

МГТУ им. Н. Э. Баумана

Кафедра «Системы обработки информации и управления»

Методические указания к лабораторным работам 4-6 по дисциплине

Сети и телекоммуникации

Для студентов 3-го курса кафедры ИУ5

Разработали:

к.т.н., доцент Галкин В.А.

ст. преподаватель Аксенов А. Н.

ст. преподаватель Антонов А. И.

ассистент Канев А.И.

Москва 2021 г.

Содержание

ЛАБОРАТОРНЫЕ РАБОТЫ №4, №5 И №6.	3
«ПРОЕКТИРОВАНИЕ И АНАЛИЗ ЛОКАЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ В ПАКЕТЕ CISCO PACKET TRACER. АДРЕСАЦИЯ. СТАТИЧЕСКАЯ И ДИНАМИЧЕСКАЯ МАРШРУТИЗАЦИЯ».....	3
1. Цель лабораторных работ.	3
2. Теоретическая часть.....	3
3. Введение в пакет Cisco Packet Tracer 5.3	10
4. Командный режим операционной системы IOS	16
4.1. Глобальный контекст конфигурирования	20
4.2. Контекст конфигурирования интерфейса	23
4.3. Контекст администратора.....	26
4.4. Контекст пользователя.....	30
4.5. Контекст конфигурирования маршрутизации.....	31
4.6 Контекст конфигурирования динамического распределения ip адресов.	45
5. Задания.	32
6. Варианты заданий.	47

Лабораторные работы №4, №5 и №6.

«Проектирование и анализ локальных вычислительных сетей в пакете Cisco Packet Tracer. Адресация. Статическая и динамическая маршрутизация».

1. Цель лабораторных работ.

Закрепление теоретических знаний в области конструирования и исследования характеристик локальных вычислительных сетей. Изучение программы Cisco Packet Tracer 5.3, приобретение практических навыков проектирования и моделирования работы сети, а также оценки принятых проектных решений.

2. Теоретическая часть.

IP-адресация версии 4

На сетевом уровне (или IP) (см на Рис.1) мы должны уникально идентифицировать каждое устройство в Интернете, чтобы обеспечить глобальную связь между всеми устройствами. Эта адресация напоминает нумерацию в телефонной сети, где каждый абонент имеет уникальный номер телефона, содержащий международный код (код страны), междугородный код города и т. д., который идентифицирует его местоположение.

Установление соединения между двумя и более узлами происходит на основе обработки адресной информации, которая по мере необходимости обрабатывается устройствами 3-го уровня в маршрутизаторах. К адресу предъявляются следующие требования:

- адрес должен быть универсальным;
- адрес должен иметь иерархическую структуру, удобную для обработки соответствующими узлами;
- адрес должен быть удобен для пользователя.

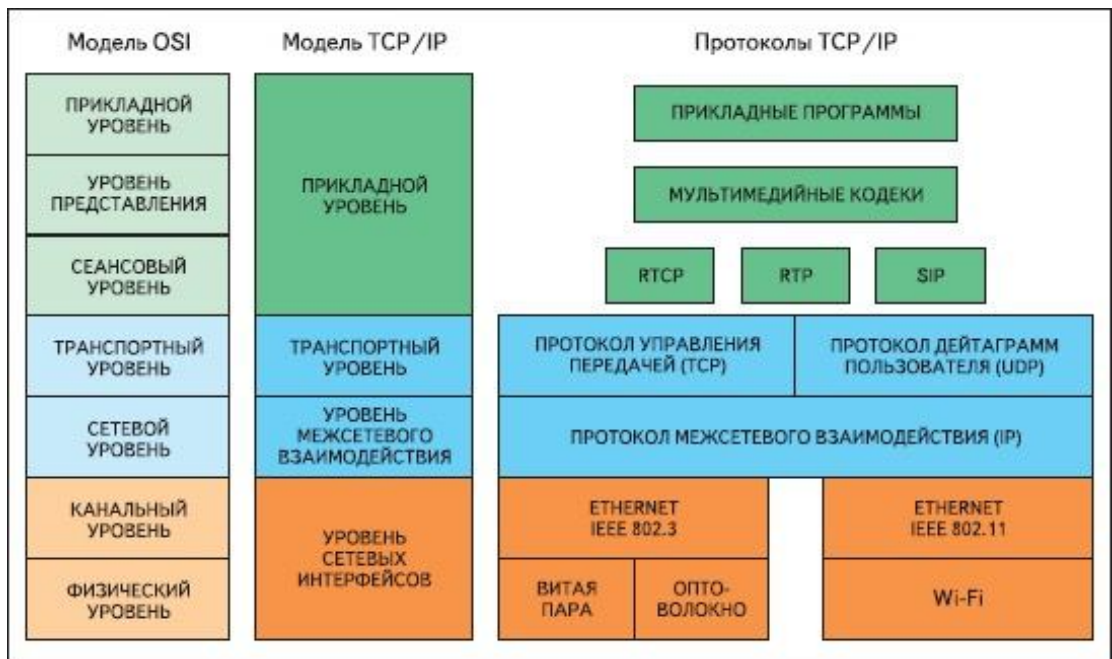


Рис. 1. Модель OSI

Идентификатор, используемый на уровне IP набора протокола TCP/IP (см на Рис2), чтобы идентифицировать каждое устройство, подключенное к Интернету, назван адресом Интернета, или адресом IP. Адрес IP — двоичный адрес на 32 бита, который уникально и универсально определяет подключение хоста или маршрутизатора к Интернету.

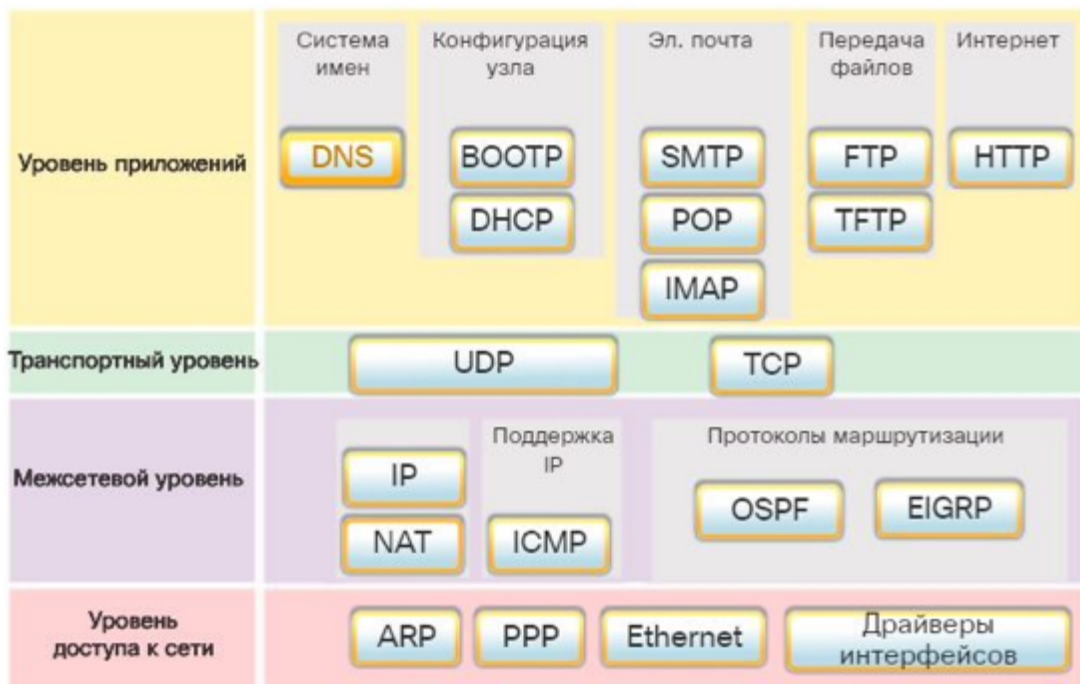


Рис. 2. Набор протокола TCP/IP

Адреса IP уникальны. Они уникальны в том смысле, что каждый адрес определяет

одно и только одно подключение к Интернету. Два устройства в Интернете никогда не могут иметь одного того же адреса. Если устройство имеет два подключения к Интернету, через две сети, оно имеет два адреса IP.

Адреса IP универсальны потому, что система адресации должна быть принята любым хостом, который хочет быть связанным с Интернетом.

Адресное пространство.

Протокол, подобный IP, то есть определяющий адреса, имеет адресное пространство. Адресное пространство — общее количество адресов, применяемых в соответствии с протоколом. Если протокол использует N бит, чтобы определить адрес, адресное пространство — 2^N , потому что каждый бит может иметь два различных значения (0 и 1), а N бит могут иметь 2^N значений.

IPv4 использует адреса на 32 бита, то есть адресное пространство — 2^{32} или 4,294,967,296 (больше чем четыре миллиарда). Это означало бы, что, теоретически, если не было бы никаких ограничений, к Интернету могли бы быть подключены более чем 4 миллиарда устройств. Мы вскоре увидим, что фактически номеров намного меньше.

Маска

Уже давно наблюдается дефицит IP-адресов, который обусловлен не только ростом числа пользователей, но и необходимостью выделения IP-адресов на каждый порт маршрутизатора. Имеется несколько подходов смягчения этой проблемы, в том числе за счет использования масок.

Традиционно номер сети и узла определяется в зависимости от класса адреса. Однако наличие только четырех классов адресов часто бывает неудобно. Например, администратор получил от поставщика услуг номер сети 135.38.0.0 (адрес класса В, двоичный код сети — 10000111 00100110 00000000 00000000). В такой сети потенциально можно иметь 65 534 узла, но такое количество узлов администратору не нужно, ему достаточно иметь 32 000. Проблема решается с помощью масок. Количество "единиц" в маске показывает число старших разрядов, которые определяют номер сети. Для нашего случая следует выбрать маску со значением 255.255.192.0 (двоичный код 11111111 11111111 11000000 00000000). В результате наложения маски на сетевой адрес получается четыре подсети: 135.38.0.0; 135.38.64.0; 135.38.128.0; 135.38.192.0.

Протокол маршрутизации RIP

RIP был повсеместно принят производителями персональных компьютеров (PC) для использования в их изделиях передачи данных по сети. Например, протокол маршрутизации AppleTalk (Протокол поддержания таблицы маршрутизации - RTMP) является модернизированной версией RIP. RIP также явился базисом для протоколов Novell, 3Com, Ungermann-Bass и Banyan. RIP компаний Novell и 3Com в основном представляет собой стандартный RIP компании Xerox. Ungermann-Bass и Banyan внесли незначительные изменения в RIP для удовлетворения своих нужд.

Формат таблицы маршрутизации

Каждая запись данных в таблице маршрутизации RIP обеспечивает разнообразную информацию, включая конечный пункт назначения, следующую пересылку на пути к этому пункту назначения и показатель (metric). Показатель обозначает расстояние до пункта назначения, выраженное числом пересылок до него. В таблице маршрутизации может находиться также и другая информация, в том числе различные таймеры, связанные с данным маршрутом. Типичная таблица маршрутизации RIP показана на таблице 1.

Таблица 1. маршрутизация RIP

Destination	Next hop	Distance	Timers	Flags
Network A	Router 1	3	t1, t2, t3	x, y
Network B	Router 2	5	t1, t2, t3	x, y
Network C	Router 1	2	t1, t2, t3	x, y

RIP поддерживает только самые лучшие маршруты к пункту назначения. Если новая информация обеспечивает лучший маршрут, то эта информация заменяет старую маршрутную информацию. Изменения в топологии сети могут вызывать изменения в маршрутах, приводя к тому, например, что какой-нибудь новый маршрут становится лучшим маршрутом до конкретного пункта назначения. Когда имеют место изменения в топологии сети, то эти изменения отражаются в сообщениях о корректировке маршрутизации. Например, когда какой-нибудь роутер обнаруживает отказ одного из каналов или другого роутера, он повторно вычисляет свои маршруты и отправляет сообщения о корректировке маршрутизации. Каждый роутер, принимающий сообщение об обновлении маршрутизации, в котором содержится изменение, корректирует свои таблицы

и распространяет это изменение.

Как и другие протоколы маршрутизации, RIP использует определенные таймеры для регулирования своей работы. Таймер корректировки маршрутизации RIP (routing update timer) обычно устанавливается на 30 сек., что гарантирует отправку каждым роутером полной копии своей маршрутной таблицы всем своим соседям каждые 30 секунд. Таймер недействующих маршрутов (route invalid timer) определяет, сколько должно пройти времени без получения сообщений о каком-нибудь конкретном маршруте, прежде чем он будет признан недействительным. Если какой-нибудь маршрут признан недействительным, то соседи уведомляются об этом факте. Такое уведомление должно иметь место до истечения времени таймера отключения маршрута (route flush timer). Когда заданное время таймера отключения маршрута истекает, этот маршрут удаляется из таблицы маршрутизации. Типичные исходные значения для этих таймеров - 90 секунд для таймера недействующего маршрута и 270 секунд для таймера отключения маршрута.

Доменные имена

Чтобы понять, как действует DNS, полезно ознакомиться с окружением, в котором выполняет свою работу эта служба. Начнем с иерархии DNS. Корневой домен известен просто как ".". Верхний домен находится на один уровень ниже, и на этом уровне находится целый ряд доменов DNS. Вы знаете все эти суффиксы: .COM (коммерческие), .GOV (правительственные), .EDU (образование), .INT (международные), .ORG (организация), .NET (Net-провайдеры, ISP [Провайдеры услуг Интернет] и т.д.) и .MIL (военные). Достаточно интересно, что ICANN (новая некоммерческая организация по назначению адресов и имен в интернете) ссылается на эти "обобщенные" домены верхнего уровня, и в период между 2000 и 2002 гг. она ввела еще семь: .BIZ, .INFO, .NAME, .PRO, .AERO, .COOP и .MUSEUM. Но пока еще используются не все эти новые имена.

На следующем уровне обычно находится домен, поддерживаемый частной фирмой; я буду использовать для своих примеров корпоративный домен .COM, но для этого можно было бы использовать любой из только что перечисленных доменов. Вы можете рассматривать домены DNS аналогично структуре папок на жестком диске в смысле разбиения пространства имен DNS. Домен "." аналогичен корневой папке; далее идет верхний уровень (.COM), и на следующем уровне находится "папка", представляющая корпоративный объект некоторого рода (частный или общественный). Имя верхнего уровня (.COM) и корпоративная "папка", например, Microsoft, совместно образуют доменное имя.

Пространство имен Microsoft может разбиваться на меньшие домены ("подпапки") Active Directory/DNS, представляющие в компании Microsoft различные подразделения или службы, например, `accounting.microsoft.com` (бухгалтерский учет). Такой домен обычно недоступен из Internet в отличие от `microsoft.com`; однако имеются исключения, например, `http://support.microsoft.com/default.aspx?scid=fh` представляет службы поддержки Microsoft. Здесь находится Knowledge Base вместе с различными рекомендациями от MS Support. Каждая субзона отвечает за правильность собственной работы.

Это обычное пространство DNS, известное как зона прямого поиска (forward lookup zone). Существует также зона обратного поиска (reverse lookup zone), известная также как `in-addr.arpa`, что является ее техническим названием. При запросе обратного поиска вместо дружественного для пользователя имени (как это происходит при поиске в зоне прямого поиска) выполняется поиск определенного IP-адреса машины. Записи в зоне обратного поиска содержат IP-адрес и затем имя машины. Resolver может определить, соответствует ли в действительности определенный IP-адрес дружественному имени, которое он указывает. Поскольку IP-адреса регистрируются вместе с доменными именами DNS, поиск по IP-адресу позволяет определить, из какого домена происходит этот IP-адрес. Если он не соответствует тому, что он должен представлять, то это может быть "самозванец".

IP-адреса организованы таким образом, что их "старшинство" повышается слева направо, а в доменных именах "старшинство" снижается слева направо. Но IP-адреса в домене `in-addr.arpa` (зона обратного поиска) записываются в обратном порядке. В записях-указателях (ptr-записях), которые добавляются в зону обратного поиска, сначала указывается IP-адрес и затем – хост-имя, – в отличие от зоны прямого поиска, где сначала идет хост-имя и затем – IP-адрес. Для выполнения успешного обратного поиска по заданному IP-адресу, например, `121.41.113.10`, выполняющий поиск сервер DNS ищет PTR-запись для `10.113.41.121.in-addr.arpa`, которая содержит определенное хост-имя и IP-адрес `121.41.113.10`.

Записи DNS

В DNS имеется много типов записей, но из-за недостатка места, времени, а также ввиду несущественности в нашем случае некоторых записей мы рассмотрим только наиболее употребительные типы записей.

- А-запись. Указывает адрес хоста. Она отображает хост-имя на адрес и может выглядеть следующим образом:
- `Myhost.mycompany.com IN A 192.168.0.1`

- AAAA-запись. Эта запись пока используется не слишком много, но ожидается, что она будет активно использоваться с появлением IPv6. Считалось, что все доменные имена и IP-адреса будут скоро исчерпаны из-за потребительского роста. Это не происходит, и пока повсеместно используется IPv4. Вот пример хост записи из зоны, которая хранится в среде IPv6.
- IN AAAA 1234:1:2:3:4:567:89cd
- CNAME-запись. Это каноническая запись, обычно используемая для алиасов (псевдонимов). Она позволяет отображать несколько хост-имен на заданный IP-адрес. Многие компании используют этот метод, чтобы убедиться, что их посетил предполагаемый заказчик, даже если этот посетитель немного ошибся в URL или имеется несколько вариантов написания URL компании. В этом случае заказчик будет уверен, что попал на нужный сайт.
- SRV-запись (локатор служб). Эта запись особенно важна для Windows 2000 и 2003 в конфигурации лес/домены. Она используется для регистрации контроллеров домена (DC) в DNS и для объявления несколькими серверами информации о том, что они предоставляют определенную службу TCP/IP. Если вы пытаетесь создать новую запись, то имеете возможность задания для нее определенной службы TCP/IP. После размещения такой записи клиент, направляющий SRV-запрос, может использовать определенную службу TCP/IP, которая предоставляется в данном домене несколькими серверами. Если вы не можете найти контроллер домена для присоединения к домену, то SRV-записи – это одно из средств, которое вам следует использовать. Эта запись позволяет находить контроллеры домена, которые используют службу LDAP (AD) через порт TCP 389.
- NS-запись. Эта запись идентифицирует сервер(ы) имен для заданного домена DNS. В NS-записях указываются первичные и вторичные серверы для пространства имен плюс дочерние зоны, происходящие из него.
- SOA-запись (Start of Authority). эта запись определяет зону, для которой данный сервер является руководящим. Она имеет такие параметры конфигурирования для сервера, как срок действия (time to live), кто несет ответственность за указанный сервер, имена сервера имен (NS server), частоту обновления, последовательный (или "магический") номер, используемый для маркировки изменений зон, и запускаемая репликация (trigger replication).
- PTR-запись. Эта запись позволяет быстро выполнять обратный поиск с помощью зоны обратного поиска (inaddr.arpa). Она считается обратной A-записью, но не похожа на нее ввиду использования inaddr.arpa в реальной записи. Такая запись для

хоста syscrusher.skillet.com с IP-адресом 100.200.252.1 имеет следующий вид:
1.252.200.100.in-addr.arpa IN PTR syscrusher.skillet.com.

- MX-запись. Эта запись для почтового обмена. Вы можете иметь несколько записей, которые указывают несколько ближайших почтовых серверов, и можете располагать их в нужном вам порядке.

Microsoft имеет несколько особых записей для собственных целей; эти записи используются для связи с различными окружениями WINS. Это следующие записи:

- WINS. Позволяет MS DNS использовать сервер WINS для разрешения хост-имени. Это полезно, если у вас имеются клиенты более ранних версий Windows, которые не получают регистрации в какой-либо зоне DNS. Нужно найти такую запись, после чего будет запрошен сервер WINS.
- WINS-R. Эта запись позволяет осуществлять обратный поиск. Это только записи Microsoft, и они могут быть ограничены при пересылке зон.

3. Введение в пакет Cisco Packet Tracer 5.3

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

Packet Tracer 5.3 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 студентам проектировать свои собственные сети, создавая и отправляя различные пакеты данных, сохранять и комментировать свою работу. Студенты могут изучать и использовать такие сетевые устройства, как коммутаторы второго и третьего уровней, рабочие станции, определять типы связей между ними и соединять их (см. рис.3).

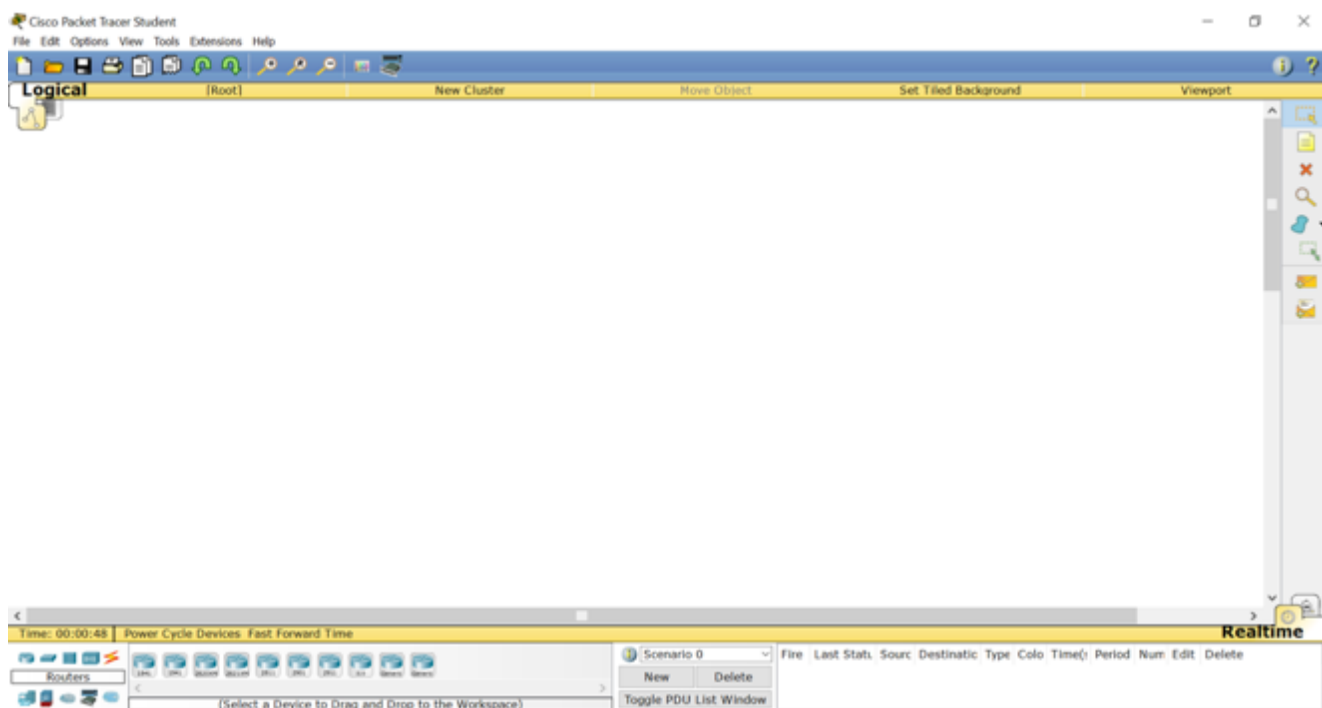


Рис. 3. Cisco Packet Tracer

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

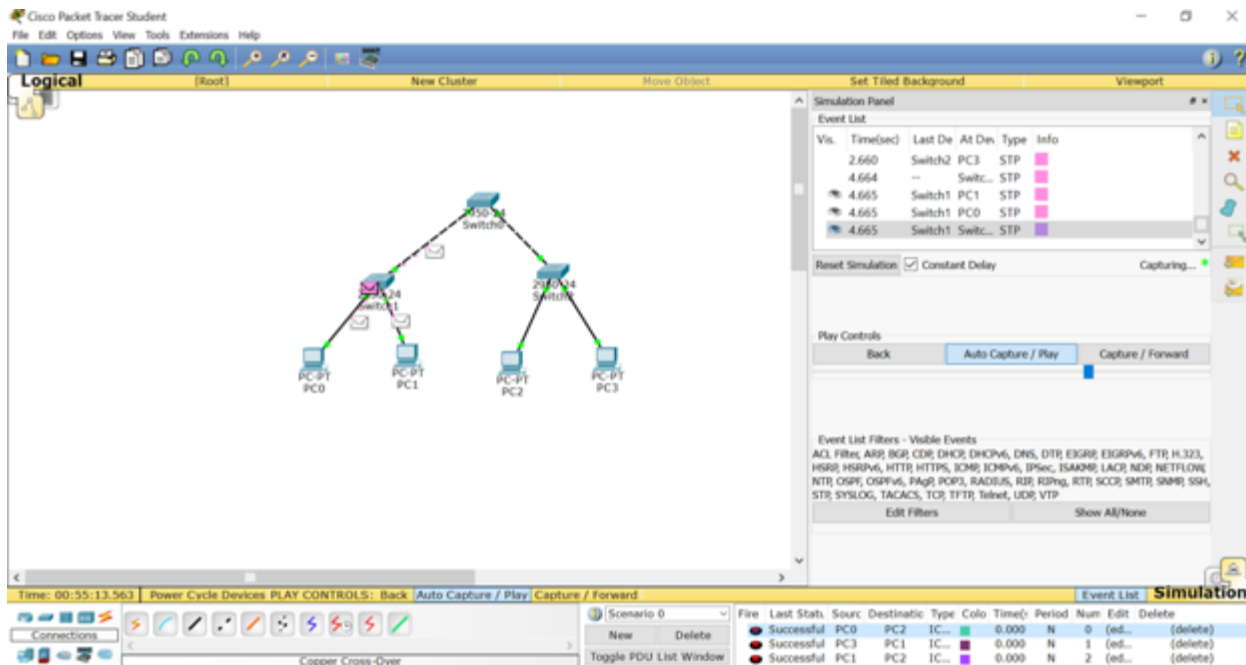


Рис. 4. Режим «Симуляции» в Cisco Packet Tracer

Однако, это не все преимущества Packet Tracer: в «Режиме симуляции» студент может не только отслеживать используемые протоколы, но и видеть, на каком из семи уровней модели OSI данный протокол задействован (см. рис. 5).

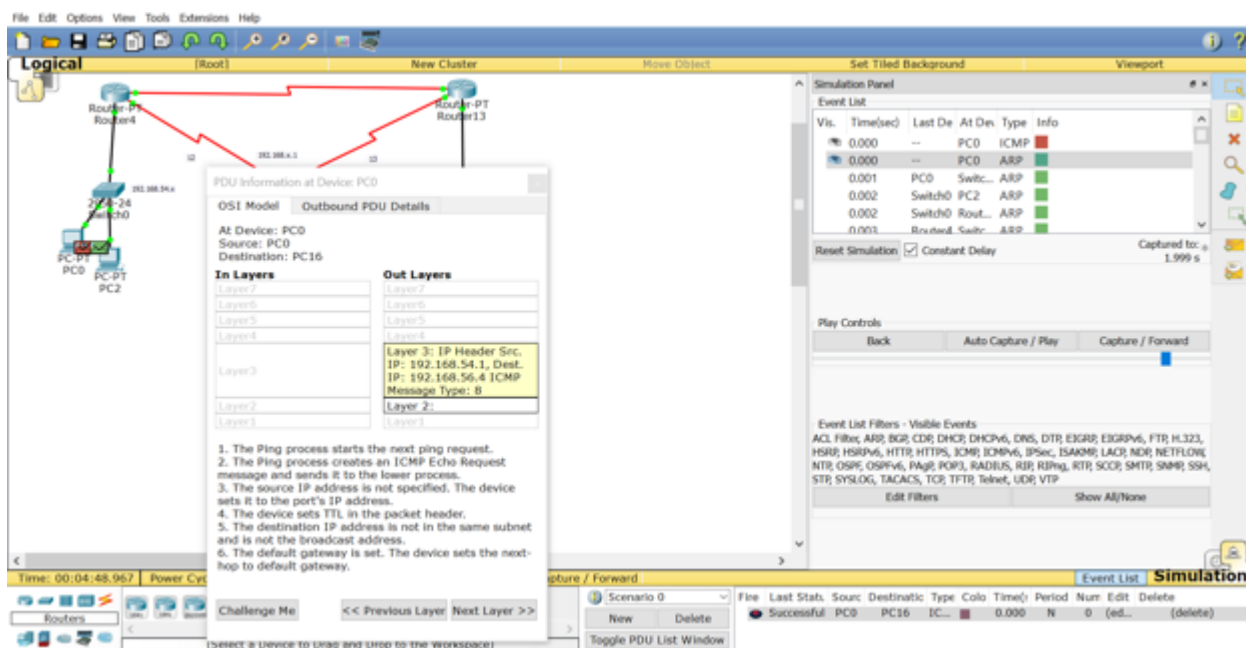


Рис. 5. Анализ семиуровневой модели OSI в Cisco Packet Tracer

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. 6).

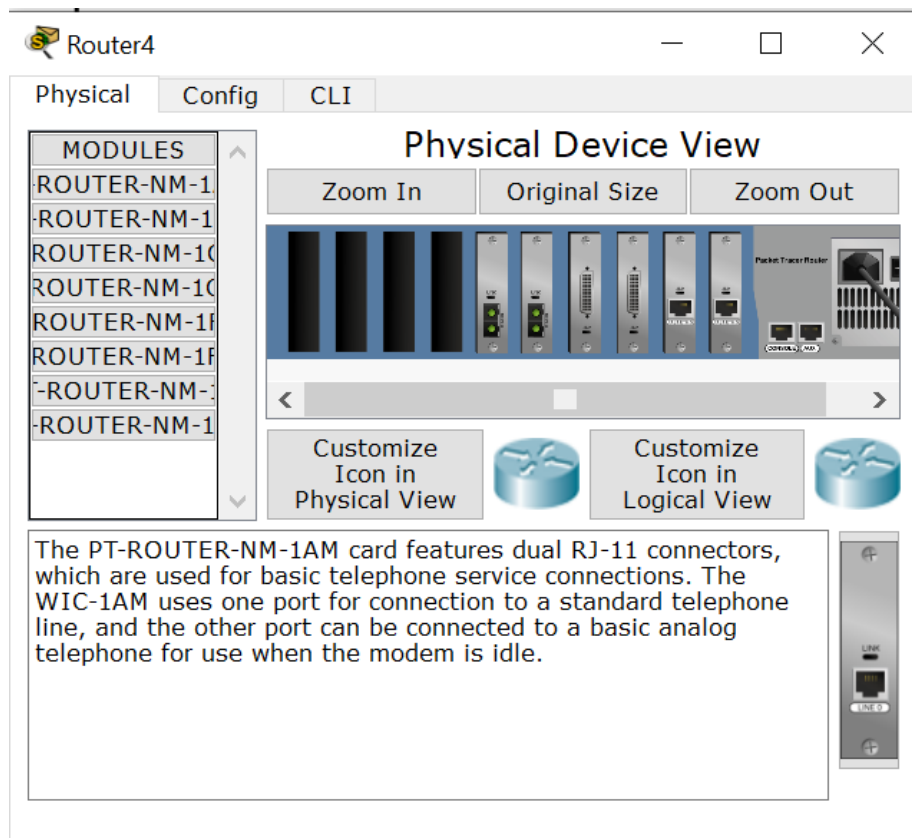


Рис. 6. Физический вид устройства.

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. 7.)

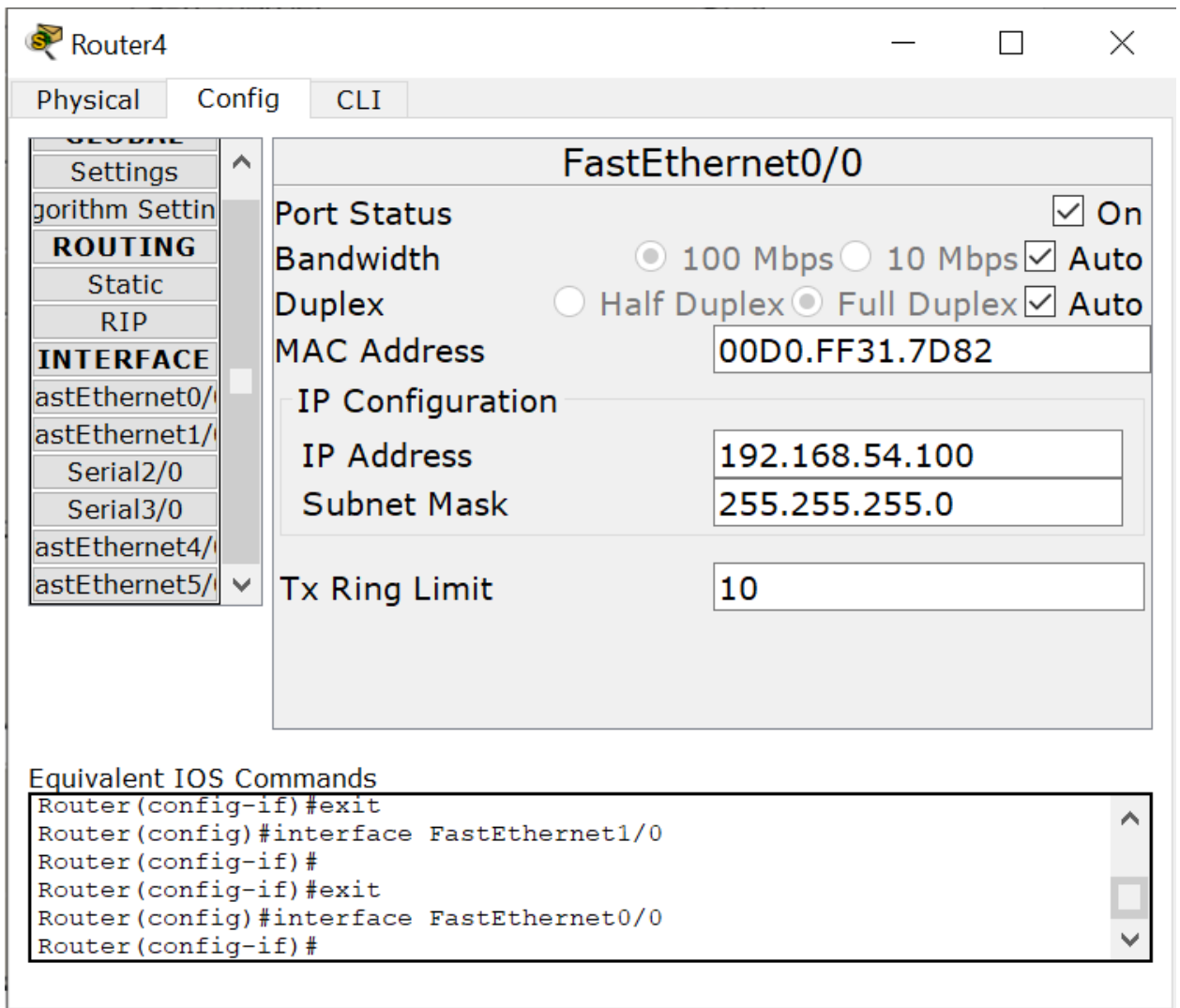


Рис. 7. Конфигурация сервера.

Третья вкладка сетевых устройств обеспечивает доступ к командной строке операционной системы IOS, с которой мы познакомимся подробнее на следующих лабораторных работах. Третья вкладка рабочих станций и серверов содержит интерфейсы доступа к различным сетевым параметрам, а также несколько клиентских приложений. (рис. 8.)

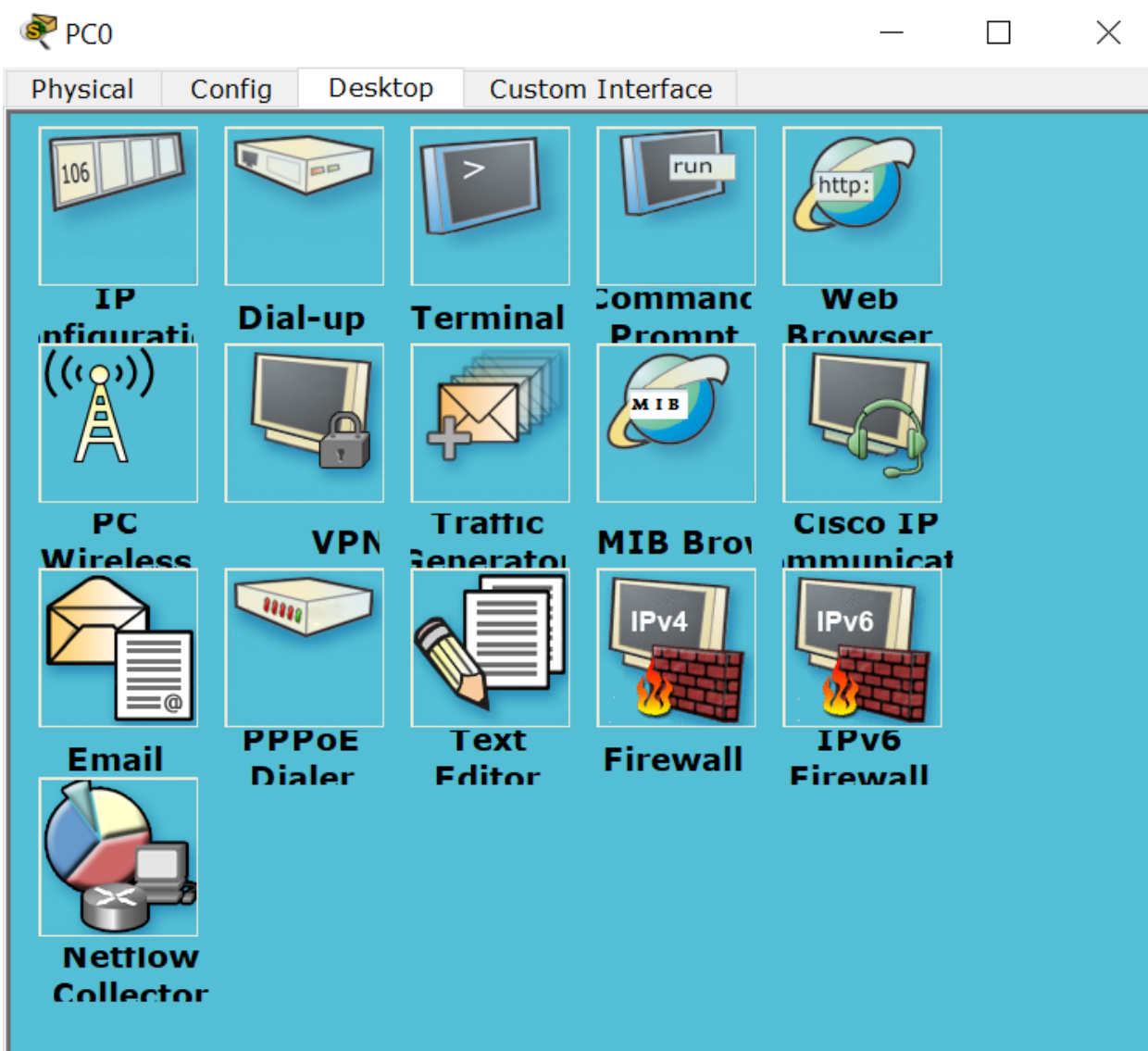


Рис. 8. Вкладка Desktop рабочей станции.

4. Командный режим операционной системы IOS

Маршрутизатор конфигурируется в командной строке операционной системы Cisco IOS. Подсоединение к маршрутизатору 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 маршрутизатору; 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>
```

Вместо слова `router` выводится имя маршрутизатора, если оно установлено.

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/
```

```
router(config-router)# /динамической маршрутизации/
```

```
router(config-line)# /терминальной линии/
```

Студенты должны 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 студенты должны определять 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.

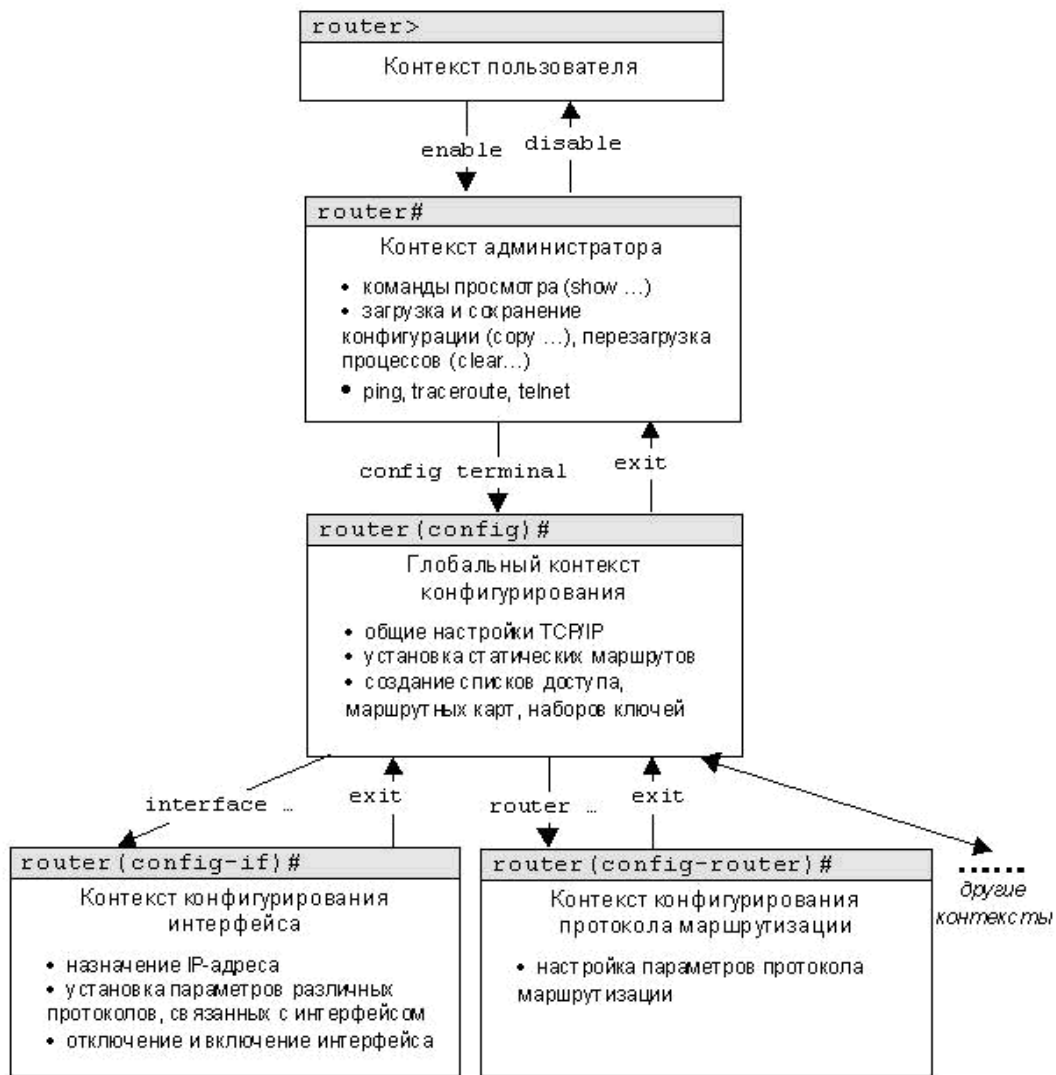


Рис. 9. Схема контекстов Cisco IOS

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.

4.1. 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.

Команда «Ip route»

Статическая маршрутизация предполагает фиксированную структуру сети: каждый маршрутизатор в сети точно знает, куда нужно отправлять пакет, чтобы он был доставлен по назначению. Для этого можно прописать статические маршруты, используя данную команду. Команда может быть записана в двух форматах:

Первый формат команды:

```
ip route A.B.C.D a.b.c.d A1.B1.C1.D1 ,
```

где A.B.C.D и a.b.c.d – сетевой адрес и маска подсети, куда необходимо доставить пакеты, A1.B1.C1.D1 – ip-адрес следующего маршрутизатора в пути или адрес сети другого маршрутизатора из таблицы маршрутизации, куда должны переадресовываться пакеты;

Второй формат команды:

```
ip route A.B.C.D a.b.c.d выходной_интерфейс_маршрутизатора
```

Примеры выполнения команды:

```
Router(config)#ip route 76.115.253.0 255.0.0.0 76.115.252.0
```

```
Router(config)#
```

Данной командой указывается маршрут, по которому пакеты из одной подсети будут доставляться в другую. Маршрут по умолчанию (Router(config)#ip route 0.0.0.0 0.0.0.0 serial 2/0) указывает, что пакеты, предназначенные узлам в другой подсети должны отправляться через данный шлюз.

Команда «Hostname»

Данная команда используется для изменения имени конфигурируемого устройства.

Формат команды:

```
hostname новое_имя
```

Пример выполнения команды:

```
R1(config)#
```

```
Router(config)#hostname R1
```

Как видно, маршрутизатор поменял своё имя с Router на R1.

Команда «Router rip»

RIP – Routing Information Protocol – протокол динамической маршрутизации. При его использовании отпадает необходимость вручную прописывать все маршруты – необходимо лишь указать адреса сетей, с которыми нужно обмениваться данными. Данная команда

позволяет включить rip-протокол.

Пример выполнения команды:

```
Router(config-router)#
```

```
Router(config)#router rip
```

Данная команда включает rip-протокол на данном маршрутизаторе. Дальнейшая настройка производится из соответствующего контекста маршрутизации, описанного отдельно.

4.2. 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 окончное 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.

4.3. 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 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

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 энергонезависимая 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#

Выводится информация о включенных протоколах маршрутизации.

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.

4.4. 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.

4.5. Контекст конфигурирования маршрутизации

Команда «Network»

Данной командой указывают адреса сетей, которые будут доступны данному маршрутизатору.

Формат команды:

network A.B.C.D , где A.B.C.D – адрес сети

Пример выполнения команды:

```
Router(config-router)#network 192.168.3.0
```

Данная команда означает, что пакеты, направленные в подсеть 192.168.3.0 будут отправляться через данный шлюз.

5. Задания.

Лабораторная работа №4.

Задание: построить локальную сеть, состоящую из сегмента на основе коммутатора из 5 компьютеров и сервера. Коммутатор соединен с маршрутизатором, к которому также подключен сервер. Необходимо задать статические IP адреса сетевым интерфейсам маршрутизаторов, локальных компьютеров и серверов. Установить на маршрутизаторах пароли для доступа к привилегированному режиму. Настроить маршрутизацию по протоколу RIP. Добиться возможности пересылки данных по протоколу ICMP между всеми объектами сети.

Расставляем на рабочем поле необходимые узлы, используя браузер в нижней части окна (рис. 10). Соединяем узлы в соответствии с заданием с помощью витой пары. Сервер с маршрутизатором соединяется кросс-овером. Соединения, обозначенные зеленым цветом, указывают, что они активны, оранжевым – что они на стадии подключения, красным – не рабочие.

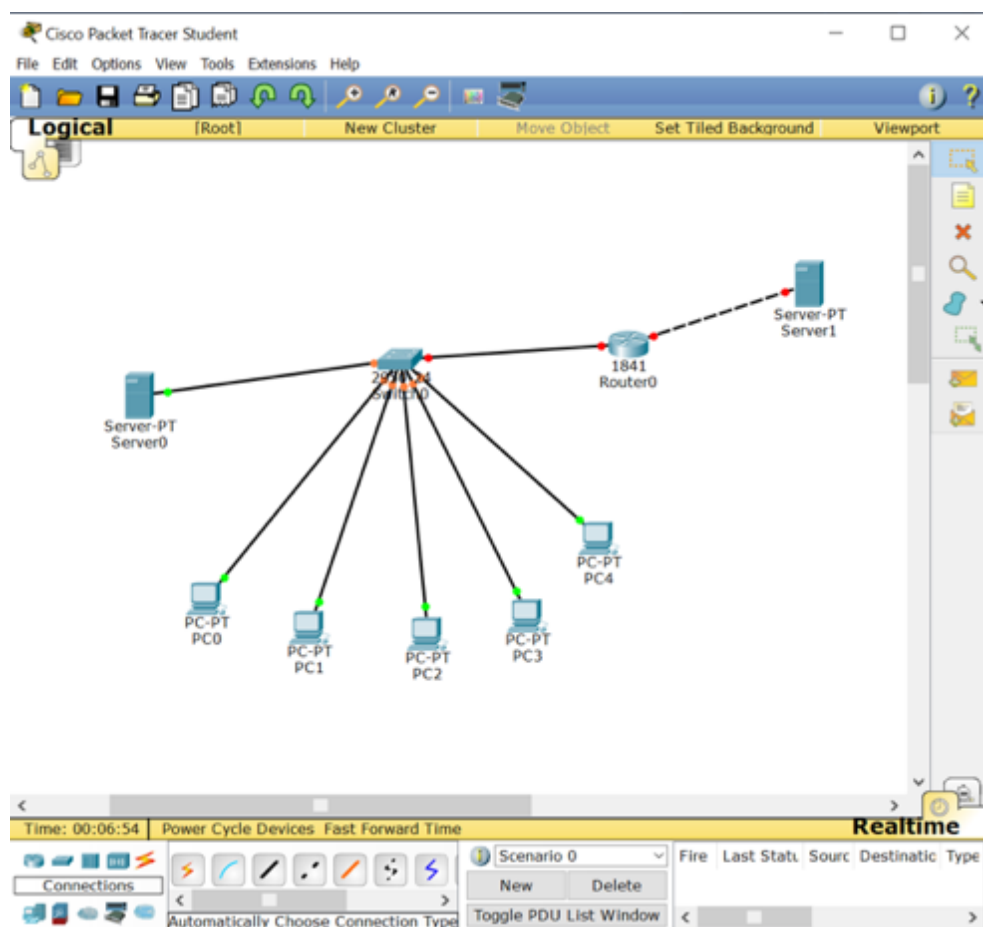


Рис. 11. Рабочее поле

Зададим ip-адреса узлам сегмента в диапазоне 192.168.0.x, а серверу, подключенному к маршрутизатору – 192.168.1.1. Маска подсети – 255.255.255.0. (Рис. 12).

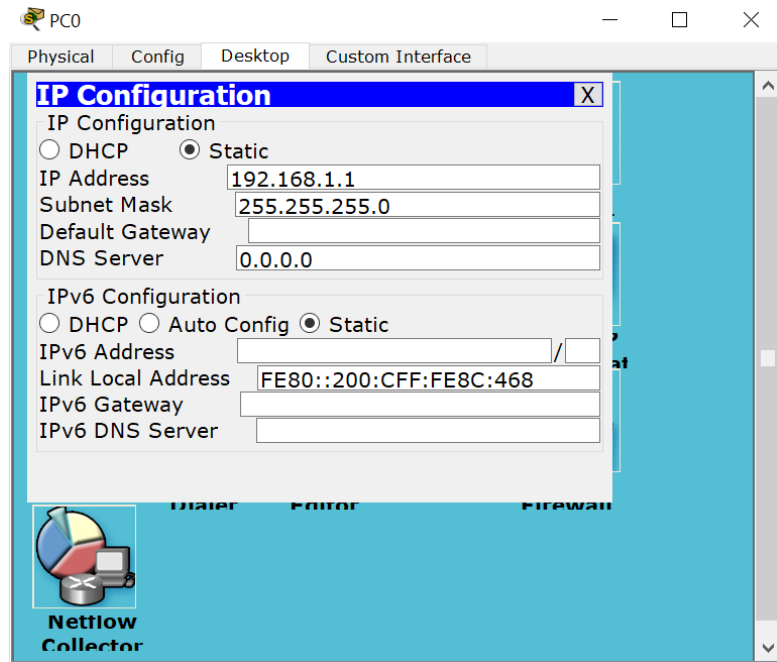


Рис. 12. IP конфигурация рабочей станции.

Зададим соответствующие ip адреса на интерфейсах маршрутизатора и включим эти порты. (Рис. 13). Адрес каждого интерфейса маршрутизатора необходимо настроить в качестве шлюза по умолчанию на всех компьютера соответствующей подсети.

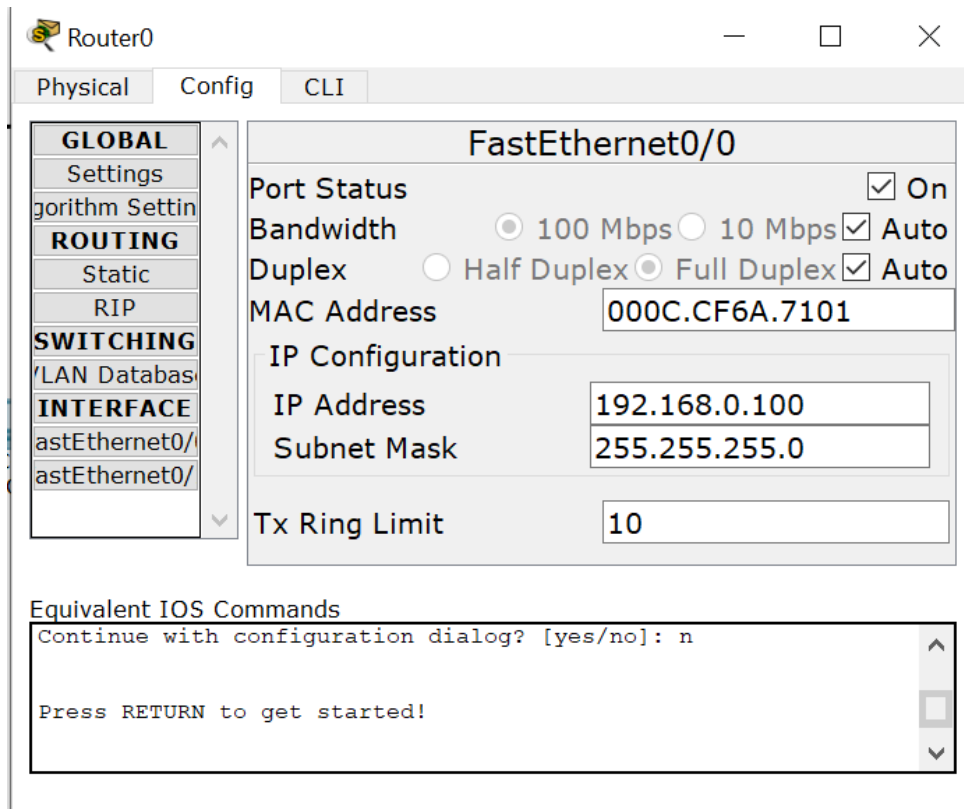


Рис. 13. IP конфигурация маршрутизатора.

Зайдем в Command Line Interface маршрутизатора и с помощью команды `enable secret` зададим пароль для доступа в привилегированный режим и сохраним конфигурацию. (Рис. 14).

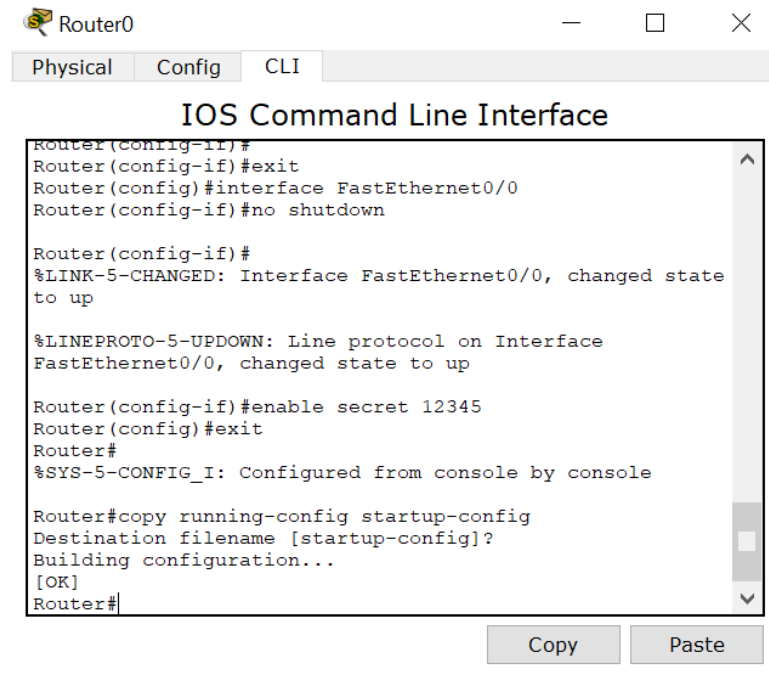


Рис. 14. Работа в Command Line Interface.

Чтобы настроить шлюз по умолчанию на коммутаторе необходимо выполнить команду `ip default-gateway` в CLI. (Рис15.)

S1> en // переходим в привилегированный режим EXEC

S1# conf t // режим глобальной конфигурации

S1(config)# ip default-gateway 192.168.1.1 // устанавливаем шлюз по умолчанию

S1(config)# exit // выход из режима глобальной конфигурации

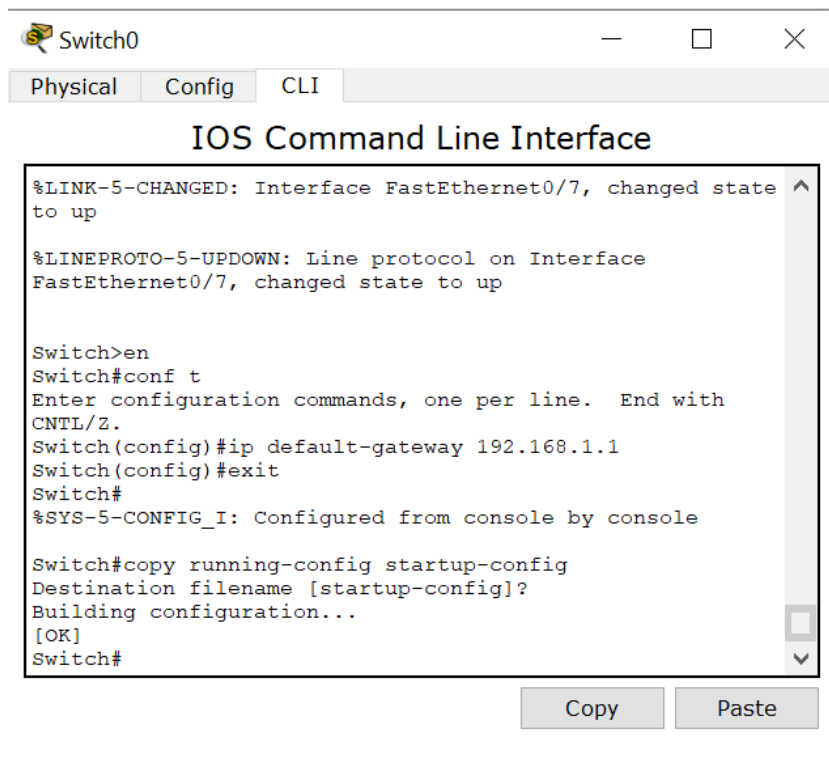


Рис. 15. Работа в Command Line Interface.

Для настройки маршрутизации по протоколу RIP откроем вкладку Config в окне свойств маршрутизатора и выберем пункт RIP. Зададим там адреса всех подсетей, которым разрешено общение. (Рис. 16).

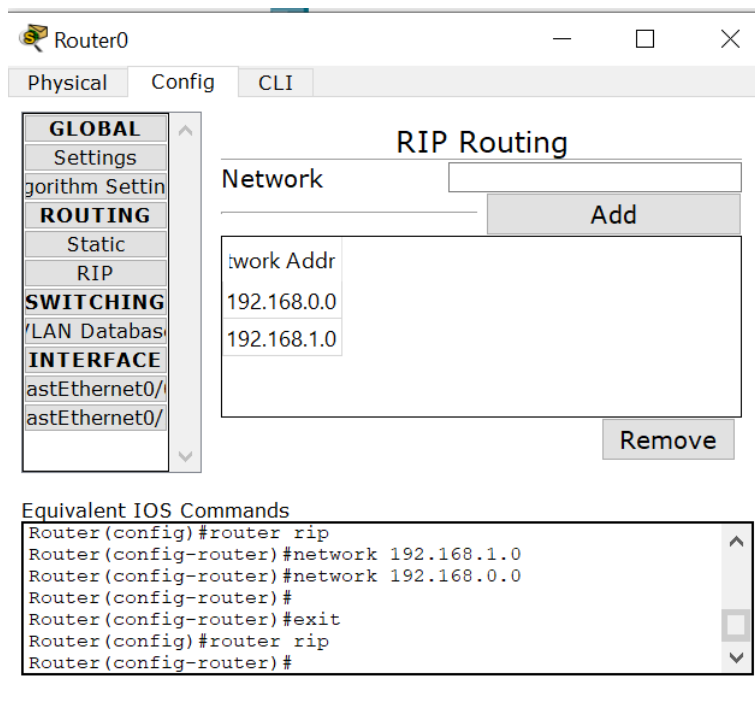


Рис. 16. Настройка маршрутизации по протоколу RIP.

Проверяем доступность рабочих станций друг для друга. Для этого в правом столбце выбираем инструмент Add simple PDU и выбираем станцию-отправитель и станцию-получатель. Убеждаемся, что передача завершена успешно. (Рис. 17).

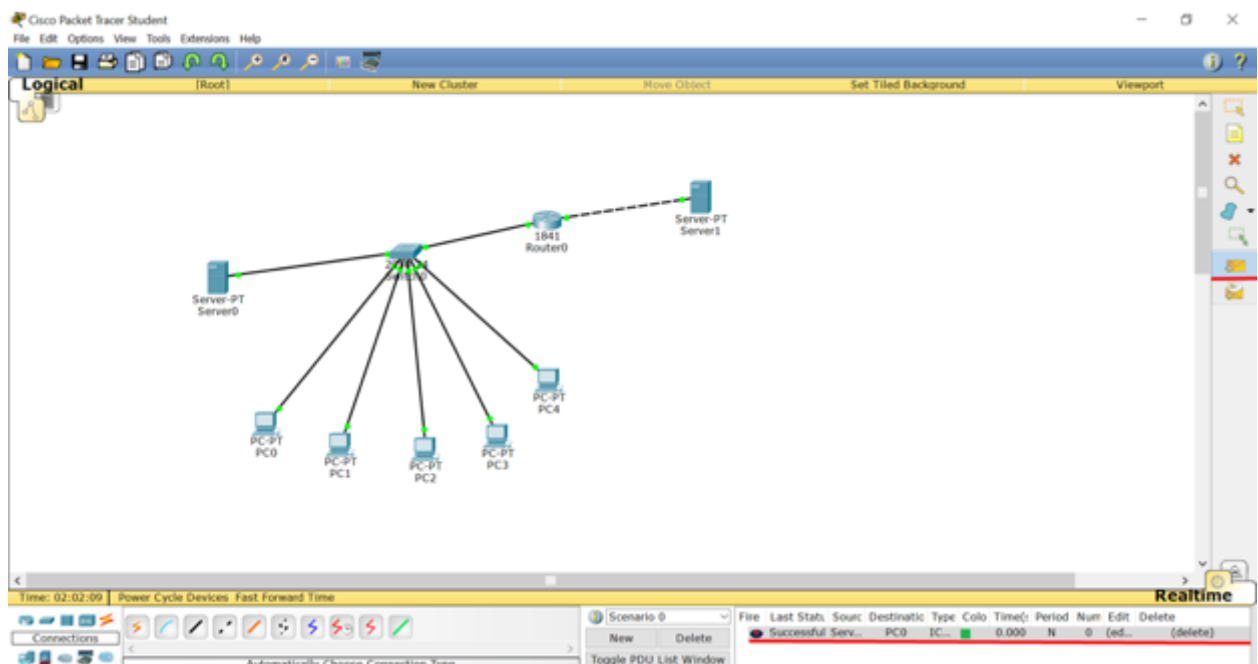


Рис. 17. Проверка доступности узлов в сети.

Для проверки работы сети, необходимо выполнить команды ping, tracert. В качестве параметра указать ip-адрес получателя. Команды необходимо писать в командной строке компьютеров внутри эмулятора Cisco.

Содержание отчета.

1. Титульный лист
2. Задание и вариант
3. Скриншоты с подписями по ходу выполнения лабораторной работы
4. Скриншоты финальной части – установка паролей, настройка маршрутизации, возможность пересылки данных по протоколу ICMP между всеми объектами сети.

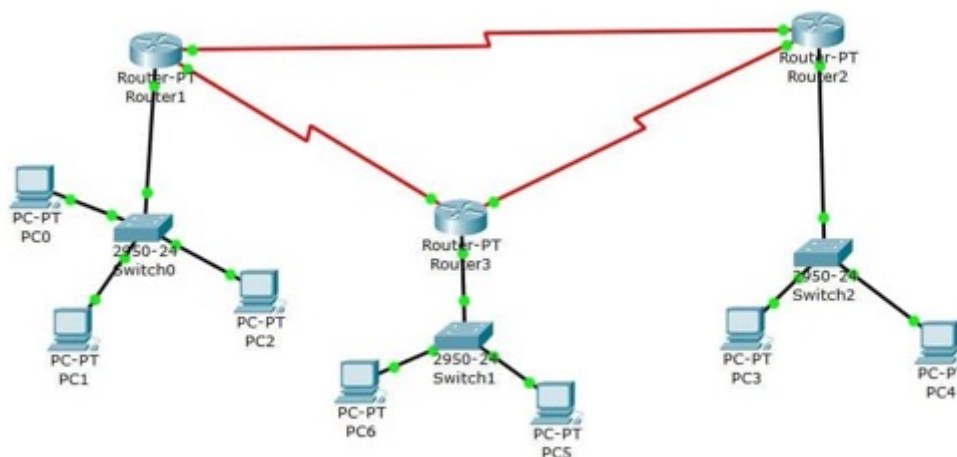
Контрольные вопросы.

1. Сетевое оборудование и его функции.
2. Стек протоколов TCP/IP.
3. Отличие между различными стандартами сетей Ethernet.
4. Формат кадров в сети Ethernet.

5. Сети wi-fi – основные стандарты и принципы работы.
6. Назначение шлюза.
7. Маршрутизация.
8. Эталонная модель OSI/ISO.
9. Выполнить команды ping и tracert в командной строке компьютеров в эмуляторе

Лабораторная работа №5. Статическая маршрутизация.

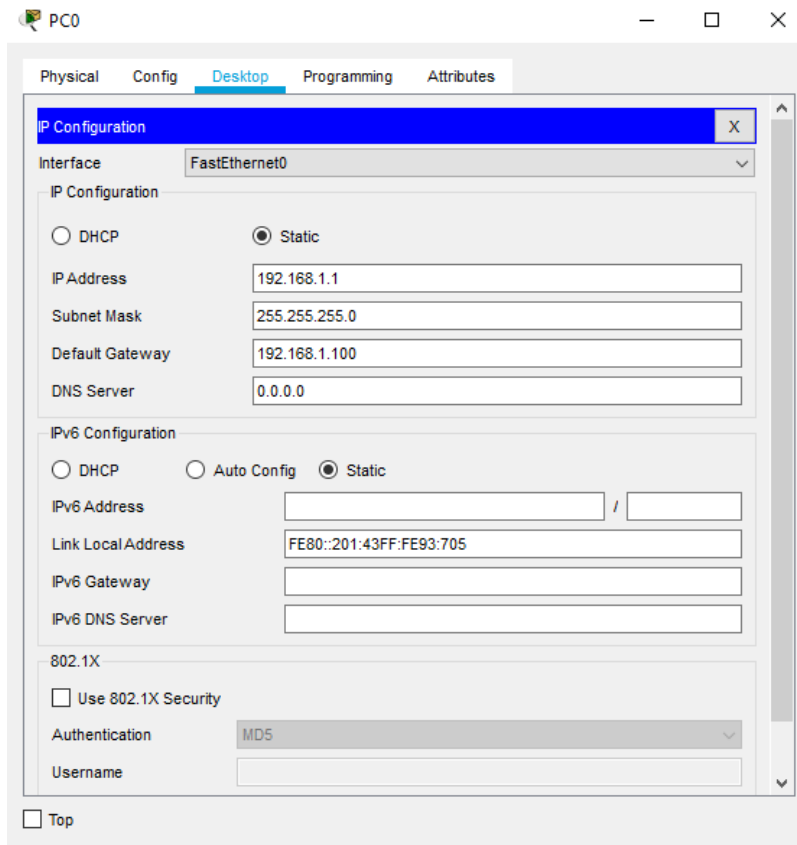
Построить сеть из трех сегментов, каждый из которых состоит из С, D и E рабочих станций соответственно. Каждый сегмент построен на базе коммутатора, и каждый коммутатор подключен к отдельному маршрутизатору.



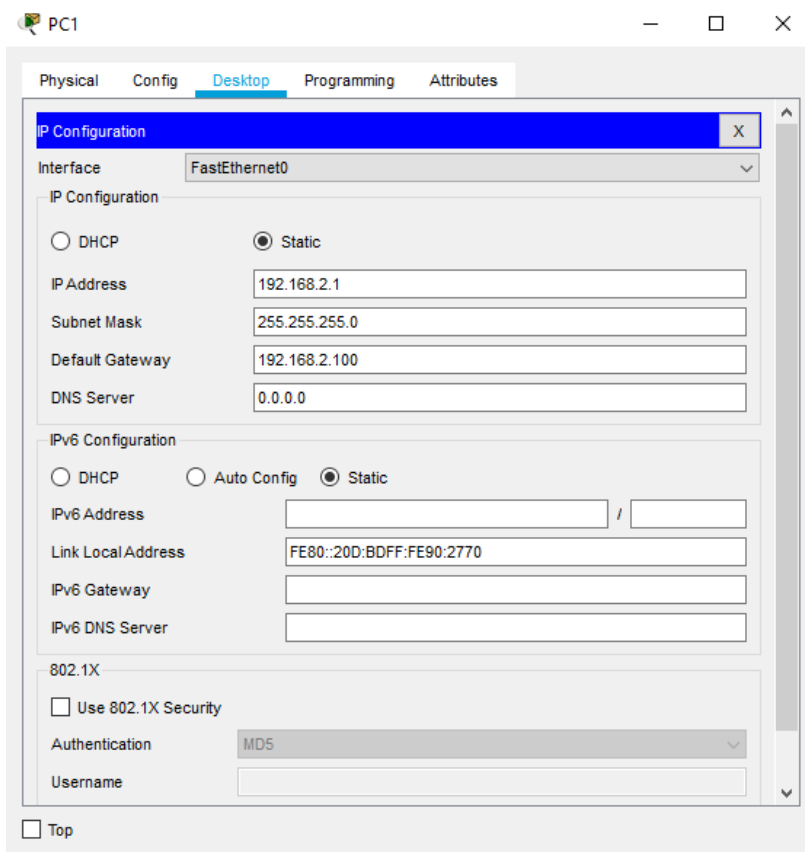
Шлюзом для каждого сегмента служит соответствующий маршрутизатор. Маршрутизаторы соединены между собой с помощью интерфейса DTE. Необходимо задать IP адреса сетевым интерфейсам маршрутизаторов и локальных компьютеров. IP адреса должны быть заданы в диапазоне 192.G.N.x, где G – номер группы (для ИУ 151-155, для РТ 156), N – номер варианта по списку плюс 0, 100 и 200 для 3 сетей соответственно. Задать параметр Clock Rate на маршрутизаторах. Установить на маршрутизаторах пароли для доступа к привилегированному режиму. Настроить статическую маршрутизацию и добиться возможности пересылки данных по протоколу ICMP между всеми объектами сети.

Сегменты PC настраиваются следующим образом:

1. Кликаем на нужный сегмент PC. Config -> FastEthernet0, назначаем IP адрес, у каждого сегмента он уникален. Также вводим Subnet mask
2. Во вкладке Setting задаем gateway



Puc. 2.16.



Puc. 2.17.

Сегменты Router настраиваются следующим образом:

1. Кликаем на нужный сегмент Router. Config -> FastEthernet0, назначаем IP адрес, у каждого сегмента он уникален. Первые три бита должны совпадать с IP PC, с которого будет в последствии получен пакет данных. Также вводим Subnet mask
2. В Serial 2.0 задаем IP. Четвёртый бит должен совпадать с третьим битом PC с которого будет получен пакет данных. Третий бит должен совпадать с третьим битом аналогичного параметра другого роутера, на который будет этот пакет данных передаваться. А также с третьим битом Gateway обоих PC

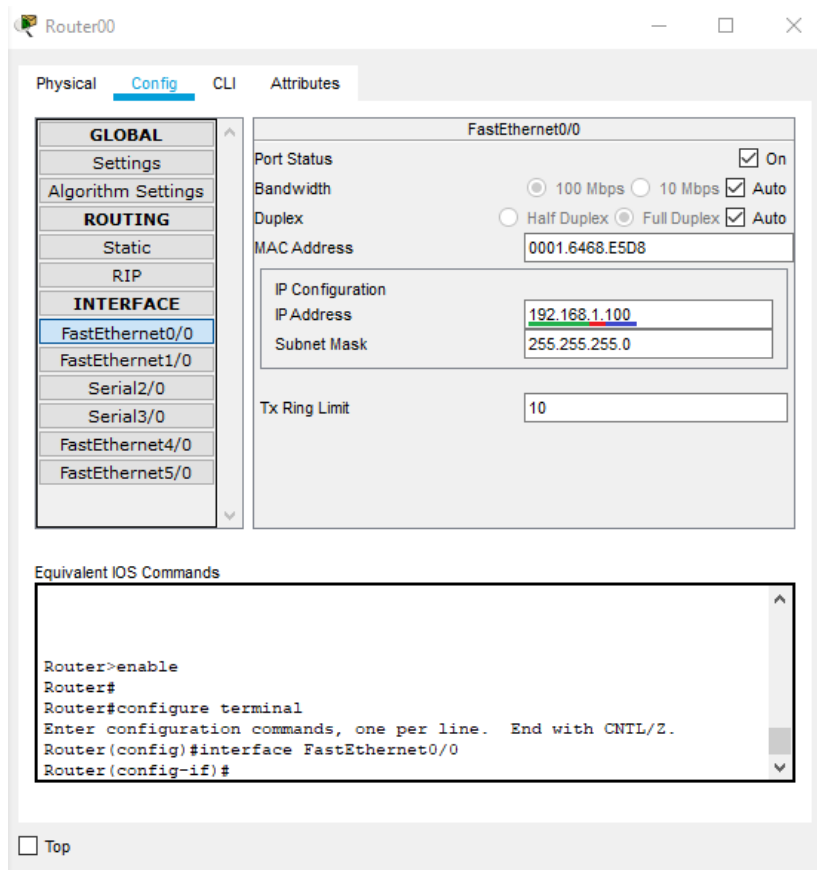


Рис. 2.18.

Router11

Physical **Config** CLI Attributes

GLOBAL

- Settings
- Algorithm Settings

ROUTING

- Static
- RIP

INTERFACE

- FastEthernet0/0
- FastEthernet1/0
- Serial2/0
- Serial3/0
- FastEthernet4/0
- FastEthernet5/0

FastEthernet0/0

Port Status On

Bandwidth 100 Mbps 10 Mbps Auto

Duplex Half Duplex Full Duplex Auto

MAC Address 0002.17CC.7977

IP Configuration

IP Address 192.168.2.100

Subnet Mask 255.255.255.0

Tx Ring Limit 10

Equivalent IOS Commands

```
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#
```

Top

Puc. 2.19.

Router00

Physical **Config** CLI Attributes

GLOBAL

- Settings
- Algorithm Settings

ROUTING

- Static
- RIP

INTERFACE

- FastEthernet0/0
- FastEthernet1/0
- Serial2/0
- Serial3/0
- FastEthernet4/0
- FastEthernet5/0

Serial2/0

Port Status On

Duplex Full Duplex

Clock Rate 2000000

IP Configuration

IP Address 192.168.100.1

Subnet Mask 255.255.255.0

Tx Ring Limit 10

Equivalent IOS Commands

```
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial2/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial2/0
Router(config-if)#
```

Top

Puc. 2.20.

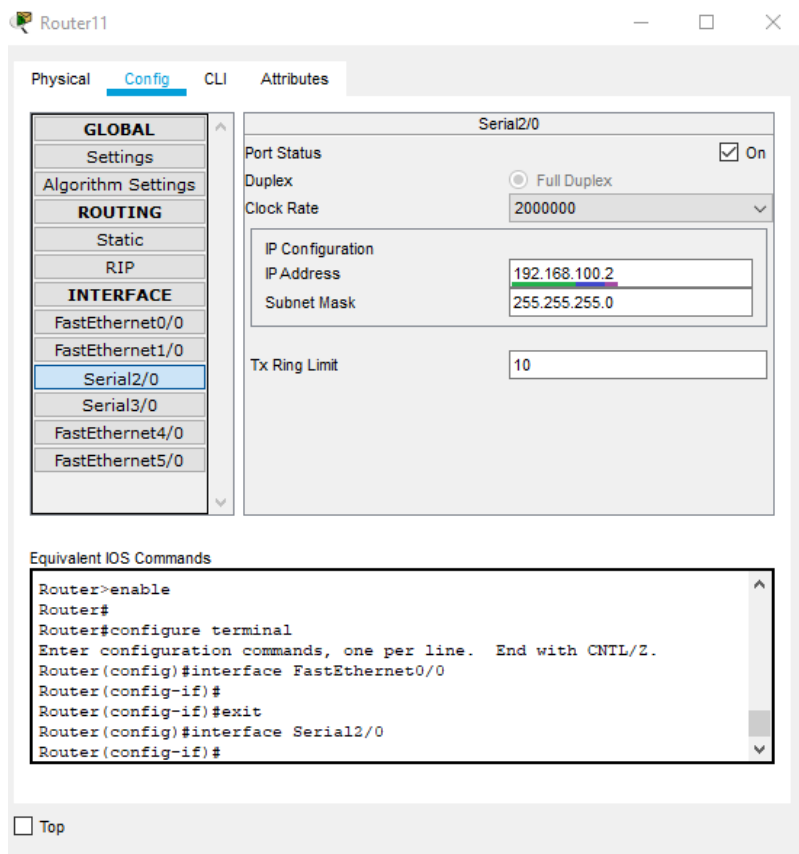


Рис. 2.21.

Шлюзом для каждого сегмента служит соответствующий маршрутизатор. Маршрутизаторы соединены между собой с помощью интерфейса DTE. Необходимо задать IP адреса сетевым интерфейсам маршрутизаторов и локальных компьютеров. IP адреса должны быть заданы в диапазоне 192.G.N.x, где G – номер группы (для ИУ 151-155, для РТ 156), N – номер варианта по списку плюс 0, 100 и 200 для 3 сетей соответственно. Задать параметр Clock Rate на маршрутизаторах. Установить на маршрутизаторах пароли для доступа к привилегированному режиму. Настроить статическую маршрутизацию и добиться возможности пересылки данных по протоколу ICMP между всеми объектами сети.

Router11

Physical Config CLI Attributes

GLOBAL

- Settings
- Algorithm Settings

ROUTING

- Static
- RIP

INTERFACE

- FastEthernet0/0
- FastEthernet1/0
- Serial2/0
- Serial3/0
- FastEthernet4/0
- FastEthernet5/0

Static Routes

Network: 192.168.2.0
Mask: 255.255.255.0
Next Hop: 192.168.100.2

Add

Network Address

192.168.2.0/24 via 192.168.100.2

Remove

Equivalent IOS Commands

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

Top

Puc. 2.21.

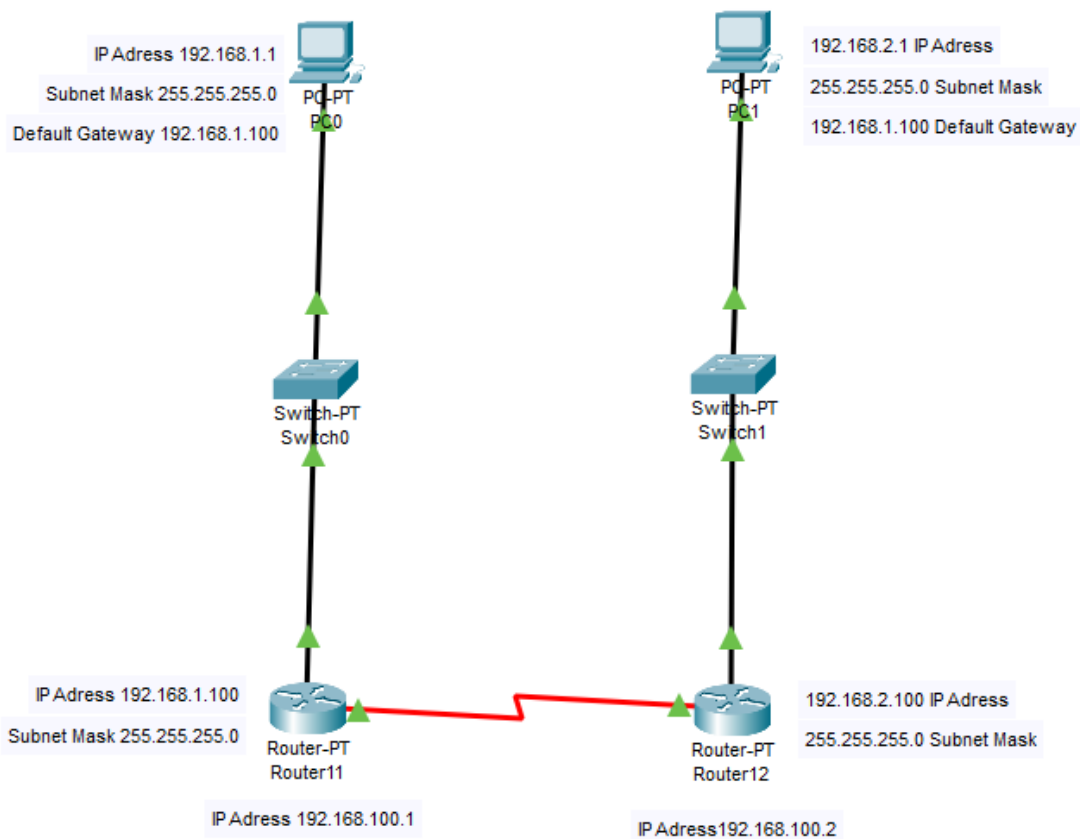


Рис. 2.22.

Содержание отчета.

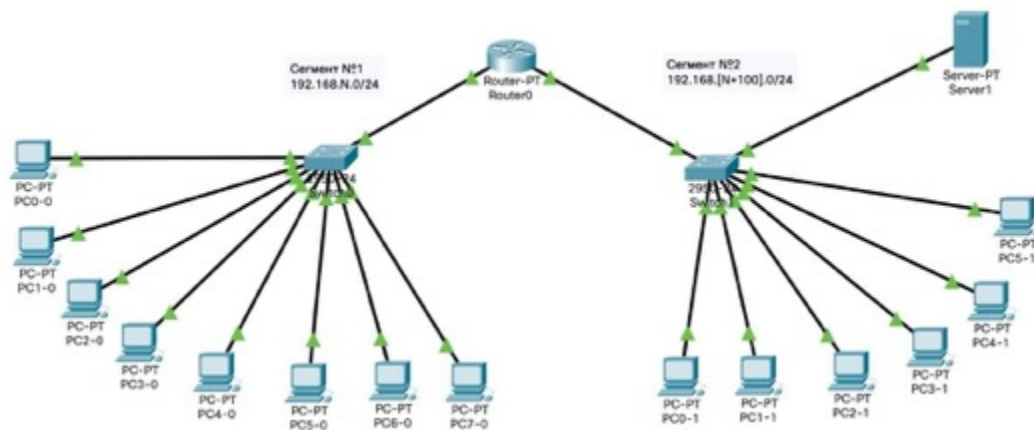
1. Титульный лист
2. Задание и вариант
3. Скриншоты с подписями по ходу выполнения лабораторной работы
4. Скриншоты финальной части – установка паролей, настройка маршрутизации

Контрольные вопросы.

1. Сетевое оборудование и его функции.
2. Стек протоколов TCP/IP.
3. Отличие между различными стандартами сетей Ethernet.
4. Формат кадров в сети Ethernet.
5. Сети wi-fi – основные стандарты и принципы работы.
6. Назначение шлюза.
7. Маршрутизация.
8. Эталонная модель OSI/ISO.

Лабораторная работа №6. Динамическое распределение IP-адресов и DNS.

Построить сеть, состоящую из двух сегментов на основе коммутаторов. Сегмент №1 содержит В рабочих станций, сегмент №2 – С рабочих станций и сервер. Маршрутизатор является шлюзом. Сегменты соединены маршрутизатором.



В первом сегменте IP адреса раздаются маршрутизатором динамически в диапазоне 192.G.N.x, где G – номер группы (для ИУ 151-155, для РТ 156), N – номер варианта по списку. Во втором сегменте IP адреса заданы статически и заданы в диапазоне 192.G.N1.x, где G – номер группы (для ИУ 151-155, для РТ 156), N1 – номер варианта по списку плюс 100. Настроить маршрутизацию по протоколу RIP. Сервер является DNS и веб-сервером. URL страницы должен содержать фамилию студента. Настроить на сервере веб-страницу произвольного формата. Добиться возможности пересылки данных по протоколу ICMP между всеми объектами сети. Добиться просмотра веб-страницы с сервера во встроенных браузерах рабочих станций.

Контекст конфигурирования динамического распределения ip адресов.

Вход в данный контекст осуществляется из контекста администратора с помощью команды `ip dhcp pool`.

Команда «`ip dhcp pool`»

Данная команда организует набор динамического распределения ip-адресов.

Формат команды:

`ip dhcp pool название_набора`

Пример выполнения команды:

```
Router(config)#ip dhcp pool POOL1
```

```
Router(dhcp-config)#
```

В данном примере организуется набор динамического распределения ip-адресов под именем POOL1.

Команда «network»

Данная команда задает диапазон IP адресов выбранного набора.

Формат команды:

```
network название_набора [маска]
```

Пример выполнения команды:

```
Router(dhcp-config)#network 192.168.0.0 255.255.255.0
```

В данном примере создается диапазон адресов 192.168.0.x с маской подсети 255.255.255.0.

Команда «default-router»

При включении динамического распределения ip-адресов клиенты начинают посылать пакеты маршрутизатору, назначенному по умолчанию. Его IP адрес должен быть из той же подсети. Данная команда задает этот маршрутизатор.

Формат команды:

```
default-router адрес_1 [адрес_2, ...]
```

Пример выполнения команды:

```
Router(dhcp-config)#default-router 192.168.0.1
```

Команда «dns-server»

Данная команда задает адрес DNS сервера.

Формат команды:

```
dns-server адрес_1 [адрес_2, ...]
```

Пример выполнения команды:

```
Router(dhcp-config)#dns-server 192.168.0.1
```

Содержание отчета.

1. Титульный лист
2. Задание и вариант
3. Скриншоты с подписями по ходу выполнения лабораторной работы
4. Скриншоты финальной части – возможность пересылки данных по протоколу ICMP, возможность просмотра веб-страницы с сервера во встроенных браузерах рабочих станций.

Контрольные вопросы.

1. Сетевое оборудование и его функции.
2. Стек протоколов TCP/IP.
3. Отличие между различными стандартами сетей Ethernet.
4. Формат кадров в сети Ethernet.
5. Сети wi-fi – основные стандарты и принципы работы.
6. Назначение шлюза.
7. Маршрутизация.
8. Эталонная модель OSI/ISO.

6. Варианты заданий.

Таблица 2. Варианты параметров

Вариант	A	B	C	D	E
1	2	3	4	9	10
2	3	4	5	9	2
3	4	5	6	7	8
4	5	6	3	8	9
5	6	7	8	2	3
6	7	4	3	6	2
7	8	9	5	2	3
8	9	4	2	3	4
9	7	3	5	4	6
10	2	4	6	8	3
11	4	6	8	3	1
12	6	8	5	1	3

13	8	4	1	3	5
14	4	6	3	5	7
15	1	3	5	7	2
16	3	5	7	2	4
17	5	7	2	4	6
18	7	3	4	6	8
19	2	4	6	8	4
20	4	6	8	5	2
21	2	5	8	3	6
22	5	8	3	6	9
23	8	3	6	9	4
24	3	6	9	4	7
25	6	9	4	7	3