МГТУ им. Н. Э. Баумана

Кафедра «Системы обработки информации и управления»

Методические указания к лабораторной работе 1 по дисциплине

Сети и телекоммуникации

Для студентов 3-го курса кафедры ИУ5

Разработали:

ст. преподаватель Антонов А. И.

Москва 2023 г.

Содержание

Лабораторная работа №1.
«Проектирование и анализ локальных вычислительных сетей с использованием коммутаторов в пакете Cisco Packet Tracer».

1.1. Цель лабораторной работы.

Закрепление теоретических знаний в области конструирования и исследования характеристик локальных вычислительных сетей. Изучение программы Cisco Packet Tracer 8.2., приобретение практических навыков проектирования и моделирования работы сети, а также оценки принятых проектных решений.

2. Теоретическая часть.

2.1. Введение в пакет Cisco Packet Tracer 8.2.0

Данный программный продукт разработан компанией Cisco и рекомендован к использованию при изучении телекоммуникационных сетей и сетевого оборудования.

Packet Tracer 8.2. включает следующие особенности:

- моделирование логической топологии: рабочее пространство для того, чтобы создать сети любого размера на CCNA-уровне сложности;
- моделирование в режиме реального времени;
- режим симуляции;
- моделирование физической топологии: более понятное взаимодействие с физическими устройствами, используя такие понятия как город, здание, стойка и т.д.;
- улучшенный GUI, необходимый для более качественного понимания организации сети, принципов работы устройства;
- многоязыковая поддержка: возможность перевода данного программного продукта практически на любой язык, необходимый пользователю;
- усовершенствованное изображение сетевого оборудования со способностью добавлять / удалять различные компоненты;
- наличие Activity Wizard позволяет студентам и преподавателям создавать шаблоны сетей и использовать их в дальнейшем.

С помощью данного программного продукта преподаватели и студенты могут

придумывать, строить, конфигурировать сети и производить в них поиск неисправностей. Packet Tracer дает возможность более подробно представлять новейшие технологии, тем самым делая учебный процесс чрезвычайно полезным с точки зрения усвоения полученного материала.

Данный симулятор позволяет проектировать свои собственные сети, создавая и отправляя различные пакеты данных, сохранять и комментировать свою работу. Packet Tracer позволяет изучать и использовать такие сетевые устройства, как коммутаторы второго и третьего уровней модели OSI, рабочие станции, а также определять типы связей между ними и соединять их (см. рис.3).

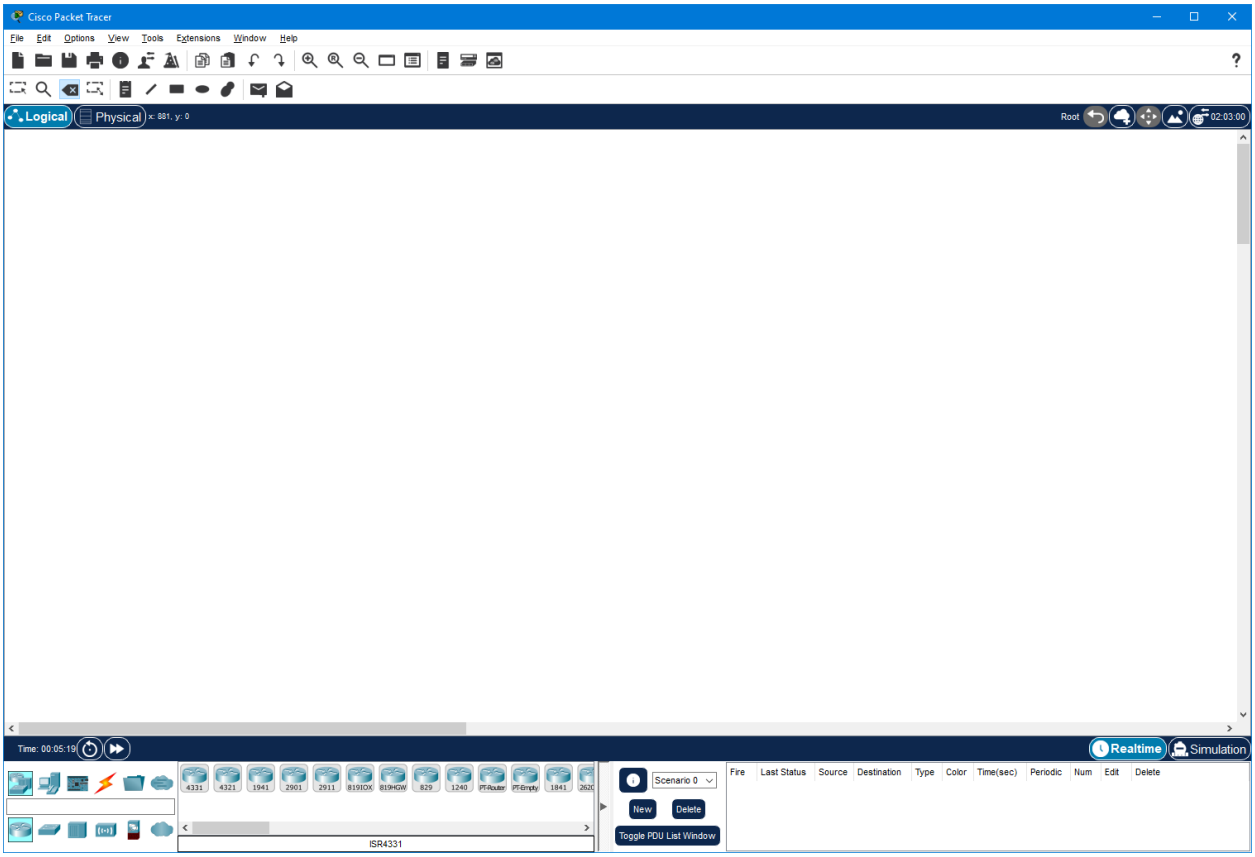

Рис. 3. Cisco Packet Tracer

Отличительной особенностью данной программы является наличие в ней «Режима симуляции» (рис. 4). В данном режиме все пакеты, пересылаемые внутри сети, отображаются графически. Эта возможность позволяет наглядно продемонстрировать, по какому интерфейсу в данные момент перемещается пакет, какой протокол используется и т. д.

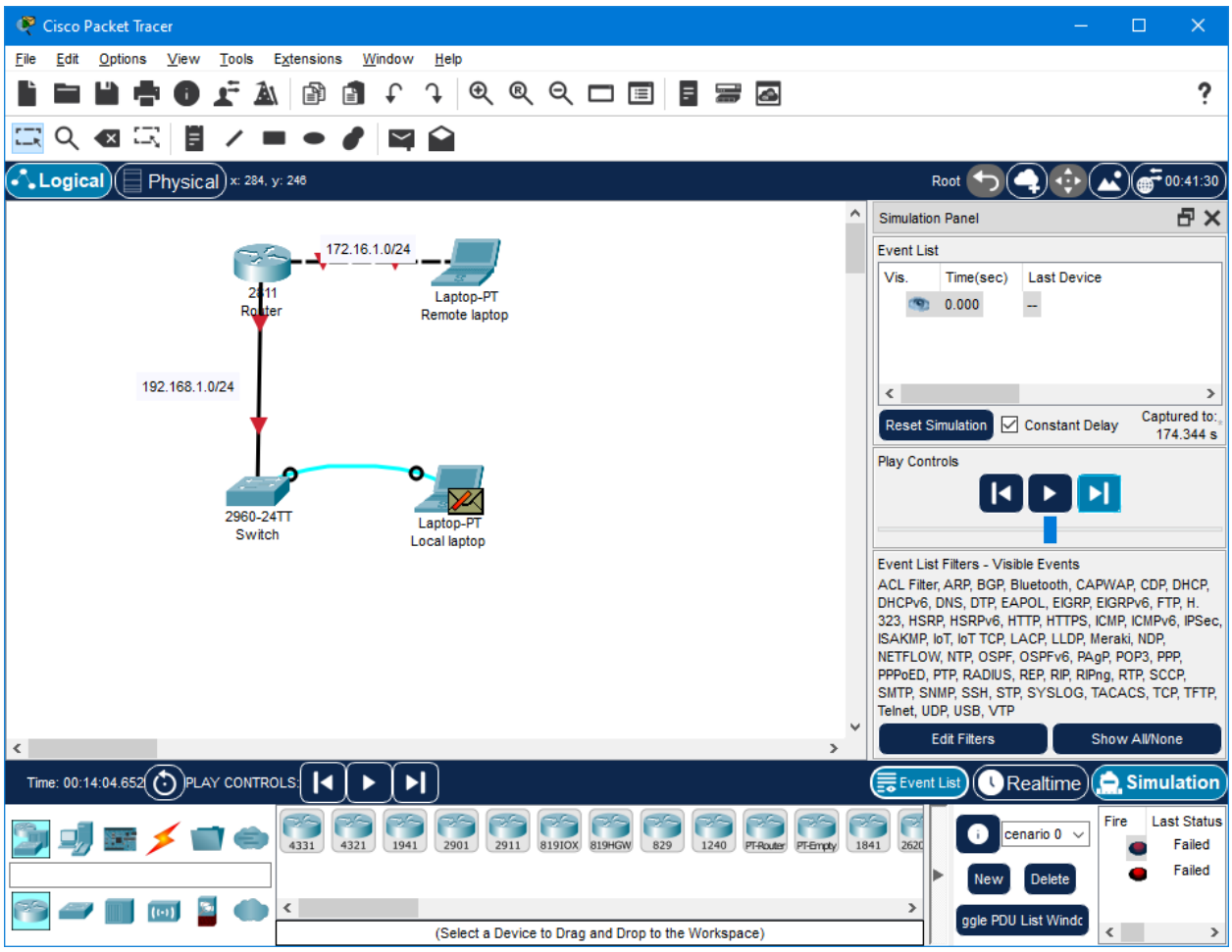

Рис. 4. Режим «Симуляции» в Cisco Packet Tracer

Однако, это не все преимущества Packet Tracer: в «Режиме симуляции» можно не только отслеживать используемые протоколы, но и видеть, на каком из семи уровней модели OSI данный протокол задействован (см. рис. 5). Для запуска окна с просмотром анализа модели OSI необходимо дважды нажать на пакет в списке Event List. Для просмотра структуры передаваемого пакета необходимо перейти на вкладку Outbound PDU Details (см. рис.6)

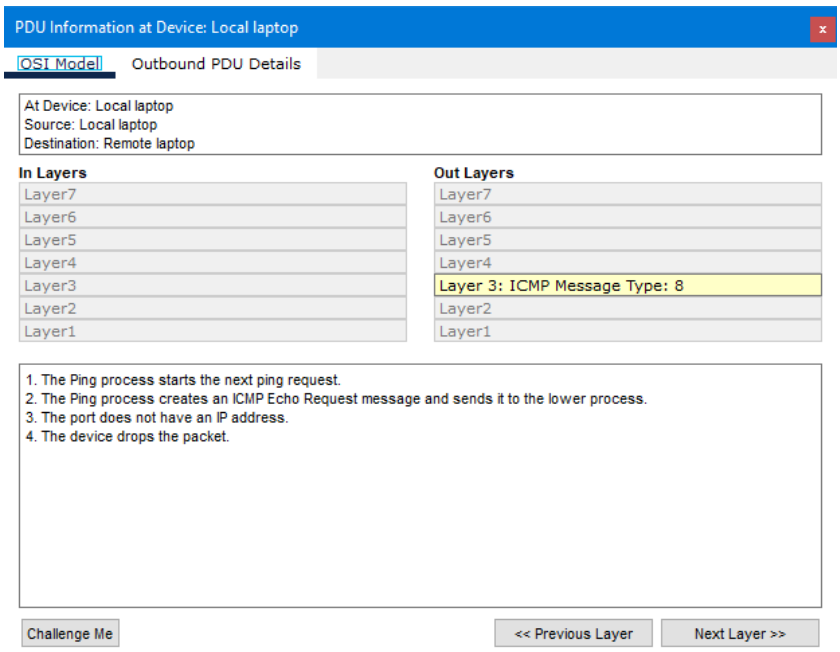

Рис. 5. Анализ семиуровневой модели OSI в Cisco Packet Tracer

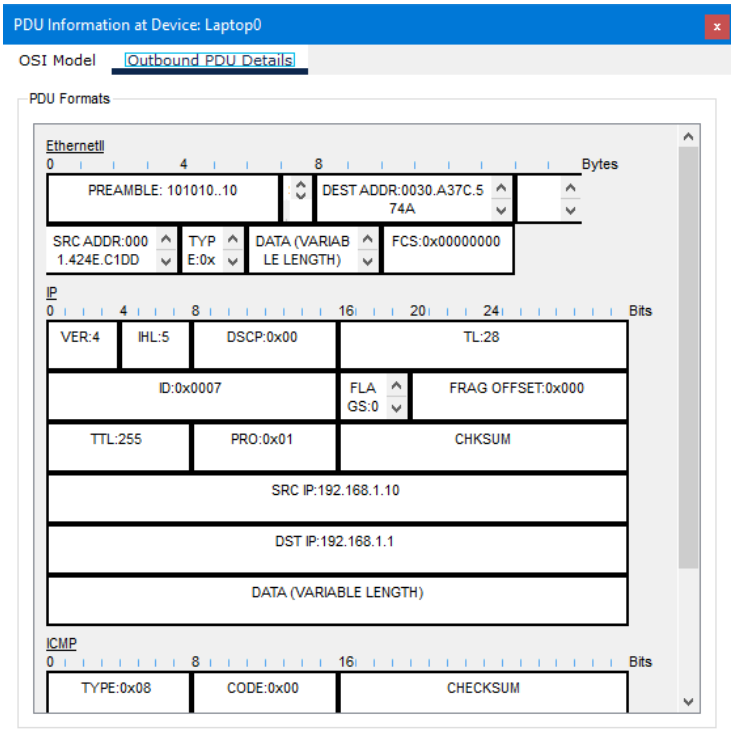

Рис. 6. Просмотр структуры PDU

Такая, кажущаяся на первый взгляд, простота и наглядность, делает практические занятия чрезвычайно полезными, совмещая в них как получение, так и закрепление полученного материала.

Packet Tracer способен моделировать большое количество устройств различного назначения, а так же немало различных типов связей, что позволяет проектировать сети любого размера на высоком уровне сложности:

Моделируемые устройства:

- коммутаторы третьего уровня
- коммутаторы второго уровня
- сетевые концентраторы
- оконечные устройства (рабочие станции, ноутбуки, сервера, принтеры)
- беспроводные устройства
- глобальная сеть WAN.

Типы связей:

1. консоль;
2. медный кабель без перекрещивания (прямой кабель);
3. медный кабель с перекрещиванием (кросс-кабель);
4. волоконно-оптический кабель;
5. телефонная линия;
6. Serial DCE;
7. Serial DTE.

Каждое устройство в программном продукте Cisco Packet Tracer может быть сконфигурировано через окно свойств, которое вызывается по двойному клику на устройстве. Первая вкладка отвечает за физические параметры устройства. В маршрутизаторы и коммутаторы можно добавлять новые модули, в рабочие станции и серверы — вставлять сетевые адаптеры. Для того чтобы переконфигурировать устройство, необходимо предварительно его выключить, нажав на кнопку отключения питания на физическом изображении устройства (рис. 7).

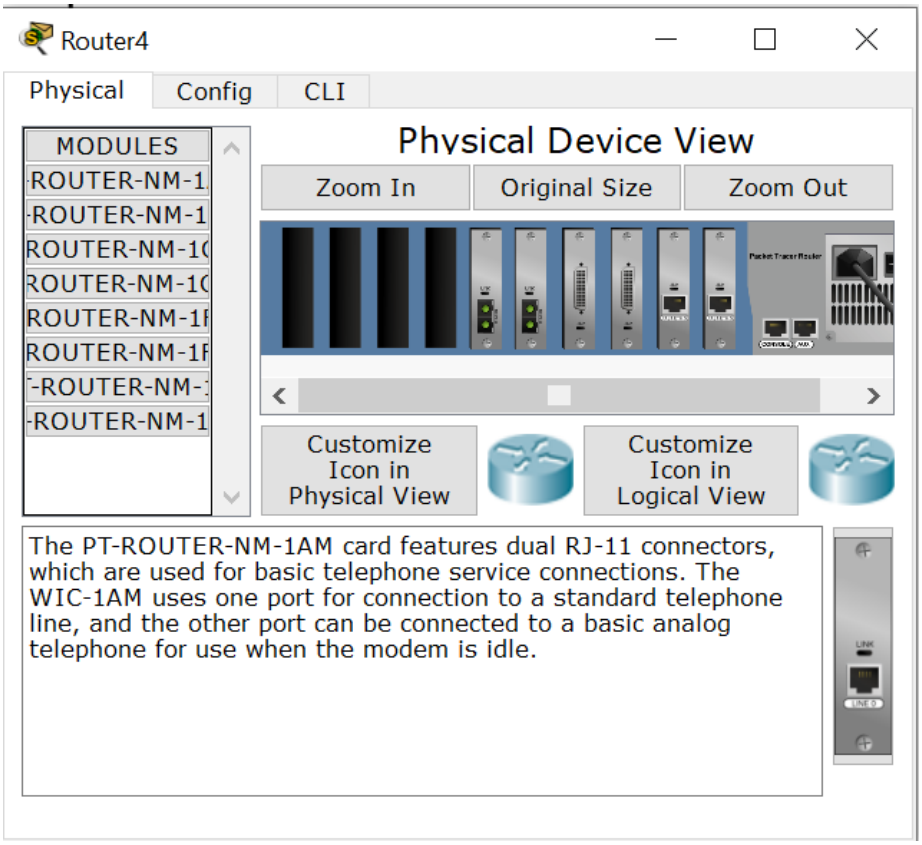

Рис. 7. Физический вид устройства.

На вкладке Config можно задавать основные параметры сетевых интерфейсов (IP-адреса, маску подсети, параметры беспроводной сети и пр.) В сетевых устройствах также можно конфигурировать маршрутизацию – статическую и по протоколу RIP, у серверов — конфигурировать службы. (рис. 8.)

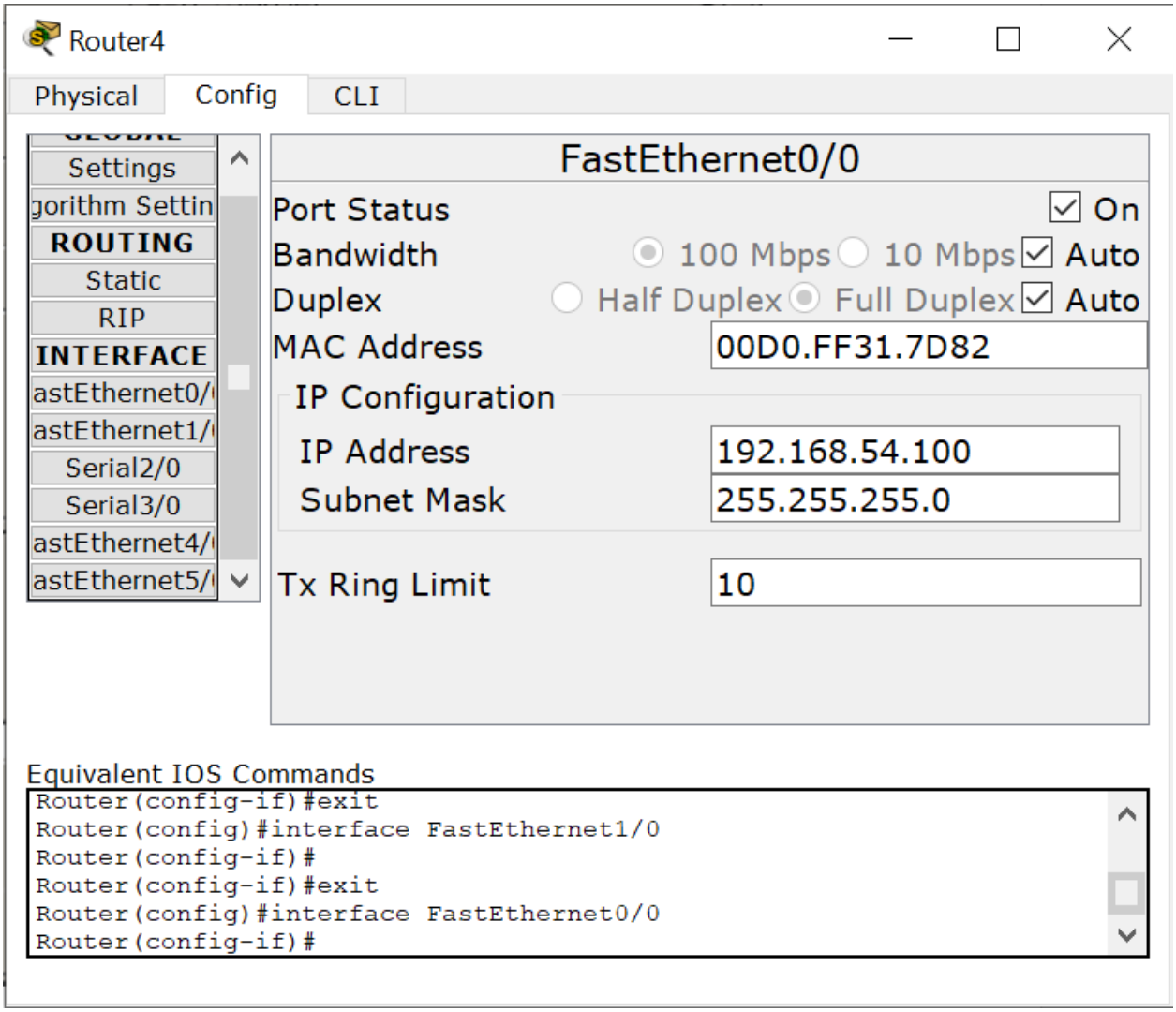

Рис. 8. Конфигурация сервера.

Третья вкладка сетевых устройств обеспечивает доступ к командной строке операционной системы IOS. Третья вкладка рабочих станций и серверов содержит интерфейсы доступа к различным сетевым параметрам, а также несколько клиентских приложений. (рис. 9.)

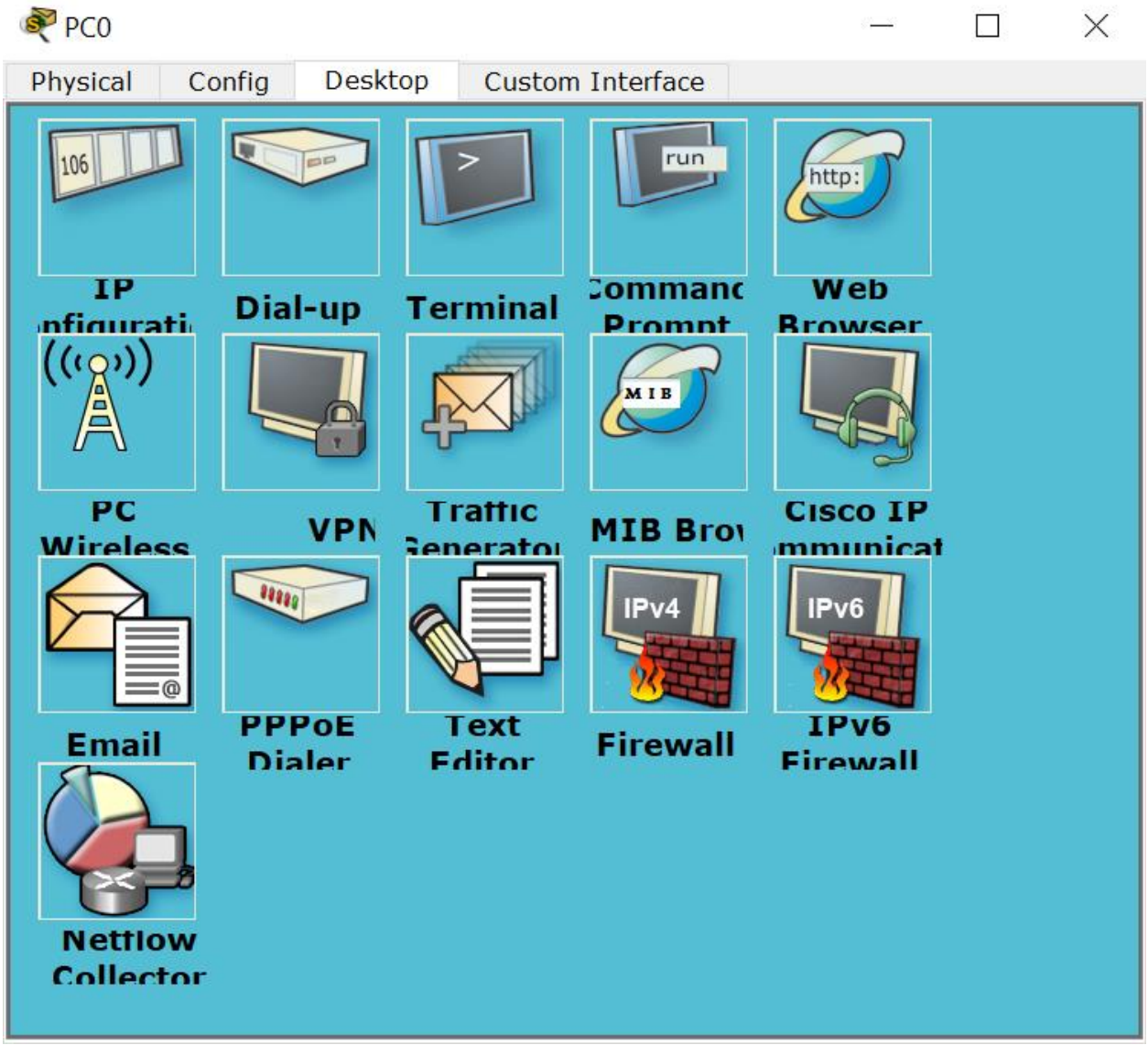

Рис. 9. Вкладка Desktop рабочей станции.

2.2. Командный режим операционной системы IOS

Сетевые устройства конфигурируются в командной строке операционной системы Cisco IOS. Подсоединение осуществляется через Telnet на IP-адрес любого из его интерфейсов или с помощью любой терминальной программы через последовательный порт компьютера, связанный с консольным портом маршрутизатора. Последний способ предпочтительнее, потому что процесс конфигурирования маршрутизатора может изменять параметры IP-интерфейсов, что приведет к потере соединения, установленного через Telnet. Кроме того, по соображениям безопасности доступ к маршрутизатору через Telnet следует запретить.

При работе в командной строке Cisco IOS существует несколько контекстов (режимов ввода команд).

Контекст пользователя открывается при подсоединении к сетевому устройству;

обычно при подключении через сеть требуется пароль, а при подключении через консольный порт пароль не нужен. В этот же контекст командная строка автоматически переходит при продолжительном отсутствии ввода в контексте администратора. В контексте пользователя доступны только простые команды (некоторые базовые операции для мониторинга), не влияющие на конфигурацию маршрутизатора. Вид приглашения командной строки:

```
router>
```

или

```
Switch>
```

Контекст администратора (контекст "exec") открывается командой **enable**, поданной в контексте пользователя; при этом обычно требуется пароль администратора. В контексте администратора доступны команды, позволяющие получить полную информацию о конфигурации маршрутизатора и его состоянии, команды перехода в режим конфигурирования, команды сохранения и загрузки конфигурации. Вид приглашения командной строки:

```
router#
```

Обратный переход в контекст пользователя производится по команде **disable** или по истечении установленного времени неактивности. Завершение сеанса работы - команда **exit**.

Глобальный контекст конфигурирования открывается командой **config terminal** ("конфигурировать через терминал"), поданной в контексте администратора. Глобальный контекст конфигурирования содержит как непосредственно команды конфигурирования маршрутизатора, так и команды перехода в контексты конфигурирования подсистем маршрутизатора.

Контекст конфигурирования интерфейса открывается командой **interface имя_интерфейса** (например, interface serial0), поданной в глобальном контексте конфигурирования;

Контекст конфигурирования процесса динамической маршрутизации открывается командой **router протокол номер_процесса** (например, router ospf 1, поданной в глобальном контексте конфигурирования).

Существует множество других контекстов конфигурирования. Некоторые контексты конфигурирования находятся внутри других контекстов конфигурирования.

Вид приглашения командной строки в контекстах конфигурирования, которые будут встречаться наиболее часто:

```
router(config)#     /глобальный/
router(config-if)# /интерфейса/
rounter(config-router)#   /динамической маршрутизации/
rounter(config-line)#     /терминальной линии/
```

Важно запомнить вид приглашений командой строки во всех вышеуказанных контекстах и правила перехода из контекста в контекст. В дальнейшем примеры команд всегда будут даваться вместе с приглашениями, из которых необходимо определить контекст, в котором подается команда. Примеры не будут содержать указаний, как попасть в необходимый контекст.

Выход из глобального контекста конфигурирования в контекст администратора, а также выход из любого подконтекста конфигурирования в контекст верхнего уровня производится командой exit или Ctrl-Z. Кроме того, команда end, поданная в любом из контекстов конфигурирования немедленно завершает процесс конфигурирования и возвращает оператора в контекст администратора.

Любая команда конфигурации вступает в действие немедленно после ввода, а не после возврата в контекст администратора.

Упрощенная схема контекстов представлена на рис. 9.

Все команды и параметры могут быть сокращены (например, "enable" - "en", "configure terminal" - "conf t"); если сокращение окажется неоднозначным, маршрутизатор сообщит об этом, а по нажатию табуляции выдаст варианты, соответствующие введенному фрагменту.

В любом месте командной строки для получения помощи может быть использован вопросительный знак:

```
router#?     /список всех команд данного контекста с комментариями/
router#co?   /список всех слов в этом контексте ввода, начинающихся на "co" - нет пробела перед "?"/
router#conf ?      /список всех параметров, которые могут следовать за командой config - перед "?" есть пробел/
```

Список команд сгруппирован в соответствии с контекстами, в котором они применяются. В данном списке собраны те команды конфигурирования, которые необходимы для выполнения всех лабораторных работ.

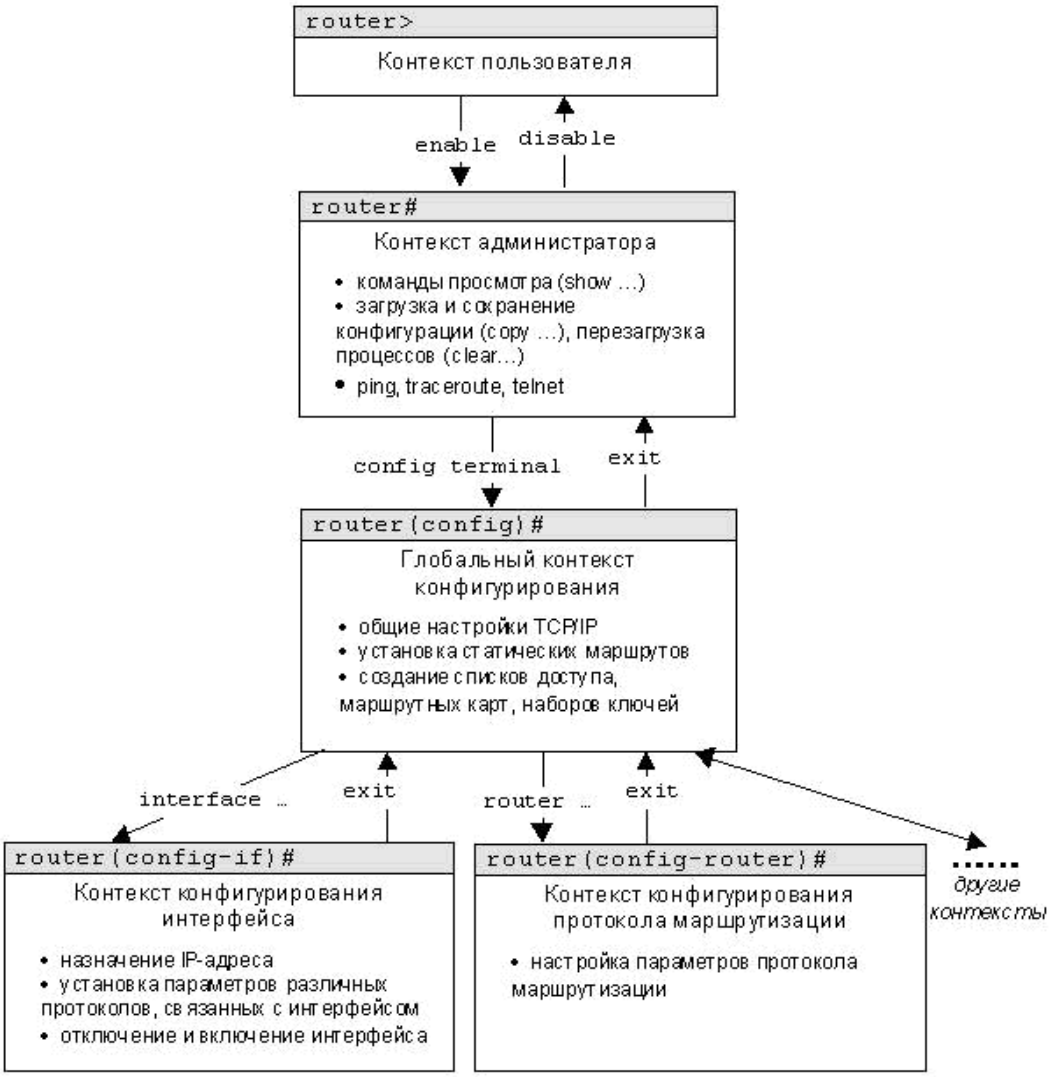

Рис. 9. Схема контекстов Cisco IOS

2.3. Глобальный контекст конфигурирования

Команда «Access-list»

Критерии фильтрации задаются в списке операторов разрешения и запрета, называемом списком доступа. Строки списка доступа сравниваются с IP-адресами и другой информацией пакета данных последовательно в том порядке, в котором были заданы, пока не будет найдено совпадение. При совпадении осуществляется выход из списка. При этом работа списка доступа напрямую зависит от порядка следования строк.

Списки доступа имеют 2 правила: permit – разрешить, и deny – запретить. Именно они определяют, пропустить пакет дальше или запретить ему доступ.

Списки доступа бывают 2-ух типов: standard – стандартные (номера с 1 до 99) и extended – расширенные (номера с 100 до 199). Различия заключаются в возможности фильтровать пакеты не только по ip-адресу, но и по другим параметрам.

Формат команды (стандартные списки доступа):

access-list номер_списка/имя правило A.B.C.D a.b.c.d , где A.B.C.D a.b.c.d – ip-адрес и подстановочная маска соответственно.

Пример выполнения команды:

```
Router(config)#access-list 10 deny 192.168.3.0 0.0.0.3
Router(config)#
```

Данная команда означает, что данный список доступа блокирует любые пакеты с ip-адресами 192.168.3.1 - 192.168.3.3.

Команда «Enable secret»

Обычно при входе в привилегированный режим требуется ввести пароль. Данная функция позволяет предотвратить несанкционированный доступ в данный режим, ведь именно из него можно изменять конфигурацию устройства. Данная команда позволяет установить такой пароль.

Формат команды:

```
enable secret пароль
```

Пример выполнения команды:

```
Switch(config)#enable secret 123
Switch(config)#
%SYS-5-CONFIG_I: Configured from console by console
Switch#exit
Switch con0 is now available
Press RETURN to get started.
Switch>enable
Password:
```

После того, как был установлен пароль, при попытке входа в привилегированный режим, коммутатор будет требовать от пользователя его ввести – в противном случае вход будет невозможен.

Команда «Interface»

Команда для входа в режим конфигурирования интерфейсов конфигурируемого устройства. Данный режим представляет собой одно из подмножеств режима глобального конфигурирования и позволяет настраивать один из доступных сетевых интерфейсов (`fa 0/0`, `s 2/0` и т.д.). Все изменения, вносимые в конфигурацию коммутатора в данном

режиме относятся только к выбранному интерфейсу.

Формат команды (возможны 3 варианта):

```
interface тип порт

interface тип слот/порт

interface тип слот/подслот/порт
```

Примеры выполнения команды:

```
Router(config-if)#

Switch(config)#interface vlan 1

Switch(config-if)#

Router(config)#interface s 3/0
```

После введения данной команды с указанным интерфейсом пользователь имеет возможность приступить к его конфигурированию. Необходимо заметить, что, находясь в режиме конфигурирования интерфейса, вид приглашения командной строки не отображает имя данного интерфейса.

2.4. Контекст конфигурирования интерфейса

Команда «Ip access-group»

Данная команда используется для наложения списков доступа. Список накладывается на конкретный интерфейс, и указывается один из 2-ух параметров: in (на входящие пакеты) или out (на исходящие). Необходимо знать, что на каждом интерфейсе может быть включен только один список доступа.

Формат команды:

```
ip access-group номер_списка/имя_параметр
```

Пример выполнения команды:

```
Router(config-if)# ip access group 10 in

Router(config-if)#
```

В данном примере на выбранный интерфейс накладывается список доступа под номером 10: он будет проверять все входящие в интерфейс пакеты, так как выбран параметр in.

Команда «Bandwidth»

Данная команда используется только в последовательных интерфейсах и служит для установки ширины полосы пропускания. Значение устанавливается в килобитах.

Формат команды:

```
bandwidth ширина_полосы_пропускания
```

Пример выполнения команды:

```
Router(config)#interface serial 2/0
Router(config-if)#bandwidth 560
Router(config-if)#
```

После выполнения данной команды ширина полосы пропускания для serial 2/0 будет равна 560 Kbits.

Команда «Clock rate»

Для корректной работы участка сети, где используется последовательный сетевой интерфейс, один из коммутаторов 3-его уровня должен предоставлять тактовую частоту. Это может быть оконечное кабельное устройство DCE. Так как маршрутизаторы CISCO являются по умолчанию устройствами DTE, то необходимо явно указать интерфейсу на предоставление тактовой частоты, если этот интерфейс работает в режиме DCE. Для этого используют данную команду (значение устанавливается в битах в секунду).

Формат команды:

```
clock rate тактовая_частота
```

Пример выполнения команды:

```
Router(config)#interface serial 2/0
Router(config-if)#clock rate 56000
Router(config-if)#
```

После выполнения данной команды тактовая частота для serial 2/0 будет равна 56000 bits per second.

Команда «Ip address»

Каждый интерфейс должен обладать своим уникальным ip-адресом – иначе взаимодействие устройств по данному интерфейсу не сможет быть осуществлено. Данная команда используется для задания ip-адреса выбранному интерфейсу.

Формат команды:

```
ip address A.B.C.D a.b.c.d ,
```

где A.B.C.D a.b.c.d – ip-адрес и маска подсети соответственно.

Пример выполнения команды:

```
Switch(config)#interface vlan 1
Switch(config-if)#ip address 172.16.10.5 255.255.0.0
Switch(config-if)#
```

Результат можно проверить командой

```
Switch#show ip interface vlan 1
```

Данной командой интерфейсу vlan 1 назначен ip-адрес 172.16.10.5 с маской подсети 255.255.0.0.

Команда «No»

Данная команда применяется в случае необходимости отменить действие какой-либо команды конфигурирования.

Формат команды:

```
no команда_которую_следует_отменить
```

Пример выполнения команды:

```
Switch(config-if)# no shutdown
%LINK-5-CHANGED: Interface Vlan1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
Switch(config-if)#
```

В данном примере использовалась команда shutdown, которая отключает выбранный интерфейс. В итоге после выполнения no shutdown интерфейс включается.

Команда «Encapsulation»

Данная команда обеспечивает инкапсуляцию - метод, используемый многоуровневыми протоколами, в которых уровни добавляют заголовки в модуль данных протокола (protocol data unit - PDU) из вышележащего.

Формат команды:

```
encapsulation тип_протокола
```

Пример выполнения команды:

```
Router(config-if)#encapsulation frame-relay
Router(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up
```

В данном примере маршрутизатор Router сможет пересылать пакеты по протоколу

Frame Relay.

Команда Speed:

Данная команда позволяет изменять скорость передачи данных через указанный порт в Мб/с.

Пример выполнения команды:

```
Switch (config-if)#speed 10
Switch (config-if)#
```

Настройка Port Security

Для включения режима Port Security необходимо применить следующие команды:

```
Switch (config-if)#switchport mode access
Switch (config-if)#switchport port-security
```

Следующие команды используются для настройки параметров Port Security:

```
Switch (config-if)#switchport port-security maximum 3 – эта команда позволяет определять максимальное количество MAC адресов, которые могут быть подключены к указанному интерфейсу.
```

Существует три способа реагирование на нарушение безопасности:

```
Switch (config-if)#switchport port-security violation restrict
Switch (config-if)#switchport port-security violation shutdown
Switch (config-if)#switchport port-security violation protect
```

Первая команда указывает режим реагирование на нарушение. Таким образом, если на данном интерфейсе одновременно «засветится» третий (неизвестный) MAC адрес, то все пакеты с этого адреса будут отбрасываться, при этом отправляется оповещение – syslog, SNMP trap, увеличивается счетчик нарушений (violetion counter).

Вторая команда — «switchport port-security violation shutdown» при выявлении нарушений переводит интерфейс в состояние error-disabled и выключает его. При этом отправляется оповещение SNMP trap, сообщение syslog и увеличивается счетчик нарушений (violation counter). Кстати, если интерфейс находится в состоянии error-disabled, то самым легким путем разблокировать его, является выключить и включить интерфейс (ввести в настройках интерфейса команду — «shutdown», а потом — «no shundown»).

Если же на интерфейсе введена команда — «switchport port-security violation protect», то при нарушениях, от неизвестного MAC адреса пакеты отбрасываются, но при этом никаких сообщений об ошибках не генерируется.

Список разрешенных MAC-адресов можно задавать вручную, пример команды:

```
Switch (config-if)#switchport port-security mac-address 0005.5E80.22A3
```

Либо можно указать sticky режим, при котором запоминаются первые обнаруженные MAC-адреса:

```
Switch(config-if)#switchport port-security mac-address sticky
```

Команда выключения port-security:

```
Switch(config-if)#no switchport port-security
```

Включение trunk режима на интерфейсе:

```
Switch(config-if)#switchport mode trunk
```

Посмотреть данные о trunk портах можно командой

```
Switch#show interfaces trunk
```

В списке выводимых этой командой столбцов есть **Native vlan**. Это тот трафик, который не должен тегироваться при передаче через trunk соединение. Если на коммутатор приходит не тегированный кадр, то он автоматически причисляется к Native Vlan (по умолчанию и в нашем случае это VLAN 1). Native VLAN можно менять в целях безопасности. Для этого в режиме настройки транкового порта нужно применить команду: Switch `(config-if)` #switchport trunk native vlan **X** , где **X** — номер присваиваемого VLAN.

2.5. Контекст администратора

Команда «Configure terminal»

Для конфигурирования устройства, работающего под управлением IOS, следует использовать привилегированную команду configure. Эта команда переводит контекст пользователя в так называемый «режим глобальной конфигурации» и имеет три варианта:

1. конфигурирование с терминала;
2. конфигурирование из памяти;
3. конфигурирование через сеть.

Из режима глобальной конфигурации можно делать изменения, который касаются устройства в целом. Также данный режим позволяет входить в режим конфигурирования определенного интерфейса.

Пример выполнения команды:

```
Router#configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
```

Переход в режим глобальной конфигурации, о чем свидетельствует изменившийся вид приглашения командной строки.

Команда «Copy»

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

Формат команды:

```
copy running-config startup-config – команда для сохранения конфигурации
copy startup-config running-config – команда для загрузки конфигурации
```

Пример выполнения команды:

```
Switch#copy running-config startup-config
Building configuration...
[OK]
Switch#
```

В данном примере текущая конфигурация коммутатора была сохранена в энергонезависимую память.

Команда «Show»

Show (англ. - показывать) – одна из наиболее важных команд, использующихся при настройке коммутаторов. Она применяется для просмотра информации любого рода и применяется практически во всех контекстах. Эта команда имеет больше всех параметров.

Здесь будут рассмотрены только те параметры, которые требуются в рамках данного курса. Другие параметры студент может изучить самостоятельно.

Параметр «running-config» команды «Show»

Для просмотра текущей работающей конфигурации коммутатора используется данная команда.

Пример выполнения команды:

```
Switch#show running-config
!
version 12.1
```

```
!
hostname Switch
…
```

На экран выводится текущие настройки коммутатора.

Параметр «startup-config» команды «Show»

Для просмотра сохраненной конфигурации используется данная команда.

Пример выполнения команды:

```
Switch#show startup-config
Using 1540 bytes
!
version 12.1
!
…
```

Если энергонезависим память не содержит информации, тогда коммутатор выдаст сообщение о том, что конфигурация не была сохранена.

Пример выполнения команды:

```
Switch #show startup-config
startup-config is not present
Switch #
```

Вывод сообщения о том, что в памяти отсутствует какая-либо информация.

Параметр «ip route» команды «Show»

Данная команда применяется для просмотра таблицы маршрутов.

Пример выполнения команды:

```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
```

```
Gateway of last resort is 0.0.0.0 to network 0.0.0.0

C    192.168.1.0/24 is directly connected, FastEthernet0/0

C    192.168.2.0/24 is directly connected, Serial2/0

S    192.168.3.0/24 is directly connected, Serial2/0

S    192.168.4.0/24 is directly connected, Serial2/0

S    192.168.5.0/24 is directly connected, Serial2/0

S*   0.0.0.0/0 is directly connected, Serial2/0

Router#
```

Параметр «ip protocols» команды «Show»

Данная команда используется для просмотра протоколов маршрутизации, включенных на данном устройстве.

Пример выполнения команды:

```
Router#show ip protocols

Routing Protocol is "rip"

Sending updates every 30 seconds, next due in 18 seconds

Invalid after 180 seconds, hold down 180, flushed after 240

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Redistributing: rip

Default version control: send version 1, receive any version

  Interface             Send  Recv  Triggered RIP  Key-chain

  FastEthernet0/0       1     2 1

  Serial2/0             1     2 1

Automatic network summarization is in effect

Maximum path: 4

Routing for Networks:

       192.168.1.0

       192.168.2.0

Passive Interface(s):

Routing Information Sources:

       Gateway         Distance      Last Update

       192.168.2.2          120
```

```
Distance: (default is 120)

Router#
```

Просмотр таблицы Mac-адресов:

```
Switch #show mac-address-table
```

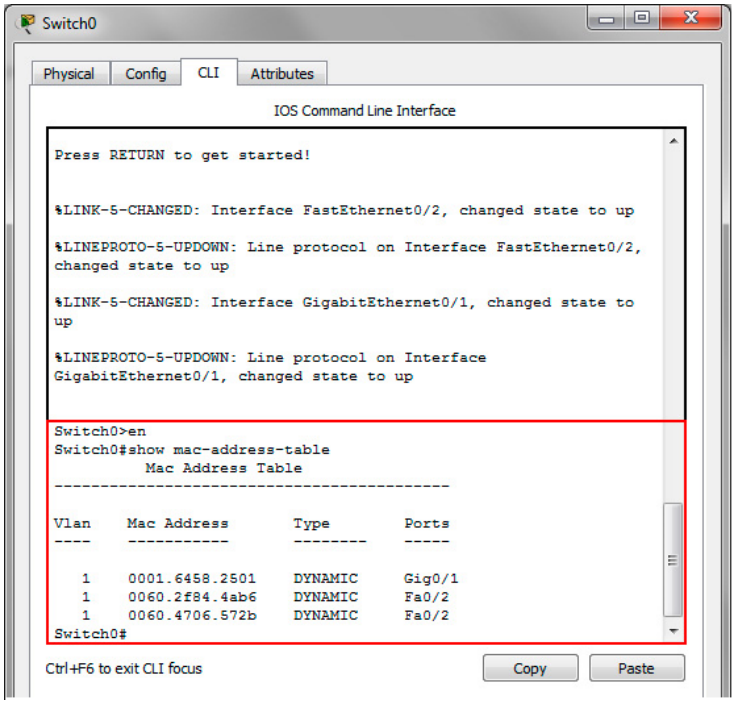

Рис.10 Просмотр таблицы Mac-адресов

Параметр port-security команды «Show»

Данная команда используется для просмотра параметров Port-Security, включенных на данном устройстве.

Пример выполнения команды:

```
Switch #show port-security
```

Просмотр таблицы безопасных Mac-адресов Port-Security:

```
Switch #show port-security address

Vlan    Mac Address       Type                  Ports
----    -----------       ----                  -----
   1    1000.2000.3000    SecureConfigured      Fa5/12
Switch #
```

Команда «Ping»

Для проверки связи между устройствами сети можно использовать данную команду. Она отправляет эхо-запросы указанному узлу сети и фиксирует поступающие ответы.

Формат команды:

```
ping A.B.C.D
```

Пример выполнения команды:

```
Router#ping 77.134.25.133
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 77.134.25.133, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5)
```

Каждый ICMP-пакет, на который был получен ответ, обозначается восклицательным знаком, каждый потерянный пакет – точкой.

2.6. Контекст пользователя

Команда «Enable»

Выполнение конфигурационных или управляющих команд требует вхождения в привилегированный режим, используя данную команду.

Пример выполнения команды:

```
Router>enable
Router#
```

При вводе команды маршрутизатор перешел в привилегированный режим. Для выхода из данного режима используется команда disable или exit.

Также следует отметить, что в данном контексте можно пользоваться командой show для просмотра некоторой служебной информации.

2.7. Конфигурирование сетевого устройста при через Serial подключение.

Для внешнего конфигурирования сетевого устройства необходимо подключить к нему другое устройство через Serial подключение. Далее на соединенном устройстве нужно запустить терминал (окно с параметрами для терминала показано на рис.10). После подтверждения параметров мы попадаем в консоль, и если все настроено правильно, появляется приглашение коммандной строки сетевого устройства, после чего можно начинать настройку, аналогично настройке через CLI.

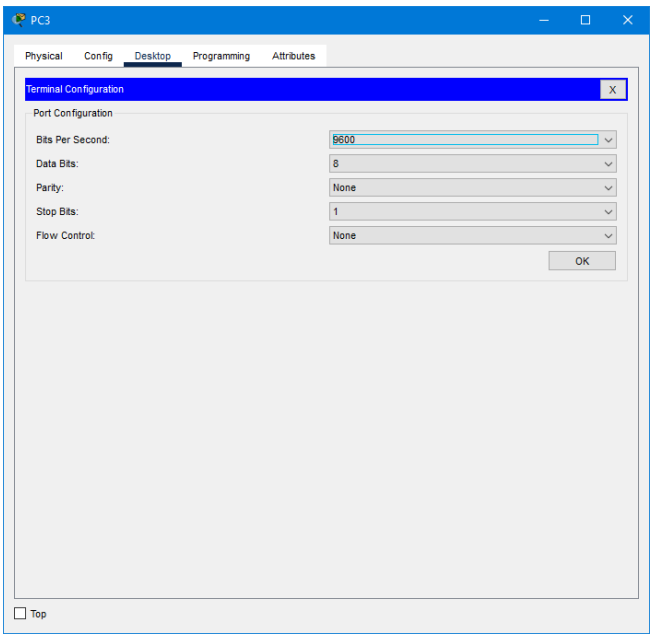

Рис.11 Окно настройки параметров соединения через терминал

2.8. Стандарт Ethernet

Ethernet - семейство технологий пакетной передачи данных между устройствами для компьютерных и промышленных сетей. Стандарты Ethernet определяют проводные соединения и электрические сигналы на физическом уровне, формат кадров и протоколы управления доступом к среде — на канальном уровне модели OSI. Ethernet в основном описывается стандартами IEEE группы 802.3[2]. Ethernet стал одной из самых распространённых технологий ЛВС в середине 1990-х годов, вытеснив такие устаревшие технологии, как Token Ring, FDDI и ARCNET.

Название «Ethernet» (буквально «эфирная сеть» или «среда сети») отражает первоначальный принцип работы этой технологии: всё, передаваемое одним узлом, одновременно принимается всеми остальными (то есть имеется некое сходство с радиовещанием). В настоящее время практически всегда подключение происходит через коммутаторы (switch), так что кадры, отправляемые одним узлом, доходят лишь до адресата (исключение составляют передачи на широковещательный адрес) — это повышает скорость работы и безопасность сет***и.***

Существует множество различных стандартов ethernet. Далее представлены сводные таблицы по различным стандартам:

Первые версии Ethernet

	Стандарт	Год выхода стандарта	Тип	Скорость передачи (Mbps)	Максимальная длина сегмента в метрах	Тип кабеля
10 Мбит/с Ethernet (Thick ethernet)	IEEE 802.3	1983	10Base5	10	500 м	коаксиальный
	IEEE 802.3a	1985	10Base2	10	185 м	
	IEEE 802.3b	1985	10Broad36	10	3600 м	
	IEEE 802.3e	1987	1Base5	1	250 м	UTP
	IEEE 802.3e	1987	StarLan 10	10	250 м	UTP
	IEEE 802.3d	1987	FOIRL	10	1000	оптоволоконный
	IEEE 802.3i	1990	10Base-T	10	100 м	UTP cat 3,5
	IEEE 802.3j	1993	10Base-F	10	2км	оптоволоконный

Каждому стандарту соответствует свой тип, различные типы ethernet отличаются скоростью передачи информации, типами кабелей. Ниже для примера приведены кабели для 10Base-T,10Base5 и 10Base2.

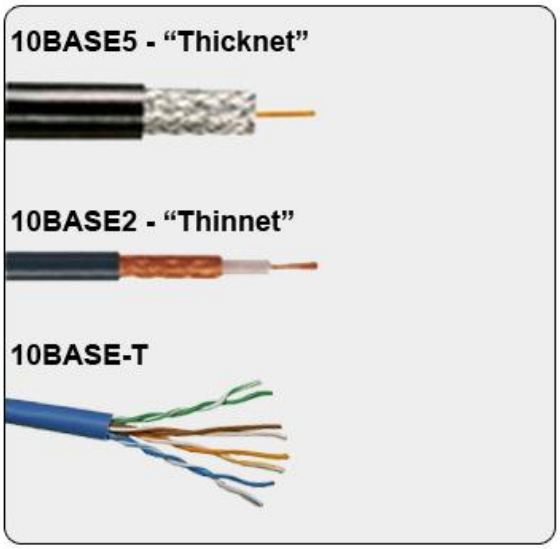

Рис.12 Кабели для стандартов 10Base

Fast Ethernet — общее название для набора стандартов передачи данных в компьютерных сетях по технологии Ethernet со скоростью до 100 Мбит/с, в отличие от исходных 10 Мбит/с.

	Стандарт	Год выхода стандарта	Тип	Скорость передачи (Mbps)	Максимальная длина сегмента в метрах	Тип кабеля
100 Мбит/с Ethernet (Fast Ethernet)	IEEE 802.3u	1995	100Base-FX	100	Одномод — 2 км Многомод — 400 м	оптоволоконный
			100Base-T	100	100 м	UTP/STP cat 5
			100Base-T4	100	100 м	UTP/STP cat >= 3
			100Base-TX	100	100 м	UTP/STP cat 5
	IEEE 802.12	1995	100Base-VG	100	100 м	UTP cat 3,5
	IEEE 802.3y	1998	100Base-T2	100	100 м	UTP cat 3,5
	TIA/EIA-785	2001	100Base-SX	100	300 м	оптоволоконный
	IEEE 802.3ah	2004	100Base-LX10	100	10 км	
	IEEE 802.3ah	2004	100Base-BX10	100	10 км	

Gigabit Ethernet (GbE) — термин, описывающий набор технологий для передачи пакетов Ethernet со скоростью 1 Гбит / с. Он определен в документе IEEE 802.3-2005.

	Стандарт	Год выхода стандарта	Тип	Скорость передачи (Mbps)	Максимальная длина сегмента в метрах	Тип кабеля
1000 Мбит/с (Gigabit Ethernet)	IEEE 802.3z	1998	1000Base-CX	1000	25 м	UTP/STP cat 5,5e,6
			1000Base-LX	1000	Одномод — 5 км Многомод — 550 м	оптоволоконный
			1000Base-SX	1000	550 м	
	IEEE 802.3ab	1999	1000Base-T	1000	100 м	UTP/STP cat 5,5e,6,7
	TIA 854	2001	1000BASE-TX	1000	100 м	UTP/STP cat 6,7
	IEEE 802.3ah	2004	1000BASE-LX10	1000	10 км	оптоволоконный
	IEEE 802.3ah	2004	1000BASE-BX10	1000	10 км	
	IEEE 802.3ap	2007	1000BASE-KX	1000	1 м	для объединительной платы
	non-standard	?	1000BASE-EX	1000	40 км	оптоволоконный

Также сейчас существуют стандарты 10 Gigabit Ethernet, 40 Gigabit Ethernet и многие другие. Самым быстрым из существующих на 2023 год являются стандарт 802.3dj обеспечивающий теоретическую скорость передачи вплоть до 1.6 Тбит/с.

Также существует несколько форматов кадров, определяемых стандартов ethernet:

1. Ethernet II
2. Ethernet_802.3 (с LLC заголовком)
3. «Raw» 802.3
4. 802.3 with SNAP Header

В качестве примера далее приведена структура наиболее распространённого типа кадра Ethernet II.

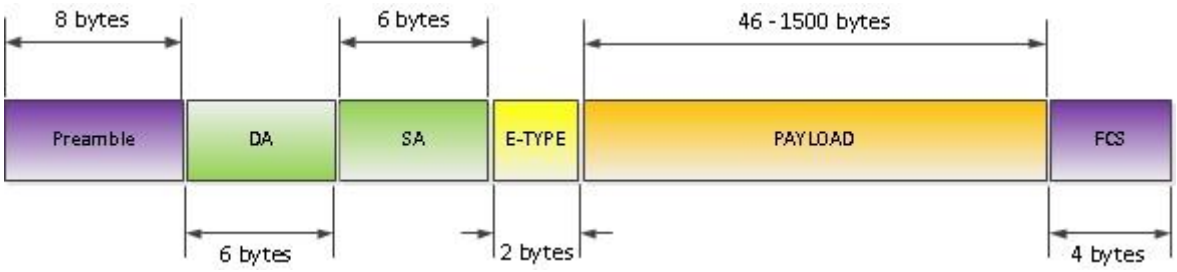

Рис.13 Структура кадра Ethernet II

Preamble – последовательность бит, по сути, не являющаяся частью ETH заголовка определяющая начало Ethernet фрейма.

DA (Destination Address) – MAC адрес назначения, может быть юникастом, мультикастом, бродкастом.

SA (Source Address) – MAC адрес отправителя. Всегда юникаст.

E-TYPE (EtherType) – Идентифицирует L3 протокол (к примеру 0x0800 – Ipv4, 0x86DD – IPv6, 0x8100- указывает что фрейм тегирован заголовком 802.1q, и т.д.)

Payload – L3 пакет размером от 46 до 1500 байт

FCS (Frame Check Sequences) – 4 байтное значение CRC используемое для выявления ошибок передачи. Вычисляется отправляющей стороной, и помещается в поле FCS. Принимающая сторона вычисляет данное значение самостоятельно и сравнивает с полученным.

Данный формат был создан в сотрудничестве 3-х компаний – DEC, Intel и Xerox. В связи с этим, стандарт также носит название **DIX Ethernet standard**. Данная версия стандарта была опубликована в 1982г (первая версия, Ehernet I – в 1980г. Различия в версиях небольшие, формат в целом остался неизменным). В 1997г. году данный стандарт был добавлен IEEE к стандарту 802.3, и на данный момент, подавляющее большинство пакетов в Ethernet сетях инкапсулированы согласно этому стандарту.

3. Задание.

Задание: построить локальную сеть, состоящую из 2х сегментов на основе коммутаторов в каждом из которых находится A и B компьютеров соответственно. Коммутаторы соединены друг с другом при помощи кроссовера. Все устройства должны находиться в одной подсети (192.168.X.Y, где X-номер группы, Y- номер устройства). Необходимо добиться свободной пересылки пакетов между устройствами сети. Один из коммутаторов необходимо сконфигурировать через устройство, подключенное по консольному (RS 232) порту. Между коммутаторами настроить trunk режим соединения и продемонстрировать различие в структуре пакетов, пересылаемых между двумя коммутаторами и между клиентскими устройствами и коммутаторами (для этого необходимо изменить номер Native VLAN для trunk соединения). Для одного из интерфейсов, по которому соединены коммутаторы, включить Port-Security и ограничить максимальное количество устройств в сети. Продемонстрировать работу Port Security при добавлении нового устройства в сеть.

Дополнительно: на одном из коммутаторов настроить доступ к консоли коммутатора через telnet и установить пароль для этого подключения.

4. Контрольные вопросы.

1. Какие протоколы физического уровня были использованы в данной работе?
2. Чем отличаются режимы работы trunk и access?
3. Для чего необходимо использовать Port Security?
4. Какие протоколы канального и физического уровня были использованы в данной работе? Для чего эти протоколы предназначены?
5. Какие режимы работы Port Security существуют, и чем они отличаются между собой?
6. Что такое VLAN и для чего он применяется?

5. Рекомендруемые источники.

1. Галкин В.А., Григорьев Ю.А. Телекоммуникации и сети: Учеб. пособие для вузов. - М.: Изд-во МГТУ им. Н.Э. Баумана, 2003.

2. Олифер В.Г., Олифер Н.А Компьютерные сети. Принципы, технологии, протоколы 3-е издание. Учебное пособие, СПб.: Питер 2007

3. Степанов А.Н. Архитектура вычислительных систем и компьютерных сетей, СПб.:

Питер 2007

4.Access и Trunk порты: [Электронный ресурс].URL: https://study-ccna.com/access-and-trunk-ports (Дата обращения: 25.05.2023)

5.Настройка Access и Trunk интерфейсов: [Электронный ресурс]. URL: https://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/configuration/nxos/Cisco_Nexus_5000_Series_NX-OS_Software_Configuration_Guide_chapter9.pdf (Дата обращения: 25.05.2023)

6. Всё, что вы хотели знать о Ethernet фреймах, но боялись спросить, и не зря. Электронный ресурс]. URL:
https://habr.com/ru/articles/227729 (Дата обращения: 04.12.2023)

7. Шпаргалка по типам и стандартам Ethernet 802.3 [Электронный ресурс].URL: https://habr.com/ru/articles/208202 (Дата обращения: 04.12.2023)