

ЗНАКОМСТВО С PACKET TRACER. МОДЕЛИРОВАНИЕ ПРОСТОЙ СЕТИ

Цель работы: Требуется изучить принципы построения сетей передачи данных и принципы настройки сетевого оборудования.

Предварительные сведения. Запуск, настройка и описание интерфейса Packet Tracer

Packet Tracer – симулятор сети передачи данных, выпускаемый фирмой Cisco Systems. С помощью данного симулятора можно строить модели сетей передачи данных, изучать настройки и принципы функционирования сетевого оборудования производителя, проводить диагностику работоспособности моделируемой сети.

Для запуска Packet Tracer, установленного под ОС Linux, достаточно в командной строке терминала ввести команду:

packettracer &

или скачать на официальном сайте <https://www.netacad.com>

Рабочее пространство Packet Tracer, представлено на рис. 1.

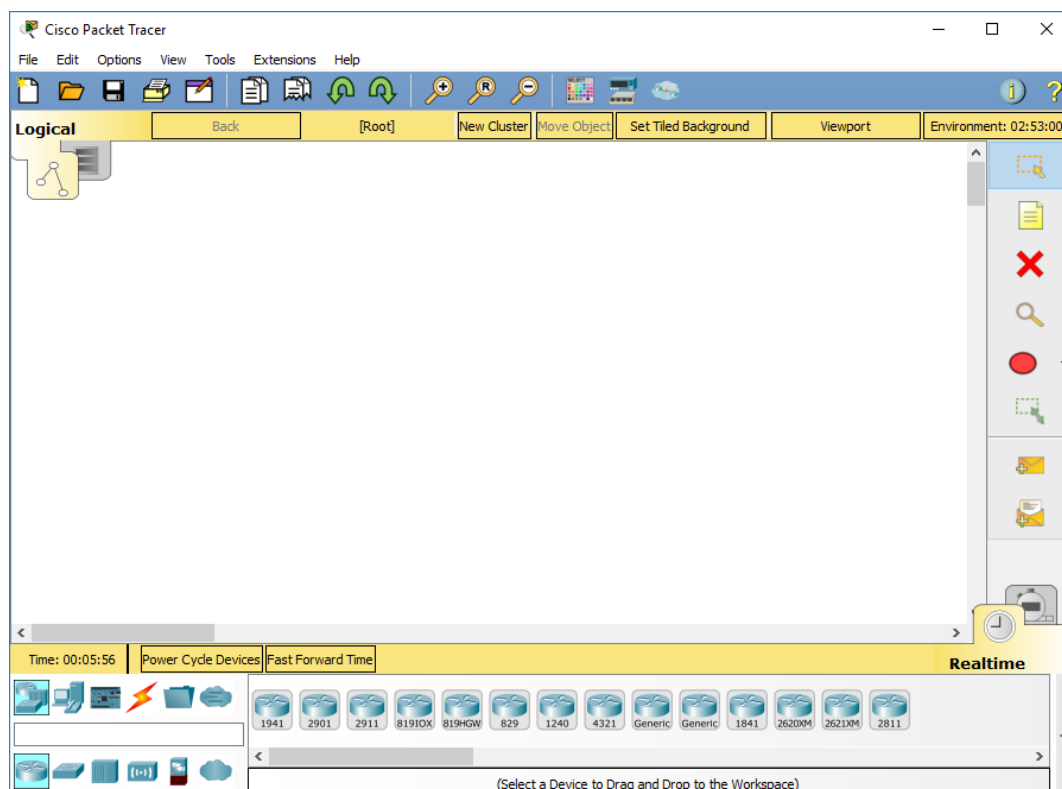


Рис. 1 – Рабочее пространство Packet Tracer

По умолчанию интерфейс Packet Tracer - английский. Для изменения его на русский необходимо в меню выбрать «Options», «Preferences», вкладку «Interface» и указать язык «RUSSIANxx.ptl», где xx обозначает версию симулятора (рис. 2). Затем нужно нажать «Change Language» и перезапустить симулятор.

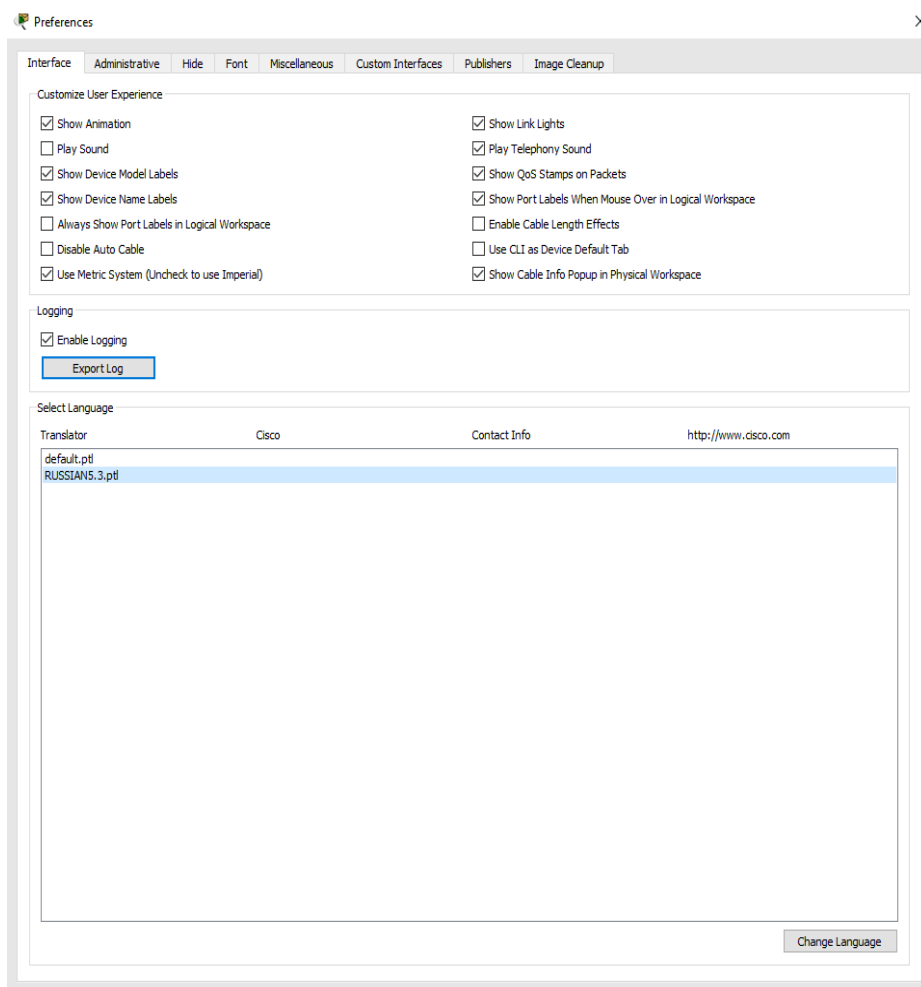


Рис. 2 – Изменение языка интерфейса Packet Tracer

Основное окно программы показано на рис. 3.

Меню (1) позволяет создать, открыть, сохранить или распечатать проект, скопировать и вставить элемент, масштабировать рабочее пространство проекта. Меню (2) содержит инструменты выделения одного или нескольких объектов проекта, прокрутки проекта, добавления подписи к элементу проекта, удаления элемента проекта. Инструмент, напоминающий лупу, используется для просмотра содержимого таблиц ARP, NAT, таблицы маршрутизации и т.д. После этого инструмента расположены инструмент изменения размеров объекта, инструменты для эмулирования отправки с последующим отслеживанием произвольного пакета данных внутри проекта.

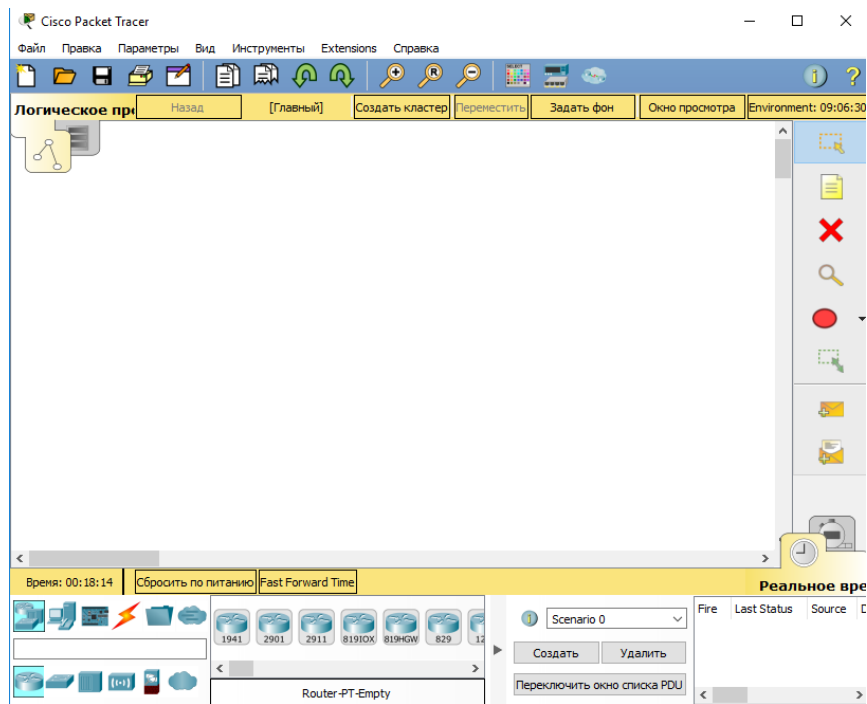


Рис. 3 – Меню Packet Tracer

В меню (3) можно выбрать тип устройства: концентратор, коммутатор, маршрутизатор, тип соединения, оконечные и пользовательские устройства. В меню (4) в зависимости от выбранного в меню (3) типа оборудования можно выбрать конкретное устройство.

Вкладка (5) позволяет переключаться с режима работы в реальном времени В режим симуляции и бывает полезна, если нужно более детально изучить, например, движение передаваемых от устройства к устройству данных, форматы конкретных пакетов.

Моделирование простейшей сети.

Протокол ICMP

Постановка задачи. Требуется построить топологию сети из двух коммутаторов и четырех пользовательских устройств (компьютеров), подсоединенных по два к каждому коммутатору. На пользовательских узлах нужно задать статическую адресацию из одного адресного пространства. Затем требуется изучить работу протокола ICMP.

Порядок выполнения работы. Создать новый проект (например, kp-01.pkt).

В рабочем пространстве разместить 2 коммутатора, например, Cisco-2960, 4 оконечных устройства (рис. 4). Подключить оконечные устройства к коммутаторам, используя прямое соединение, и коммутаторы между собой, используя кроссовое соединение.

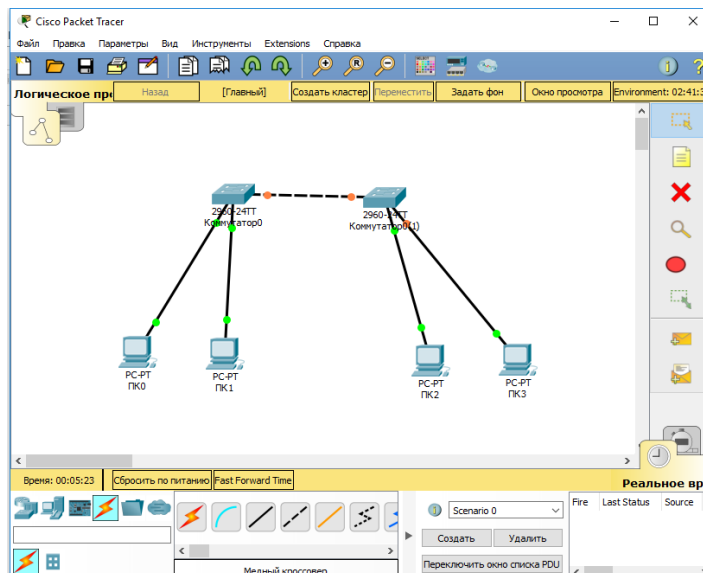


Рис. 4 – Модель простой сети

Щелкнув последовательно на каждом оконечном устройстве, задайте статический адрес из диапазона 192.168.1.2 – 192.168.1.5 (рис. 5)

На одном из оконечных устройств запустите командную строку (рис. 6) и с помощью команды `ipconfig /all` посмотрите его сетевые настройки (рис. 7). Проверьте доступность другого узла сети с помощью команды `ping`.

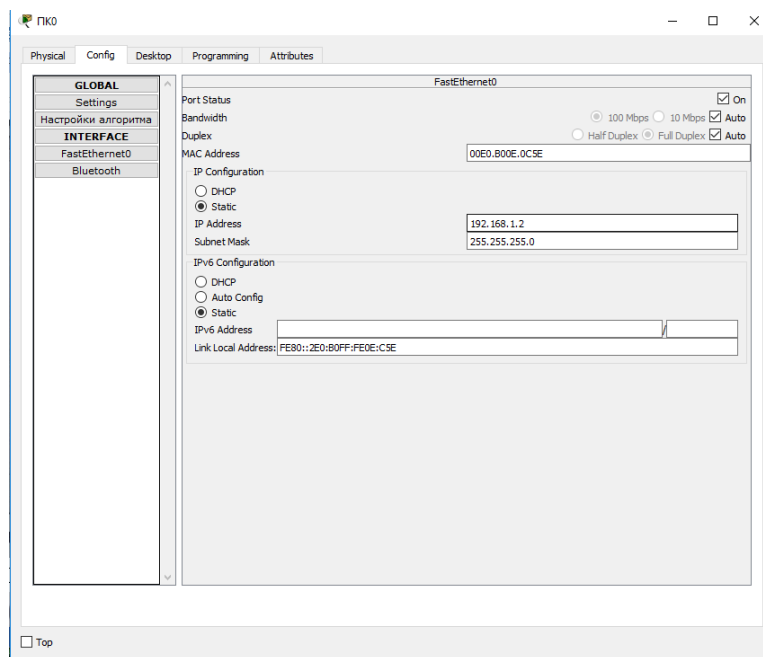


Рис. 5 – Статическая адресация на оконечном устройстве

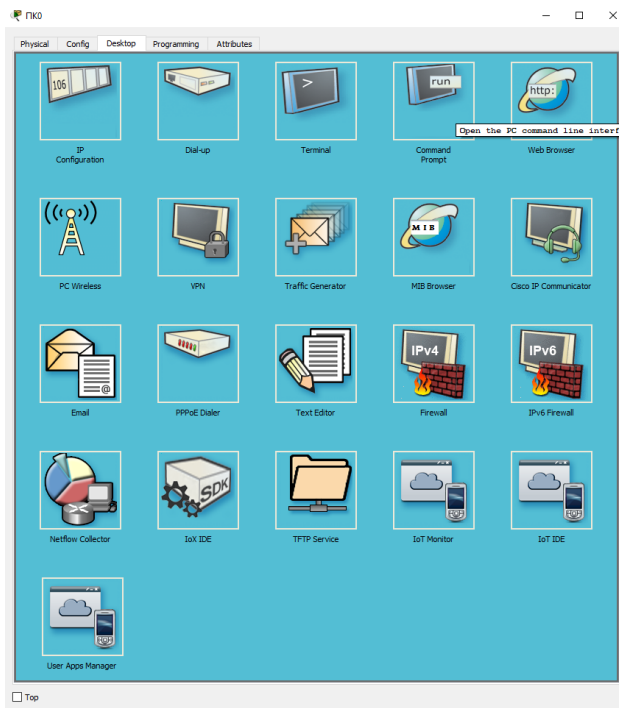


Рис. 6 – Запуск командной строки на оконечном устройстве

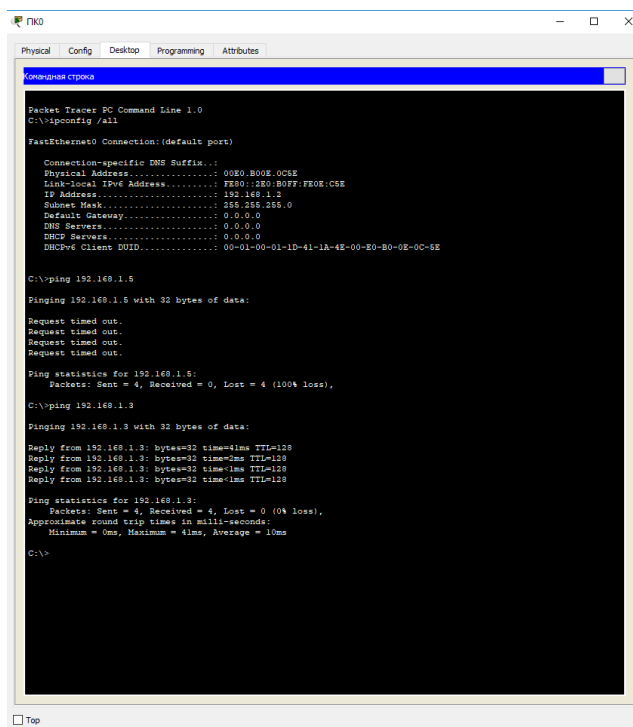


Рис. 7 – Выполнение команды ipconfig на оконечном устройстве

В основном окне проекта перейти из режима реального времени в режим симуляции. В командной строке одного из оконечных устройств повторите команду ping. С помощью кнопки «Захват/Вперед» проследите движение пакета ICMP от одного оконечного устройства к другому (рис. 8)

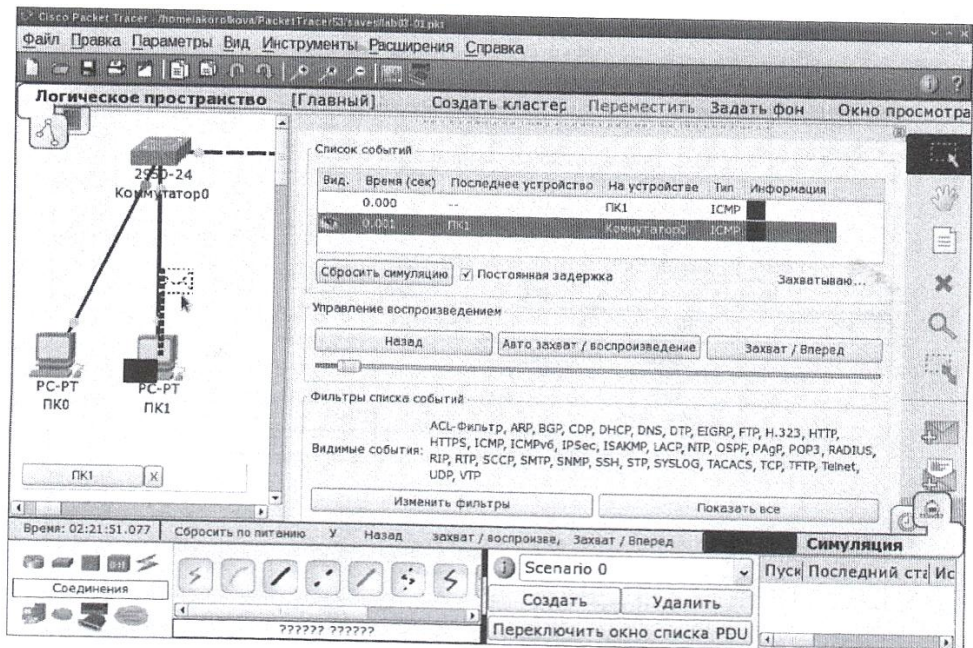


Рис. 8 – Выполнение команды ping в режиме симуляции

Щелкнув на значке пакета, откройте окно информации о PDU на устройстве и изучите его детали (рис. 9, 10). Используя кнопку «Проверить себя» ответьте на вопросы. Прodelайте эту операцию на каждом этапе следования пакета и дайте пояснения об изменениях. Изучите информацию о PDU, передаваемых между коммутаторами (рис. 11, 12). Изучите изменения формата передаваемых пакетов других протоколов по вариантам (например, telnet).

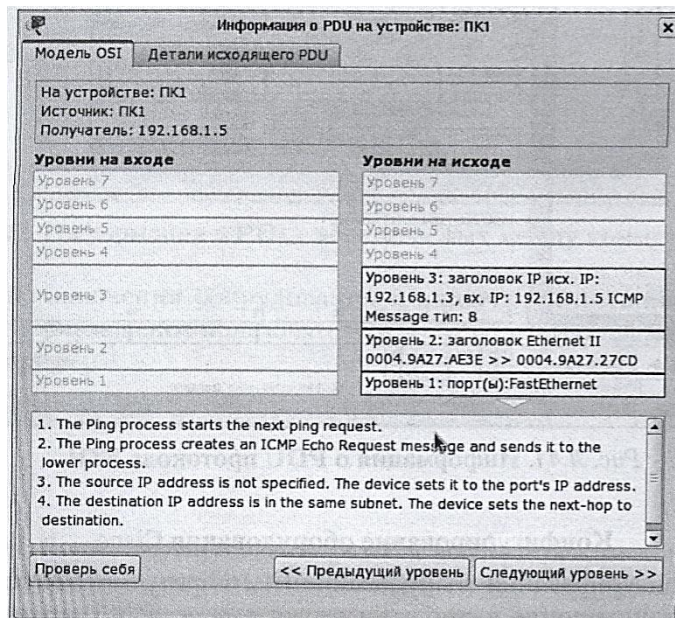


Рис. 9 – Информация о PDU: уровень OSI

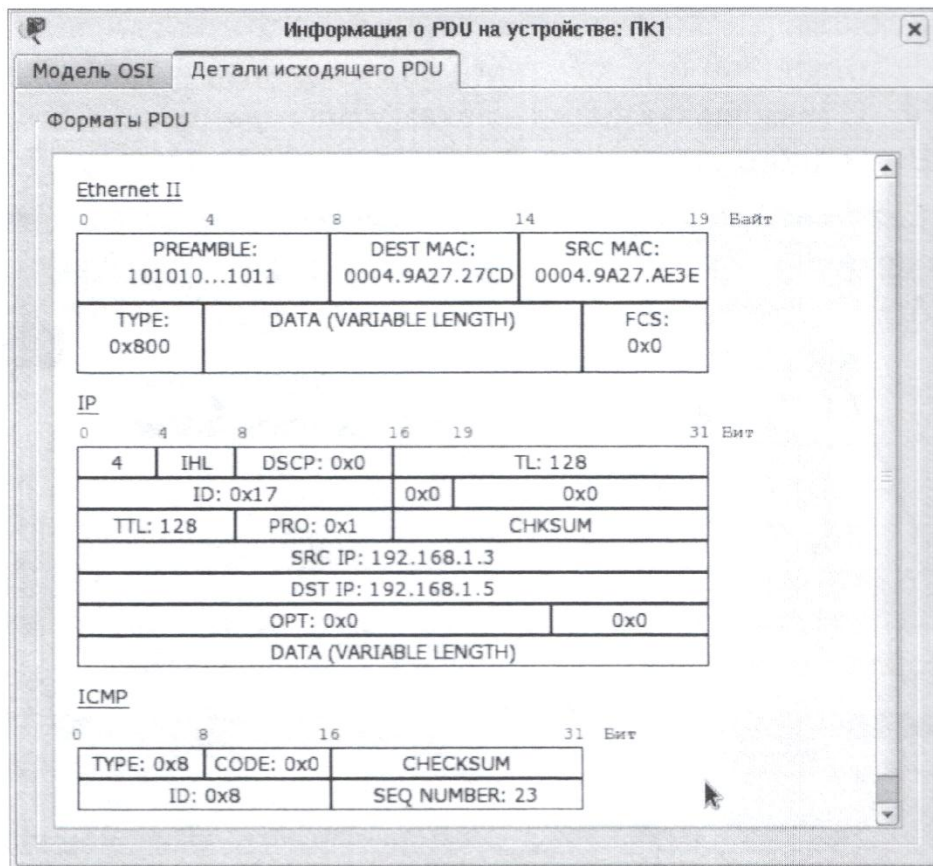


Рис. 10 – Информация о PDU: форматы пакетов

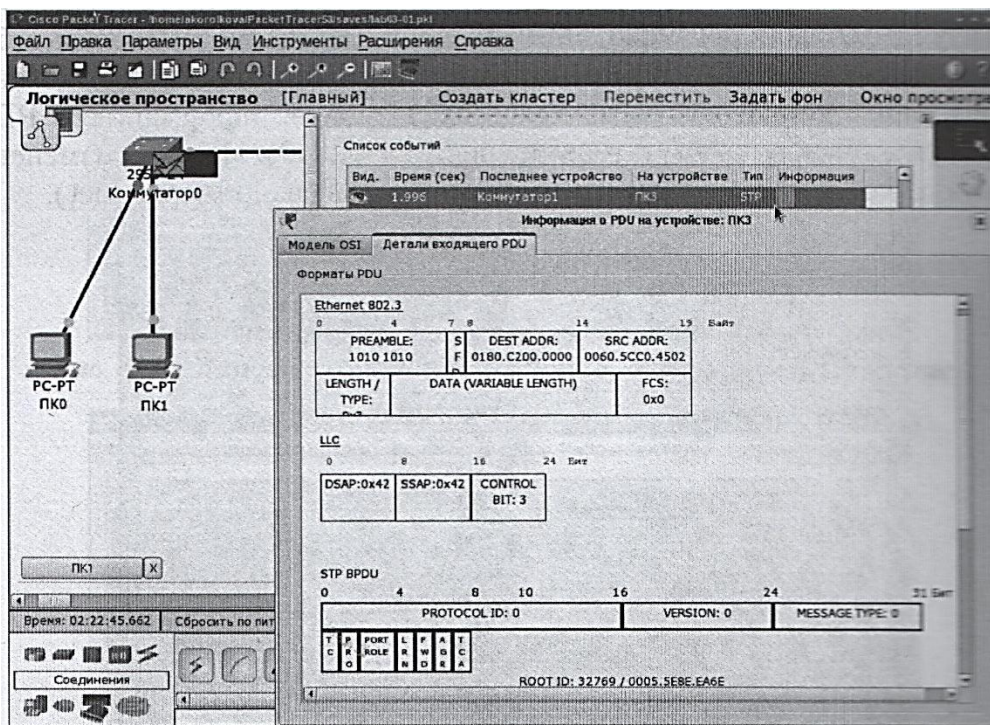


Рис. 11 – Информация о PDU протокола STP

Конфигурирование оборудования Cisco

Для конфигурирования оборудования Cisco предусмотрен консольный кабель, на одном конце которого имеется разъем RJ45, подключаемый в соответствующий порт на оборудовании Cisco, а на другом — RS-232, подключаемый к COM-порту компьютера, с которым будет производиться настройка. Для управления через COM-порт в системах Windows можно использовать HyperTerminal, а в Linux, например, minicom.

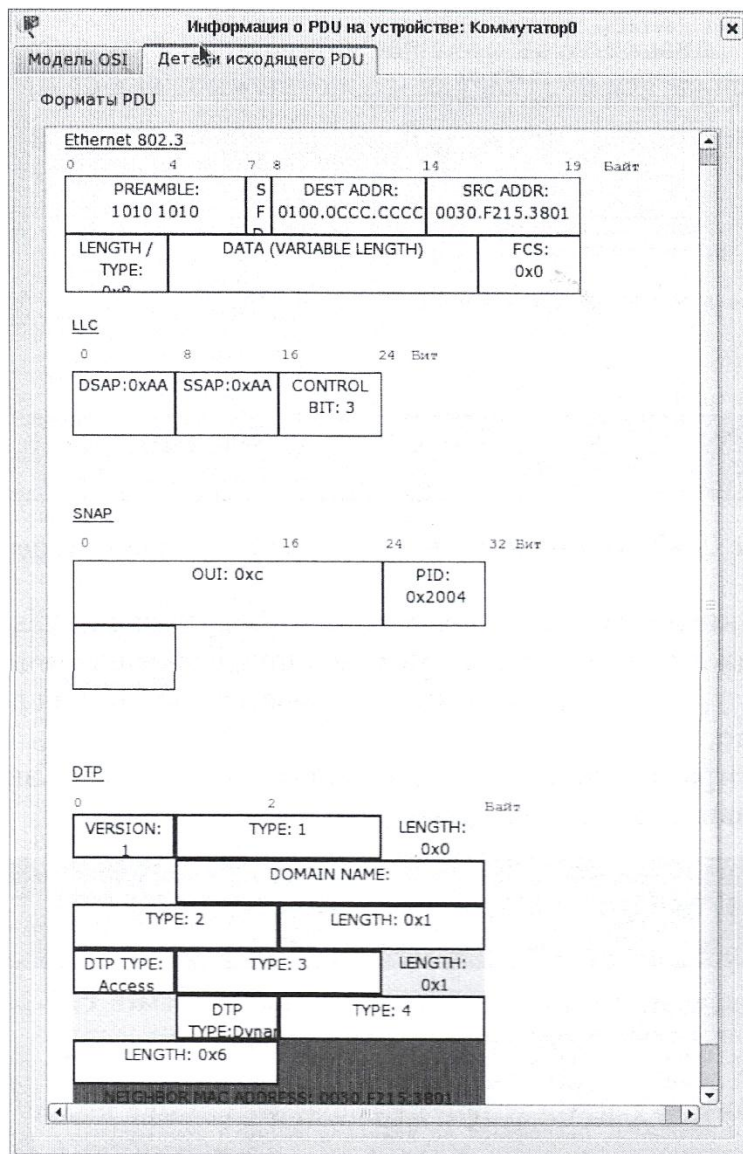


Рис. 12 – Информация о PDU, передаваемых между коммутаторами

После подключения оборудования и включения питания на экране пользовательского режима (отображается символом >), например

Router>

или

Switch>

В Packet Tracer соответственно, чтобы войти в режим конфигурирования оборудования, необходимо разместить это оборудование в рабочем пространстве, щелкнуть на нем и перейти на вкладку CLI (рис. 13) командного интерфейса IOS (Internetwork Operating System).

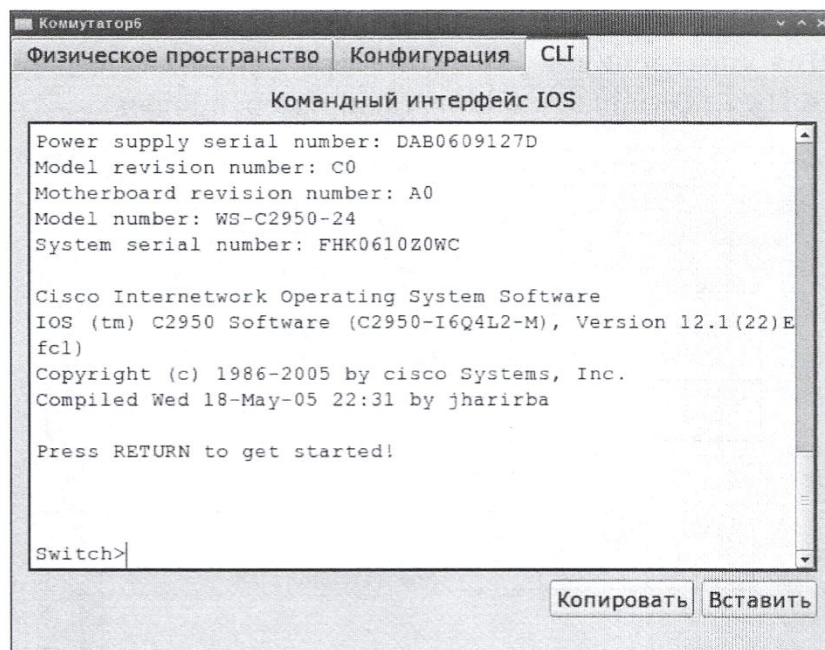


Рис. 13 – Командный интерфейс ISO в Packet Tracer

Основные команды конфигурирования оборудования Cisco. Пользовательский режим на оборудовании Cisco предназначен только для просмотра конфигурации устройства и ввода простейших команд диагностики, например ping.

Для просмотра доступных команд используется команда «?» знака вопроса и нажатие клавиши Enter (рис. 14).

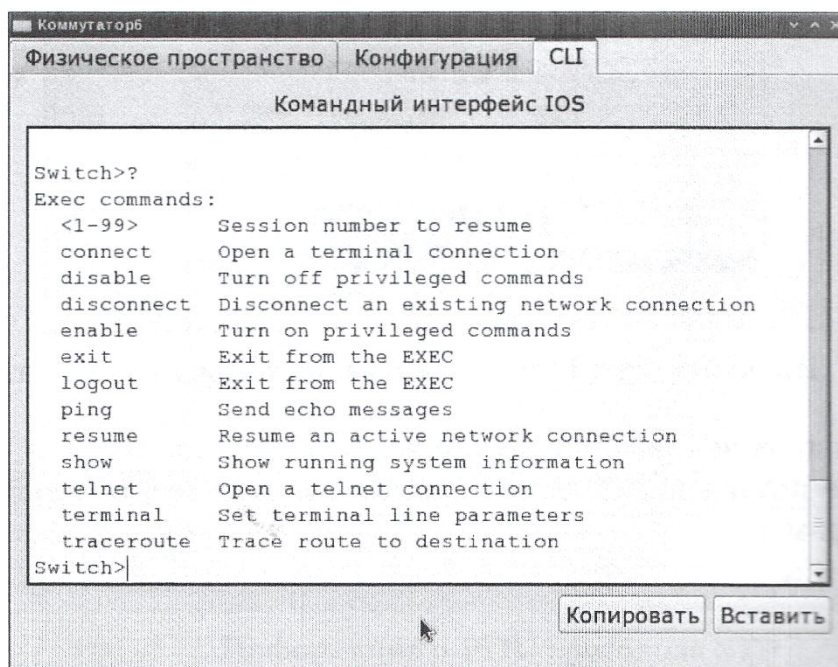


Рис. 14 – Вызов списка команд, доступных в пользовательском режиме

Чтобы перейти в привилегированный режим и иметь возможность настраивать оборудование, вводится команда *enable* и приглашение заменяется на #, например:

Router#

или

Switch#

Список доступных в привилегированном режиме команд продемонстрирован на рис. 15 для коммутаторов и на рис. 16 для маршрутизаторов.

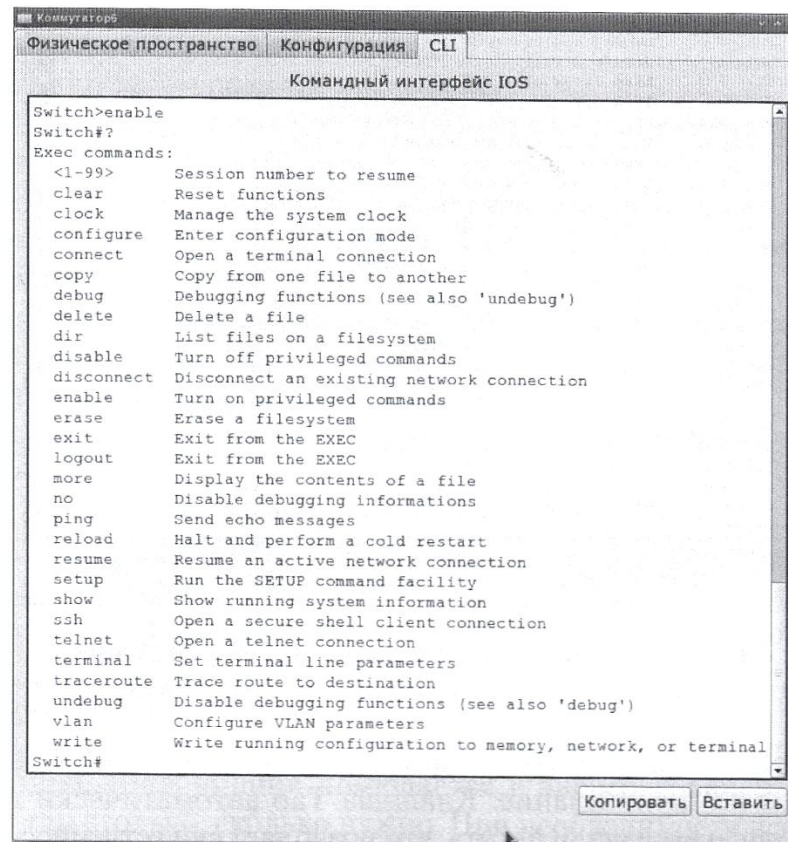


Рис. 15 – Вызов списка команд коммутаторов, доступных в привилегированном режиме

Для упрощения администрирования в устройствах Cisco) применяется концепция VLAN-доменов.

VLAN (Virtual Local Area Network) – логическая («виртуальная») локальная компьютерная сеть, представляющая собой группу хостов с общим набором требований, которые взаимодействуют так, как если бы они были подключены к широковещательному домену, независимо от их физического местонахождения.

VLAN можно назначить:

- определенному порту устройства;
- определенному MAC-адресу;
- определенному протоколу;
- по данным аутентификации пользователя или устройства.

По умолчанию на каждом порту устройства Cisco имеется сеть VLAN1 или VLAN управления. Сеть управления не может быть удалена, однако могут быть созданы дополнительные сети VLAN и этим альтернативным VLAN могут быть дополнительно назначены порты.

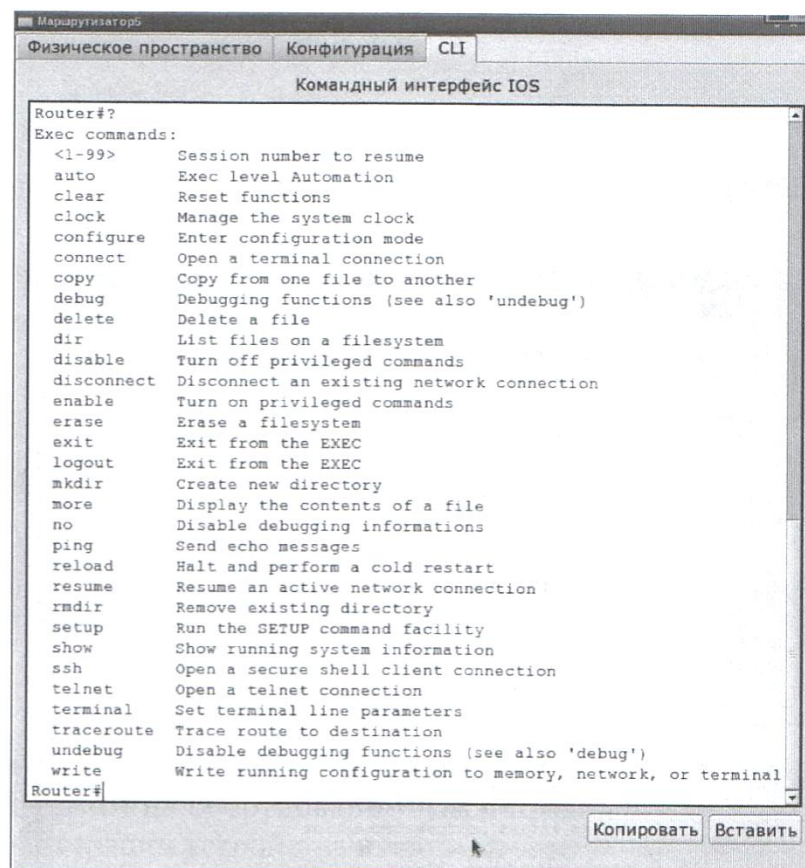


Рис. 16 – Вызов списка команд маршрутизатора, доступных в привилегированном режиме

Операционная система IOS понимает, как укороченное написание команд, так и их дописывание. Клавиша Tab автоматически дополняет команду, которую вы начали писать, что позволяет существенно уменьшить количество печаток и повысить скорость работы. Клавиша Tab дополнит команду, а знак вопроса выведет на экран список дальнейших возможных действий, а также небольшое описание к ним.

Рассмотрим некоторые общие и часто используемые команды.

1. show - просмотр параметров устройства:

- show running-config - просмотр текущей конфигурации настраиваемого оборудования;

- show startup-config - просмотр стартовой конфигурации;

- show mac-address-table - просмотр таблицы MAC-адресов.

2. configure terminal - переход в режим конфигурации и настройки:

- hostname имя - задать имя устройства;

- service password-encryption - включить режим хранения паролей в файле конфигурации устройства в зашифрованном виде;

- line console номер - перейти в настройку консольного подключения:

- login - разрешение проверки пароля,

- password пароль - задать пароль;

- line vti 0 4 - настройка определенных виртуальных терминалов (в данном случае с 0 до 4 терминала):

- login - разрешение проверки пароля,

- password пароль - задать пароль;

- enable password пароль - назначить пароль привилегированного уровня;
 - service password-encryption - зашифровать систему паролей;
 - interface тип/номер - настройка определенного интерфейса (например, interface fastEthernet 0/1):
 - ip address ip-адрес маска — задать IP-адрес и маску,
 - no shutdown - поднять интерфейс,
 - description текст - задать текстовое пояснение назначения интерфейса;
 - vlan номер - настройка определенного VLAN;
 - interface vlan номер - настройка определенного VLAN на интерфейсах (например, interface vlan 1):
 - ip address адрес маска - задать IP-адрес и маску на интерфейсе VLAN,
 - no shutdown - поднять интерфейс VLAN,
 - description текст - задать текстовое пояснение назначения интерфейса VLAN,
 - exit - выход из режима конфигурирования.
3. write memory - запись внесенных изменений в память оборудования.
 4. disable - выход из привилегированного режима в пользовательский.
 5. logout - выйти из режима консоли.

После настройки коммутатора рекомендуется сохранять его текущую конфигурацию. Информация помещается в энергонезависимую память и хранится там столько, сколько нужно. При необходимости все настройки могут быть восстановлены или сброшены. Формат команды:

copy running-config startup-config - команда для сохранения конфигурации;

copy startup-config running-config - команда для загрузки конфигурации.

Если, например, на коммутаторе 2-го уровня требуется задать IP-адрес по которому можно обратиться к нему, то это можно реализовать, задав адрес на VLAN1:

Switch> enable

Switch# configure terminal

Switch (config) # interface vlan 1

Switch (config-if) # ip address ip-адрес маска

Switch (config-if) # no shutdown

Switch (config-if) # exit

Switch (config) # exit

Switch# write memory

Для проверки связи между устройствами сети можно использовать команду ping. Результаты выполнения команды ping представлены в табл. 1.

Таблица 1. – Результаты выполнения команды ping

Символ	Значение
!	Успешный прием эхо-ответа
.	Превышено время ожидания
U	Пункт назначения недостижим
C	Перезагрузка сети

I	Выполнение команды прервано администратором
?	Неизвестный тип пакета
&	Пакет превысил значение параметра время жизни TTL пакета

Задание для выполнения

Схема модулируемой сети представлена на рис. 17.

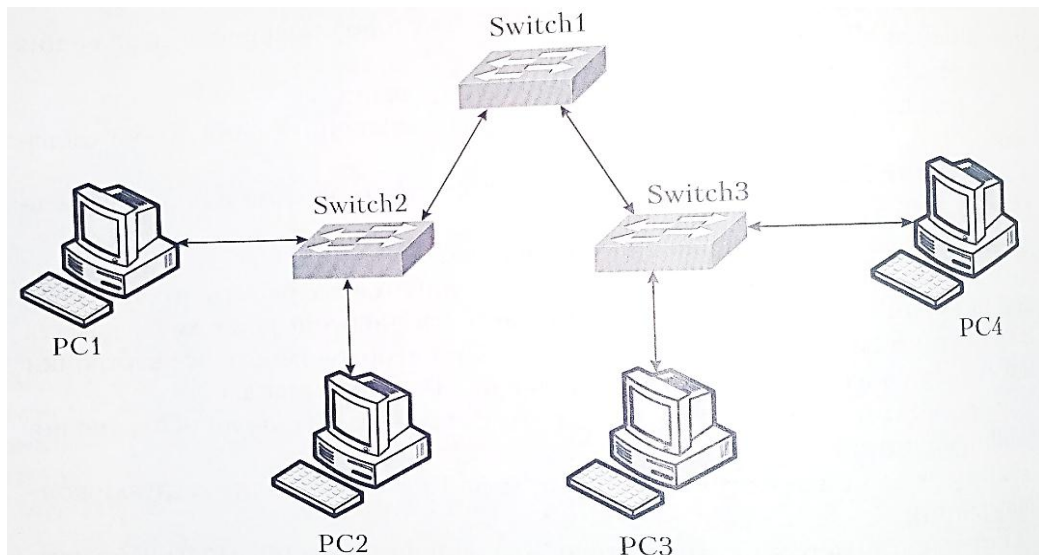


Рис. 17 – Схема моделируемой сети

1. Изменить имя коммутаторам Cisco.
2. Обеспечить парольный доступ к привилегированному режиму на коммутаторах.
3. Задать IP-адреса и маски коммутаторам (172.16.1.11/24, 172.16.1.12/24, 172.16.1.13/24).
4. Задать IP-адреса и маски сетей персональным компьютерам (172.16.1.1/24, 172.16.1.2/24, 172.16.1.3/24, 172.16.1.4/24).
5. Убедиться в достижимости всех объектов сети по протоколу IP.
6. Переключившись в режим симуляции (его описание приведено в методических указаниях), рассмотреть и пояснить процесс обмена данными по протоколу ICMP между устройствами (выполнив команду ping с одного компьютера на другой), пояснить роль протокола ARP в этом процессе. Детальное пояснение включить в отчет.

Структура отчета данной работы:

- титульный лист;
- задание;
- схема сети;
- ход работы: раздел состоит из последовательного описания значимых выполняемых шагов (с указанием их сути) и копий экранов (должна быть видна набранная команда и реакция системы, если она есть);
- выводы.

