроме того, вы проанализируете задержки сети, вызванные обменом сообщениями ARP между устройствами.

1. **Настройте программу Wireshark для захвата пакетов.**
2. Запустите программу Wireshark.
3. Выберите сетевой интерфейс, который будете использовать для захвата сообщений ARP.

**Шаг 2: Захватите и оцените сообщения ARP.**

1) Начните захват пакетов в программе Wireshark. С помощью фильтра отобразите только пакеты ARP.

* Очистите ARP-кэш, набрав в командной строке команду **arp –d \***.
* Убедитесь в том, что ARP-кэш очищен.
* Отправьте эхо-запрос с помощью команды ping на шлюз по умолчанию с помощью команды **ping IP-адрес шлюза по умолчанию.**
* После отправки эхо-запроса на шлюз по умолчанию остановите захват данных программой Wireshark.
* В захваченных данных найдите сообщения ARP в панели сведений о пакетах.

Какой пакет ARP был первым?  ARP-запрос

Заполните приведённую ниже таблицу данными первого захваченного пакета ARP.

|  |  |
| --- | --- |
| **Поле** | **Значение** |
| **MAC-адрес отправителя** |  |
| **IP-адрес отправителя** | 192.168.43.1 |
| **MAC-адрес назначения** |  |
| **IP-адрес назначения** | 192.168.43.23 |

Какой пакет ARP был вторым?

Заполните приведённую ниже таблицу данными второго захваченного пакета ARP.

|  |  |
| --- | --- |
| **Поле** | **Значение** |
| **MAC-адрес отправителя** |  |
| **IP-адрес отправителя** | 192.168.43.23 |
| **MAC-адрес назначения** |  |
| **IP-адрес назначения** | 192.168.43.1 |

**Шаг 3: Проанализируйте задержки сети, вызванные ARP.**

1. Очистите записи ARP на своем ПК

2. Начните захват данных программой Wireshark.

3. Отправьте эхо-запрос с помощью команды ping на шлюз по умолчанию и на ПК другого учащегося.

C:\Users\User1> **ping IP-адрес другого устройства**

Approximate round trip times in milli-seconds:

    Minimum = 1ms, Maximum = 3ms, Average = 2ms

* После отправления эхо-запросов с помощью команды ping остановите захват данных программой Wireshark. С помощью фильтра отобразите только данные ARP и ICMP. В поле **Filter:** (Фильтр) программы Wireshark введите **arp** или **icmp**.
* Изучите захваченные данные. Как показано в захвате данных Wireshark, ARP — это яркий пример компромисса производительности. При отсутствии кэша протокол ARP должен непрерывно запрашивать трансляцию адресов каждый раз при помещении кадра в сеть. В этом случае для установления связи прибавляется время ожидания, что может вызвать перегрузку локальной сети.

1. **Вопросы на закрепление**

1. Как и когда удаляются статические записи ARP?

Статические записи ARP не удаляются автоматически, в отличие от динамических записей, которые имеют ограниченное время жизни (TTL). Статические записи остаются в кэше ARP до тех пор, пока не будут вручную удалены администратором или пока устройство не будет перезагружено. В некоторых системах также может быть возможность удалить статические записи при изменении конфигурации сети.

2. Зачем добавить статические записи ARP в кэш?

Статические записи ARP добавляются в кэш для повышения производительности и снижения нагрузки на сеть. Они позволяют избежать необходимости отправки ARP-запросов для устройств с известными MAC-адресами, что уменьшает количество сетевого трафика и задержки. Это особенно полезно в стабильных сетях, где адреса устройств не меняются.

3. Если ARP-запросы способны вызывать задержки сети, почему не рекомендуется снимать ограничения на время ожидания отклика для записей ARP?

Снятие ограничений на время ожидания отклика для записей ARP может привести к проблемам с актуальностью данных в кэше. Если записи остаются слишком долго, это может привести к использованию устаревшей информации о MAC-адресах, особенно если устройства перемещаются или их адреса меняются. Это, в свою очередь, может вызвать проблемы с маршрутизацией и доступностью устройств в сети. Умеренное время ожидания позволяет поддерживать кэш актуальным и минимизировать вероятность ошибок при передаче данных.

**4. Контрольные вопросы**

1. Перечислите 7 уровней модели OSI/ISO

2. Назначение каждого уровня модели OSI/ISO

3. Чем отличается две сетевые модели: OSI/ISO и стек протоколов TCP/IP

4. Логическая и физическая топология. В чем отличие?

5. Типы каналов связи

6. На какие подуровни делиться канальный уровень и за что они отвечают

7. Режимы конфигураций в Cisco IOS