Золотых М.О., версия 2023.04

ЗНАКОМСТВО С ОПЕРАЦИОННОЙ СИСТЕМОЙ IOS И СИМУЛЯТОРОМ CISCO PACKET TRACER

Описание работы

Неотъемлемой частью компьютерной сети являются промежуточные устройства. Они предназначены для перемещения пакетов между физическими средами и сетями, а также для выполнения над ними транспортных операций: маркировка, контроль целостности, модификация, формирование очередей, удаление и т.д. При этом, в общем случае, промежуточные устройства не генерируют и не затрагивают передаваемые в сети пользовательские данные.

К промежуточным устройствам относятся: модемы (работают с физическим сигналом), коммутаторы (работают с Ethernet и другими L2 заголовками), точки доступа (например, Wi-Fi), маршрутизаторы (работают с IP заголовками), МСЭ (могут работать с любым уровнем модели ВОС) и др. Очень часто функции нескольких устройств совмещаются в одном. Например, коммутатор с функциями маршрутизации называют L3-коммутатором; маршрутизатор часто содержит в себе хотя бы частичный функционал МСЭ; в домашних сетях часто точка доступа совмещается с маршрутизатором и т.д.

Промежуточные устройства, как правило, обладают специфическим аппаратным обеспечением (позволяющими обрабатывать сетевые пакеты быстрее, чем процессоры общего назначения) и специализированной ОС. Эти ОС гораздо более разнообразны, чем их серверные и персональные аналоги, хотя некоторые из них используют ядро Linux. Большинство производителей сетевого оборудования разрабатывают собственные операционные системы под своё оборудование: иногда под отдельные линейки устройств, а иногда под целые классы. Одной из наиболее распространённых ОС является Cisco IOS [1] (Internetwork Operating System – Межсетевая Операционная Система). Это проприетарная ОС фирмы Cisco Systems.

В эпоху взрывного роста компьютерных сетей (1990-е, 2000-е гг.) с ОС IOS было знакомо большинство сетевых администраторов. Это объяснялось рядом факторов. Во-первых, огромной долей устройств Cisco на телекоммуникационном рынке. Во-вторых, тем, что Cisco смогла сделать универсальную ОС для большей части коммутаторов, маршрутизаторов и точек доступа. Т.е. администратор, освоивший работу с одним устройством, мог по аналогии настраивать и другие (производители, которые меняли интерфейсы в каждой линейке заслужи-

[1] Операционная система iOS от Apple никак технически не связана с IOS, но арендует её торговую марку

вали свою долю ненависти инженерного персонала). И в-третьих, огромной методической базой: учебниками, справочниками, фирменными курсами и аттестационными программами, подготовленными Cisco.

#Дополнительно
У IOS есть различные модификации: IOS, IOS-XE (на базе ядра Linux), IOS-XR (на базе ядра QNX), а также родственная ОС того же разработчика: NX-OS (для коммутаторов ЦОД и сетей хранения данных). Но все эти ОС обладают схожими интерфейсами и принципами конфигурирования. Различия заключаются в архитектуре программного обеспечения и способах работы с аппаратным обеспечением. Помимо названных существовали ещё операционные системы CatalystOS и SAN-OS, но на текущий момент они устарели и не используются.

В конце концов, популярность ОС привела к тому, что интерфейсы IOS начали массово копировать и другие производители, даже не смотря на патентную защиту. Например, китайский Huawei или российский Eltex используют очень похожие на IOS интерфейсы. Специалист, хорошо знакомый с ОС IOS, способен быстро обучиться работе с аналогичными системами.

#Дополнительно
IOS и подобные ей операционные системы оперируют концепцией присвоения VLAN и других параметров для каждого порта. Существуют и другие подходы в операционных системах устройств D-Link, Extreme, Mellanox и др. В этих устройствах для свойств настраивается список портов. Преимущество одного подхода над другим иногда вызывает ожесточённые споры среди сетевых специалистов.

Запуск операционной системы IOS возможен не только на полноценном аппаратном обеспечении, но и в различных симуляторах и эмуляторах.

Симулятор – это программное обеспечение, которое имитирует поведение объекта. Симулятор обладает собственным программным кодом, как правило меньшей функциональности. Симуляторы удобны для целей обучения, но плохо подходят, например, для сложных исследований и поиска уязвимостей, так как имеют собственный программный код и, как следствие, набор слабых мест. Наиболее популярным симулятором IOS является фирменный **Cisco Packet Tracer** (**CPT**)[1].

Эмулятор – это программное обеспечение, которое позволяет запускать оригинальную операционную систему в виде виртуальной машины. Эмуляторы более сложны в развёртывании, но более точно отражают поведение исследуемого объекта. Наиболее популярными эмуляторами IOS являются **GNS3**, **EVE-NG**.

[1] В Cisco PIX/ASA/NGFW есть инструмент packet-tracer, однако несмотря на почти идентичное название – он не имеет никакого отношения к CPT

Данная работа посвящена знакомству с **IOS CLI** (**Command Line Interface** – **интерфейс командной строки**), как наиболее распространённому способу управления сетевыми устройствами. Все задания выполняются в симуляторе CPT.

Системные требования:

- компьютер с ОС Windows 7 или выше с доступом к сети Интернет;
- симулятор Cisco Packet Tracer версия не ниже 8.0.

Командная строка в Cisco IOS

Существуют различные способы управления IOS устройством, такие как веб-интерфейс, SNMP и другие (с некоторыми из них вы познакомитесь в других лабораторных работах). Однако, наиболее распространённым и универсальным является интерфейс командной строки. Доступ к CLI можно получить различными способами: при помощи прямого ввода/вывода по протоколу UART/RS-232 (COM-порт в компьютере) или удалённо, через TCP/IP сеть по протоколам telnet и SSH.

Доступ по RS-232 называется **консольным доступом** и является единственным доступным, при отсутствии сетевых подключений, т.е. в состоянии устройства «из коробки» (Рисунок 1). В отличии от устройства класса SOHO, профессиональное сетевое оборудование часто не имеет сетевых настроек по умолчанию, поэтому нуждается в предварительной настройке. Также управление по консоли ещё относят к **внеполосному** управлению, которое позволяет сохранить доступ к управлению устройством в моменты перегрузки сети, под воздействием атаки, при ошибках конфигурации и т.д.

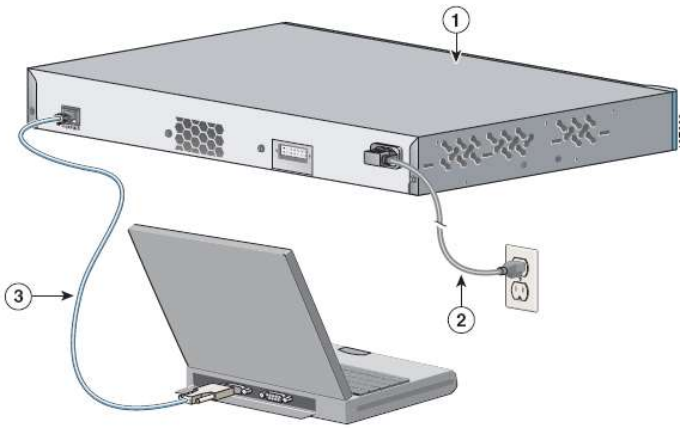

Рисунок 1. Фрагмент из инструкции по первичной настройке коммутатора Cisco 2960 (1 – коммутатор, 2 – кабель питания, 3 – консольный кабель, 4 – ноутбук с COM-портом)

Командная строка IOS может работать в нескольких **режимах**. Каждый режим предназначен для решения своей определённой задачи и обладает собственным набором команд. Определить текущий режим можно по приглашению командной строки. Существует три основных режима IOS CLI.

- **Пользовательский режим** – предназначен для ввода команд, используемых в реальном времени, т.е. непосредственно выполняющих какое-либо действие. Например, показать текущее состояние устройства. Приглашение командной строки заканчивается на «>». Доступные в режиме действия не влияют на работу устройства и предназначены для сбора диагностической информации.
- **Привилегированный режим** – также, как и пользовательский режим предназначен для выполнения команд, однако обладает максимальными полномочиями на устройстве (аналог консоли пользователя *root* в Linux). Например, позволяет перезагрузить систему или записать настройки в энергонезависимую память. Приглашение командной строки заканчивается на «#».
- **Режим конфигурации** – команды вводимые в этом режиме не выполняются непосредственно, а изменяют настройки (логику работы) устройства. Например, позволяют задать имя устройства, шлюз по умолчанию и т.д. Приглашение командной строки заканчивается на «***(config)#***». Режим конфигурации может быть активирован как для всего устройства (глобальный режим), так и для его отдельных подсистем. Например, чтобы настроить интерфейс «*Fa0*» необходимо в глобальном режиме конфигурации ввести команду «*interface Fa0*». После этого устройство перейдёт в режим конфигурации конкретного интерфейса (команды будут определять только его настройки), а окончание приглашения командной строки изменится на «***(config-if)#***».

Диаграмма взаимосвязи режимов приведена на Рисунке 2. На стрелочках, соединяющих режимы указаны команды для соответствующего перехода.

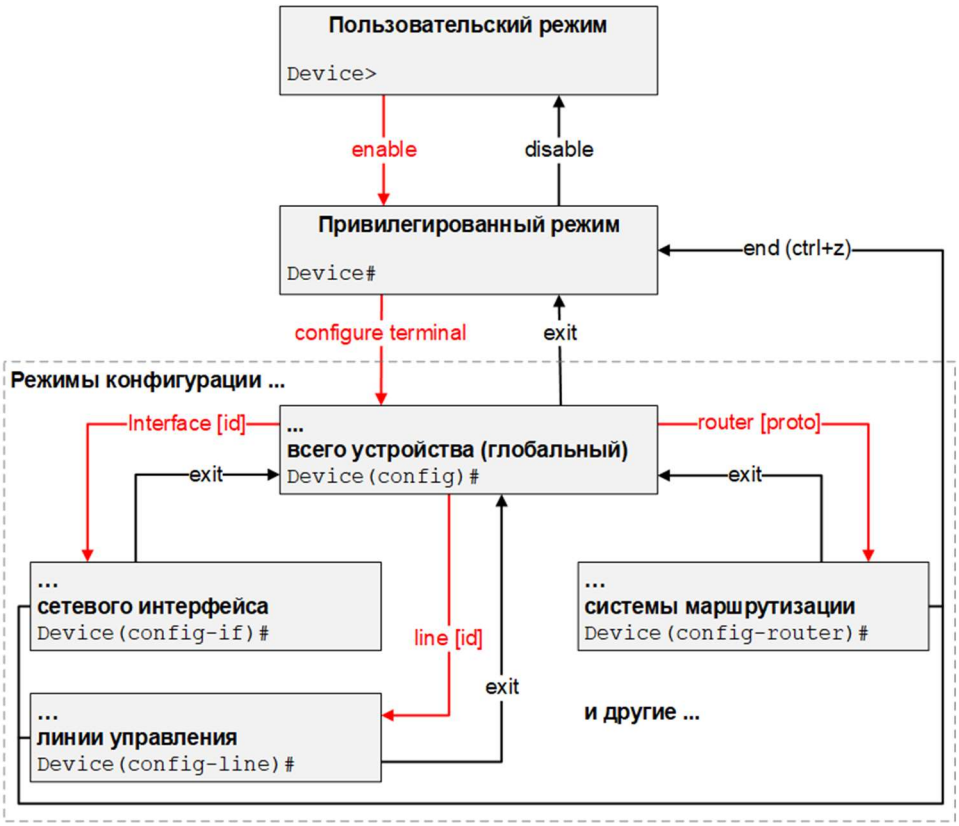

Рисунок 2. Диаграмма переходов между режимами CLI IOS

Каждый режим командной строки обладает собственным набором команд. Команды из других режимов, как правило, недоступны.

#Дополнительно

Из этого правила два исключения. Во-первых, в режиме конфигурации без выхода из него можно вызывать команды привилегированного режима. Для этого достаточно использовать ключевое слово «*do*». Например, команда «*do show version*» в контексте конфигурации покажет версию программного и аппаратного обеспечения. Во-вторых, если в режиме конфигурации подсистемы будет использована команда, отсутствующая в этом режиме, но существующая в режиме глобальной конфигурации, то произойдёт автоматический переход в глобальный режим.

Чтобы узнать список доступных команд в текущем контексте необходимо воспользоваться ключевым символом «***?***». Этот символ срабатывает автоматически, даже без нажатия клавиши *Enter*. Полный список доступных команд будет получен, если ввести «***?***» в пустой строке. Если в строке уже введено начало команды, то «***?***» покажет возможные её завершения (аналог клавиши *Tab* в Linux). А если «***?***» задан через пробел после команды, то будут выведены её аргументы (своеобразная замена команды «***man***» в Linux). Например:

- «***device#?***» – все команды, доступные в контексте;
- «***device#co?***» – все команды, доступные в контексте и начинающиеся с «*co*»;
- «***device#conf ?***» – все возможные аргументы команды «*configure*».

Как и в Linux клавиша *Tab* позволяет автоматически завершить не полностью введённую команду, если её завершение однозначно. Но в отличии от Linux, CLI IOS позволяет не завершать такие команды вообще, а оставлять их недописанными. Например, «***show version***» часто вводят как «***sh ver***» или вместо громоздкого «***configure terminal***» большинство администраторов вводит «***conf t***»

Все команды, вводимые в конфигурационных режимах, начинают действовать незамедлительно после их ввода. Поэтому надо быть особо внимательным при настройке сетевых параметров удалённого устройства. Ситуация, когда администратор по ошибке уничтожает свой собственный доступ к устройству на жаргоне называется «*выстрел себе в ноги*». Случается, что восстановление работоспособности устройства может потребовать проехать не одну тысячу километров для получения физического (внеполосного) доступа к консоли устройства.

Если какую-то настройку требуется отменить, то необходимо её продублировать с префиксом «***no***». Например, настройка «***ip domain-lookup***» (разрешает преобразование DNS-имён в IP) отменяется командой «***no ip domain-lookup***».

Несмотря на то, что команды настройки сразу производят эффект, они не сохраняются в энергонезависимой памяти устройства автоматически. Поэтому без сохранения настройки теряются после перезагрузки.

У устройства IOS всегда существует две конфигурации:

- **running-config** – настройки устройства, определяющие логику его работы в текущий момент времени, хранимые в оперативной памяти;
- **startup-config** – настройки устройства, которые будут использованы после его перезагрузки.

Если вы хотите сохранить настройки, то необходимо в привилегированном режиме выполнить копирование текущей конфигурации в стартовую: «***copy running-config startup-config***» (сокращённо «***cop run start***») или его псевдоним «***write***» (сокращённо «***wri***»). Посмотреть конфигурацию можно при помощи команды «***show***»: «***show running-config***» или «***show startup-config***».

#Дополнительно
Если администратор не уверен в командах, отдаваемых удалённому устройству, то он может установить отложенную перезагрузку при помощи команды «***reload in [interval]***». Тогда, если он ошибётся и потеряет доступ к устройству, то оно в установленное время перезагрузится и тем самым сбросит ошибочные настройки. Если же изменение настроек пройдёт успешно, то администратор отменит запланированную перезагрузку командой «***reload cancel***».

Все действия в IOS выполняются от имени какого-либо пользователя. При этом каждому пользователю соответствует уровень привилегий (метка доступа) от 0 до 15. По умолчанию определены только уровни 0 (гостевой доступ) и 15 (полный доступ). Промежуточные уровни 1-14 заданы с тем же набором команд, что и уровень 0. Однако, администратор с уровнем 15 может задать для каждого другого уровня свой независимый набор доступных команд.

#Дополнительно
Назначение прав для каждого уровня доступа, аутентификация и авторизация пользователей могут быть делегированы централизованному серверу, работающему с протоколом TACACS+ (проприетарный протокол Cisco для управления оборудованием) или RADIUS (открытый протокол, описанный в RFC2865 от 2000 г.).

Симулятор Cisco Packet Tracer

Cisco Packet Tracer (CPT) – это проприетарный, бесплатно распространяемый симулятор Cisco IOS от Cisco Systems, разработанный для приобретения начального уровня навыков работы с сетевым оборудованием. Загрузить его можно на сайте сетевой академии – **netacad.com**. Для этого необходимо пройти на нём регистрацию (в последствии полученная учётная запись ещё понадобится для запуска локальной версии программы), затем выбрать в меню «Resources» пункт «Download Cisco Packet Tracer» и выбрать версию ПО для своей операционной системы.

После установки, запуска программы и ввода данных учётной записи открывается главное окно CPT (рисунок 3). Программа имеет обширный функционал, в том числе в части многопользовательского взаимодействия, отправки результатов работы на проверку, симуляции IoT и т.д. Однако, мы рассмотрим только базовый функционал симуляции коммутации и маршрутизации. Для этого нам понадобятся области: 1 – кнопки для работы с файлом проекта; 2 – кнопки для создания графических объектов (не влияют на симуляцию, предназначены для улучшения читаемости схемы сети); 3 – основная рабочая область, в которой строится схема исследуемой сети; 4 – управление временем симуляции; 5 – переключение между реальным временем и режимом пошаговой симуляции; 6 – кнопки для создания элементов исследуемой сети.

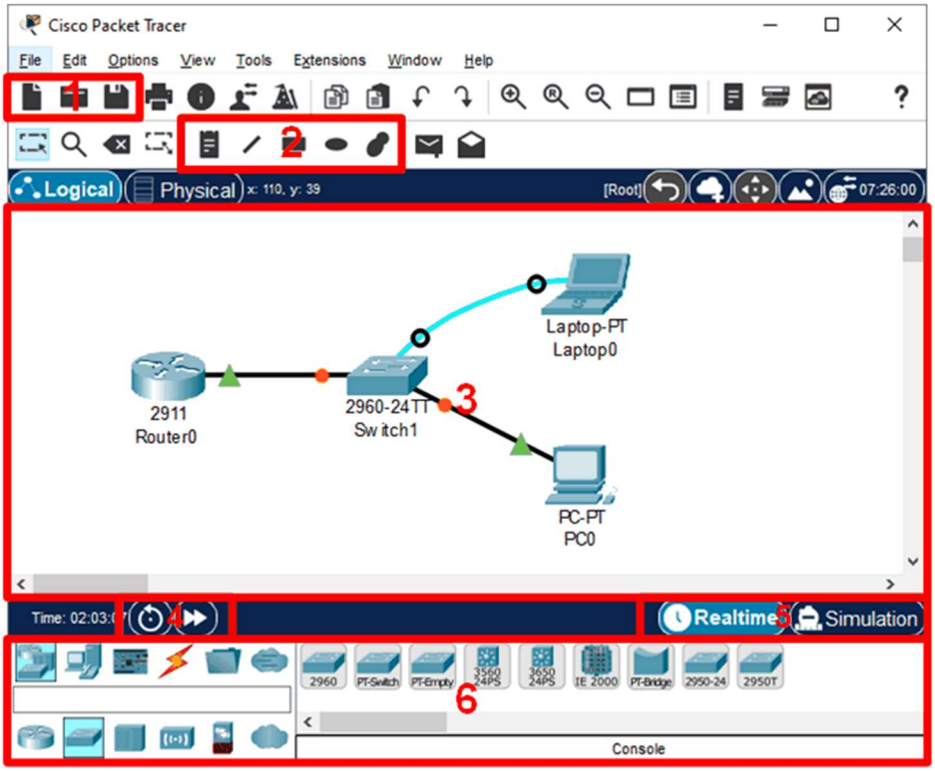

Рисунок 3. Главное окно Cisco Packet Tracer

CPT обновляется гораздо реже обычных устройств Cisco, поэтому среди доступных сетевых элементов есть уже давным-давно не актуальные модели (2960, 3560, 3650 и др.), однако для целей базового обучения они вполне подходят, так как IOS отличается хорошей преемственностью командного интерфейса. Есть в наборе элементов и окончательно устаревшие сетевые элементы (Hub, 2950, Coaxial Cables и др.), мы не будем их рассматривать, так как уже более 15 лет такие устройства не производятся и, соответственно, практической ценности не представляют. Так как данное программное обеспечение лишь имитирует функционирование реальных устройств и сетевое взаимодействие между ними, то существуют определенные ограничения и условности в работе поддерживаемых устройств и сетевых протоколов (доступны не все команды Cisco IOS: присутствуют основные, часто используемые команды, либо позволяющие освоить

основные моменты тех или иных концепций и принципов, заложенных в работу сетей, сетевых протоколов и устройств.).

При моделировании сети её конструируют из элементов, расположенных в области (6), размещая их в основном рабочем пространстве (3). Все сетевые элементы должны быть связаны линиями связи (группа элементов под символом молнии). Наиболее часто используемые кабели: UTP и RS-232 (консольный). Для того, чтобы соединить устройства необходимо выбрать требуемый кабель из набора (6), а затем последовательно щёлкнуть по соединяемым устройством и выбрать желаемые порты на них. Наиболее распространённая ошибка при сборке сетевой топологии – соединение устройств неподходящим для этого кабелем. Например, COM-порт компьютера следует соединять RS-232 кабелем с консольным портом коммутатора, а порт FastEthernet может быть соединён только с портом Fast- или GigabitEthernet кабелем типа витая пара.

#Дополнительно

Кабели UTP в CPT двух типов: прямой (Straight-Through) и перекрёстный (Cross-Over). Это устаревшая классификация кабелей для стандартов Ethernet и Fast Ethernet и устройств без поддержки Auto MDI-X (для Gigabit Ethernet и более поздних стандартов такая классификация кабелей не актуальна). Для исключения путаницы с прямым и перекрёстным подключением используйте устройства с поддержкой Auto MDI-X (2960 вместо 2950) или используйте линию с автоматическим определением типа.

Интерфейсы в устройствах Cisco нумеруются через «/»: «*X/Y/Z*», «Y/Z» или «*X/Z*», где *X* – номер устройства если это стек и 0, если это одиночное устройство, *Y* – номер модуля расширения (при наличии таковых в конструкции) и 0, если это основное шасси, *Z* – порядковый номер порта в устройстве/модуле.

CPT симулирует не только коммутаторы и маршрутизаторы, но и оконечные сетевые устройства. При этом симуляция персонального компьютера далека даже от виртуальной машины, так как имитируется только пара десятков приложений, большая часть из которых связана с сетевыми функциями узла. Работа с устройством осуществляется через специальную вкладку «*Desktop*» (Рисунок 4).

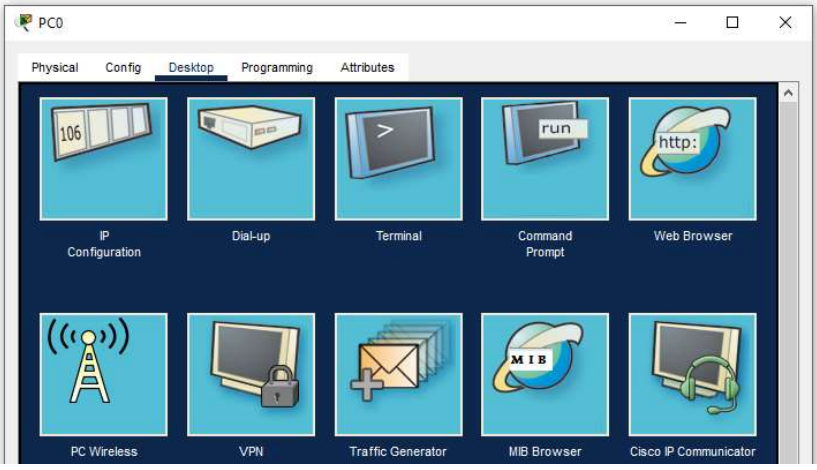

Рисунок 4. Приложения, доступные в симуляторе рабочей станции

Для таких сетевых устройств как «Маршрутизатор» или «Коммутатор» вкладка «*Desktop*» заменена на «*CLI*», предоставляющую доступ пользователя к командной строке Cisco IOS напрямую.

1. Моделирование простой сети

1.1. Запустите на своём рабочем месте CPT. Найдите информацию о текущей версии программы (меню «*Help → About…*») и запишите версию в отчёт.

1.2. В последующих пунктах работы вы столкнетесь с коммутатором Cisco Catalyst 2960-24TT (Рисунок 5). Самостоятельно найдите в Интернет его основные характеристики и запишите в отчёт 5 из них, наиболее важных на ваш взгляд.

Рисунок 5. Внешний вид коммутатора Cisco Catalyst 2960-24TT

1.3. При помощи области сетевых элементов (6) соберите в рабочей области (1) топологию, аналогичную рисунку 3 (обратите внимание, что бирюзовым цветом окрашено консольное подключение, а чёрным – сетевое). Зафиксируйте результат на снимке экрана и укажите в тексте отчёта названия интерфейсов, при помощи которых вы организовали связи.

1.4. Щёлкните один раз по маршрутизатору **Router0** и в открывшемся окне свойств перейдите на вкладку «*CLI*»: теперь вы попали в командную строку ОС IOS выбранного устройства. На предложение запустить конфигурационный диалог ответьте отрицательно («***no***»). Теперь вы находитесь в пользовательском режиме. При помощи команд, указанных на рисунке 2, перейдите в режим конфигурации интерфейса, к которому вы подключили линию связи в сторону коммутатора **Switch0**. Приглашение командной строки должно принять вид: «***Router0(config-if)#***». Введите последовательно команды: «***no shutdown***» (включает интерфейс), «***ip address 192.168.0.1 255.255.255.0***». Какие изменения произошли в рабочей области (1) после ввода команд?

1.5. Вернитесь в режим глобальной конфигурации. Введите команду, задающую имя устройства: «***hostname MyRouter***» Как изменилось приглашение командной строки? Обратите внимание, что имя устройства в рабочей области и его сетевое имя не связаны. В рабочей области по-прежнему отображается имя «*Router0*». Щёлкните непосредственно по этой надписи и приведите в соответствие подпись с сетевым именем.

1.6. Щёлкните по компьютеру **PC0** и в открывшемся окне свойств перейдите на вкладку «*Config → FastEthernet0*». В блоке «*IP configuration*» выберите ручное присвоение адреса («*Static*»), задайте адрес 192.168.0.2/24. Затем перейдите на вкладку «*Desktop*», на которой собраны некоторые приложения для симуляции сетевой активности рабочей станции, запустите командную строку («*Command prompt*») и выполните эхо-тестирование маршрутизатора («*ping 192.168.0.1*»). Результат зафиксируйте на снимке экрана.

1.7. Щёлкните по ноутбуку **Laptop0**, перейдите на вкладку «*Desktop*» и запустите приложение «*Terminal*», которое организует ввод/вывод для COM-порта (бирюзовая линия связи). Примите настройки порта по умолчанию, после чего откроется окно с CLI сессией, которое симулирует внеполосное управление коммутатором. С её помощью присвойте устройству имя «***MySwitch***» уже известным вам способом. Сохраните изменения в конфигурации коммутатора при помощи команды «***write terminal***» глобального режима. Зафиксируйте введённые вами команды и реакцию устройства на них на снимке экрана.

1.8. Для удаления лишних устройств из рабочей области программы используется клавиша *Delete*. Удалите консольное подключение к коммутатору и создайте новое к маршрутизатору. В приложении «*Terminal*» на ноутбуке нажмите *Enter*. Что произошло в консольном выводе? В дальнейшем при работе с CPT вы можете использовать любой удобный вам доступ к консоли устройства: из вкладки свойств или через симуляцию терминального подключения. Первый способ проще, но у настоящего оборудования, воплощённого в «железе» он отсутствует и консольное конфигурирование возможно только через выделенный компьютер и RS-232 интерфейс.

1.9. На панели инструментов с графическими примитивами (2) найдите кнопку создания надписей. Подпишите в рабочей области названия интерфейсов на концах каждой линии связи. Подпишите в произвольном месте рабочей области Фамилию И.О. участников бригады, номер группы и дату. При помощи любого графического примитива (овал, прямоугольник, область и т.д.) любым цветом кроме чёрного и белого визуально отделите коммутатор и маршрутизатор от клиентских устройств. Зафиксируйте результат на снимке экрана. CPT удобен для рисования сетевых топологий, поэтому его иногда используют не как симулятор, а как специфический графический редактор.

1.10. Переключите систему в режим пошаговой симуляции (5). Нажмите кнопку «Show All/None» один или два раза так, чтобы в поле «Event List Filters» осталось только «None». Нажмите кнопку «Edit Filters» и на вкладке «IPv4» выберите протокол ICMP. Закройте выбор фильтров. Нажмите клавишу «▶». Дождитесь, пока закончатся события, вызванные установкой фильтра. Повторите эхо-тестирование **Router0** от **PC0**. Пронаблюдайте обмен пакетами. В списке «*Event List*» выберите произвольный пакет, щёлкните по нему и ознакомьтесь с его параметрами на трёх вкладках («OSI…»,

«Inbound…», «Outbound…»). Зафиксируйте результат на снимке экрана. Вернитесь в режим реального времени.

1.11. Сохраните файл проекта при помощи меню «File» или кнопок на панели инструментов (1). Какое расширение и размер имеет полученный файл?

1.12. При помощи кнопки «*Power Cycle Devices*» (4) перезагрузите все устройства в топологии, а затем дождитесь их загрузки (процесс можно ускорить соседней кнопкой «*Fast Forward Time*». Процесс загрузки будет завершён, когда на всех концах медных линий связи появятся зелёные индикаторы. Повторите эхо-тестирование **Router0** от **PC0**. Поясните, почему оно завершилось неудачей и как этого можно было избежать?

2. Операционная система Cisco IOS

2.1. Любым способом подключитесь к консоли маршрутизатора **Router0** (через закладку «*CLI*» в его свойствах или переключив к нему консольный (бирюзовый) кабель и используя приложение «*Terminal*» на **Laptop0**). В привилегированном режиме выполните команду «***show version***». Найдите в её выводе: а) версию программного обеспечения б) имя файла-образа ОС в) модель маршрутизатора г) время, прошедшее с загрузки. Выпишите именно эту информацию в отчёт (не делайте снимок экрана или полную копию текста).

2.2. При помощи команды «***dir ?***» определите, какие носители доступны устройству. Перечислите их в отчёте. При помощи той же команды просмотрите содержимое носителей. На каком из них хранится стартовая конфигурация, а на каком – файл-образ ОС?

2.3. При помощи команды «***show proc***» определите текущую загрузку центрального процессора.

2.4. При помощи клавиши «?» определите список команд, доступных в привилегированном и пользовательском контекстах. Выпишите (можно в табличной форме) команды, которые доступны а) в обоих режимах б) только в привилегированном в) только в пользовательском.

2.5. Установите в качестве имени устройства значение **MyRouter**. Перейдите в привилегированный режим и последовательно просмотрите сначала текущую конфигурацию («***show running-config***»), а затем стартовую («***show startup-config***»). Чему равно значение параметра «***hostname***» в первом и втором случае?

2.6. Скопируйте текущую конфигурацию в стартовую («***copy run startup***»). Чему теперь равен параметр «*hostname*» в обоих конфигурациях? В дальнейшем в работах вам не будет даваться явных указаний по сохранению настроек. Выполняйте сохранение по своему усмотрению (периодически), чтобы не потерять прогресс работы.

3. Создание локальных пользователей

3.1. Консольный анонимный доступ небезопасен, поэтому необходимо его ограничить. Для этого в глобальной конфигурации создайте нового пользователя: «***username user privilege 15 secret azsxd***», где «*azsxd*» – его пароль, *15* – уровень его привилегий. В качестве имени пользователя вместо «*user*» используйте свой никнейм. Какая строка появилась в конфигурации после ввода этой команды? Создайте ещё одного пользователя, например, «*looser*», но вместо ключевого слова «*secret*» используйте слово «*password*». Какая строка появилась в конфигурации после ввода этой команды? Чем она отличается от предыдущей? Какой из вариантов команды безопаснее? Предложите сценарий действий злоумышленника, при котором использование «*secret*»/«*password*» сыграет роль?

3.2. Слегка сгладить ситуацию с использованием ключевого слова «*password*» можно при помощи директивы «***service password encryption***», введённой в глобальном режиме конфигурации. Введите её и проверьте, что изменилось в текущей конфигурации устройства? Самостоятельно найдите в Интернет информацию о том, что обозначают цифры 0, 5 и 7 перед паролем в строке «***username …***». Кратко эту поясните разницу в отчёте.

3.3. Используя ключевое слово «***no***» удалите пользователя с нестойким паролем. Убедитесь, что он исчез из конфигурации и зафиксируйте этот результат на снимке экрана.

3.4. Теперь, чтобы указать на необходимость аутентификации пользователя при консольном доступе, из режима глобальной конфигурации перейдите в режим конфигурации консольного подключения: «***line con 0***». Как изменилось приглашение командной строки? В этом режиме введите команду «***login local***», которая указывает на необходимость аутентификации по локальной базе пользователей при входе через текущую линию («***con 0***»). Дополнительно введите команду «***enable secret azsxd***», которая установит отдельный пароль на вход в привилегированный режим.

3.5. Возможно вы заметили, что при ошибке ввода команды в привилегированном режиме устройство пытается найти ошибочное слово в DNS, чтобы открыть подключение к узлу. Такое поведение может быть очень неудобным, так как обращение к несуществующему серверу занимает много времени. Чтобы его отключить, находясь в режиме настройки линии, введите команду «***transport output none***». Ещё одной неудобной особенностью консоли является то, что вывод событий системного журнала может прерывать ввод команд. Чтобы отключить это поведение дополнительно введите команду «***logging synchronous***». Просмотрите текущую конфигурацию для консольного подключения, на выходя из режима конфигурирования. Используйте для этого команду «***do …***». Скопируйте итоговую конфигурацию консольной линии в отчёт.

3.6. Завершите сеанс работы в консоли при помощи команды «***exit***» привилегированного или пользовательского режима, а затем снова инициируйте подключение нажатием клавиши *Enter*. Система должна запросить имя

пользователя и пароль. Аутентифицируйтесь созданными ранее реквизитам и зафиксируйте результат на снимке экрана.

4. Настройка удалённого доступа

4.1. Восстановите настройки интерфейса маршрутизатора, выполненные вами ранее (включение, присвоение IP-адреса) и утраченные при перезагрузке сети.

4.2. Консольное управление устройством надёжно, однако оно не обеспечивает достаточно гибкости и его сложно организовать в большой сети. Поэтому в большинстве случаев для устройств настраивают удалённый CLI доступ по протоколу SSH (или telnet, но он по праву считается небезопасным из-за передачи пароля по сети в открытом виде, без шифрования). Для того, чтобы это сделать перейдите в контекст настройки линий VTY (virtual terminal line). Всего существует 16 виртуальных линий, поэтому при их настройке надо указывать диапазон от первой до последней: «***line vty 0 15***». В режиме настройки линии введите ранее использованные вами команды для использования локальной аутентификации и отключения исходящих подключений при вводе неправильных команд. Дополнительно укажите в явном виде использование протокола SSH для входящих подключений: «***transport input ssh***». Зафиксируйте в отчёте полученную конфигурацию виртуальных терминальных линий.

4.3. Создания пользователя и разрешения подключений по SSH недостаточно для удалённого подключения. Дополнительно необходимо в режиме глобальной конфигурации задать доменную зону, в которой находится устройство: «***ip domain-name urfu.ru***», для неё создать ключи ассиметричного шифрования «***crypto key generate rsa***» и после этого явно указать используемую версию протокола «***ip ssh version 2***». Теперь маршрутизатор готов принимать удалённые подключения.

4.4. На рабочем столе («*Desktop*») компьютера **PC0** запустите SSH/Telnet клиент, укажите IP-адрес маршрутизатора, имя созданного пользователя и подключитесь к устройству. При подключении введите пароль. Зафиксируйте результат подключения на снимке экрана. Обратите внимание, что при SSH подключении вы начинаете всегда с одного и того же режима, тогда как при консольном подключении вы начинаете работу с тем режимом, где остановились в прошлый раз (если только не сработал автоматический выход в режим пользователя по таймеру неактивности).

4.5. Для повторного вызова ранее введенных команд в любом режиме работы интерфейса командной строки служат клавиши [*стрелка вверх*] (предыдущая) и [*стрелка вниз*] (следующая). Вызванные из хронологического списка команды можно редактировать как введенные с клавиатуры. С помощью команды «***show history***» можно отобразить журнал ранее введённых команд. Зафиксируйте этот журнал на снимке экрана.

5. Дополнительные инструменты

5.1. В привилегированном контексте выполните команду «***show cdp***». Она покажет вам настройки проприетарного протокола **Cisco Discovery Protocol** (**CDP**) – это протокол исследования сетевого окружения. С каким интервалом отправляются его сообщения? При помощи встроенной справочной системы определите, как вывести собранную о соседних устройствах детальную информацию, включающую в себя версию программного и аппаратного обеспечения соседа. Выведите эту информацию и зафиксируйте результат на снимке экрана. Как вы считаете, какую пользу и какой вред приносит этот протокол? В каком случае вы бы его выключили, а в каком – включили?

5.2. В режиме пошаговой симуляции установите отслеживание CDP пакетов и зафиксируйте на снимке экрана содержимое любого из перехваченных пакетов. Какой тип Ethernet кадра используется в CDP?

5.3. Сводную информацию (состояние портов, IP- и MAC- адреса и т. п.) об устройстве, находящемся в рабочей области, можно получить, наведя на него указатель мышки. Кнопка «*Inspect*» (увеличительное стекло) на панели инструментов рабочей области также выводит определенную информацию об устройстве: в зависимости от типа устройства контекстное меню содержит различное количество пунктов. Не используя CLI зафиксируйте на снимке экрана таблицу интерфейсов и таблицу MAC-адресов для коммутатора.

5.4. В глобальном режиме консоли коммутатора выполните команду «***setup***». Она запускает мастер начальной настройки, от использования которого вы ранее (при установке имени коммутатора) отказались. На собственное усмотрение ответьте на вопросы мастера. Зафиксируйте результат на снимке экрана.

5.5. Перезагрузите коммутатор при помощи команды «***reload***» глобального привилегированного режима. Пронаблюдайте процесс загрузки устройства. Из каких стадий состоит загрузка и какая информация выводится на экран?