

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ
ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение
высшего образования

**«МОСКОВСКИЙ АВТОМОБИЛЬНО-ДОРОЖНЫЙ
ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ (МАДИ)»
ВОЛЖСКИЙ ФИЛИАЛ МАДИ**

УТВЕРЖДАЮ
Зав. кафедрой ИиТТП
Петрова А.В.

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ К ЛАБОРАТОРНЫМ РАБОТАМ
ПО ДИСЦИПЛИНЕ
«СЕТИ ЭВМ И ТЕЛЕКОММУНИКАЦИИ»**

Направление подготовки

09.03.01 «Информатика и вычислительная техника»

Направленность (профиль)

***Автоматизированные системы обработки информации и
управления в отраслях транспортно-дорожного комплекса***

Квалификация

Бакалавр

Кафедра: ИиТТП

Чебоксары

1 НАЧАЛО РАБОТЫ С PACKET TRACER

Итак, вы начинаете свой путь в мир Cisco, возможно, для подготовки к сдаче экзаменов на промышленные сертификаты CCENT/CCNA, и хотели бы попробовать на вкус все, что есть в сетях Cisco? При этом не можете себе позволить роскошь реального оборудования. Тогда Packet Tracer – отличная замена для всех, кто нуждается в нескольких реальных устройствах: вы можете разработать сложную топологию из десятков (если не сотен) устройств Cisco и следить как за тем, как пакеты передвигаются между ними. И все это возможно в пределах вашего ноутбука вне зависимости от вашего местонахождения. Еще большую пользу окажет вам эта программа, если вы являетесь инструктором или экзаменатором: с помощью Packet Tracer можно создать необходимую топологию с практическими вопросами.

В этой главе рассмотрена установка Packet Tracer, описан графический интерфейс программы и показано как легко можно создать свою первую простую топологию. Но надо заметить, что Packet Tracer – программный симулятор сетей и устройств Cisco, а оттого в нем реализован не весь мир протоколов (читай, не все реальное оборудование). Потому и мы начнем с беглого осмотра, какие протоколы поддерживаются в программе.

Протоколы, работающие в Packet Tracer

Симулятор, как следует из значения этого слова, отображает работу реальных сетевых устройств и их окружения. Надо заметить, что и протоколы в Packet Tracer ведут себя почти также же, как если бы они работали на реальном оборудовании. В таблице 1 указаны технологии и протоколы, которые поддерживаются в программе.

Отмеченные звездочкой (*) протоколы имеют существенные ограничения: не все их команды и сервисы поддерживаются в Packet Tracer.

Таблица 1 – Протоколы, поддерживаемые в Packet Tracer

Технология	Протоколы
LAN	Ethernet (включая CSMA/CD*), 802.11 a/b/g/n wireless*, PPPOE
Коммутация	VLAN, 802.1q, trunking, VTP, DTP, STP*, RSTP*, многоуровневая коммутация*, EtherChannel, LACP, PAgP
TCP/IP	HTTP, HTTPS, DHCP, DHCPv6, Telnet, SSH, TFTP, DNS, TCP*, UDP, IPv4*, IPv6*, ICMP, ICMPv6, ARP, IPv6 ND, FTP, SMTP, POP3, and VOIP(H.323)
Маршрутизация	Статическая, маршрутизация по умолчанию, RIPv1, RIPv2, EIGRP, OSPF, BGP, inter-VLAN, перераспределение маршрутной информации
WAN	HDLC, SLARP, PPP*, Frame Relay*
Безопасность	IPsec, GRE, ISAKMP, NTP, AAA, RADIUS, TACACS, SNMP, SSH, Syslog, CBAC, Zone-Based Policy Firewall, and IPS
QoS	Layer 2 QoS, Layer 3 DiffServ QoS, FIFO Hardware queues, Priority Queuing, Custom Queuing, Weighted Fair Queuing, MQC, and NBAR*
Прочие технологии	Списки доступа (стандартные, расширенные и именованные), CDP, NAT (статический, динамический, входящий/исходящий и с перегрузкой), NATv6

Установка Packet Tracer

Для загрузки Packet Tracer следует открыть страницу Сетевой академии Cisco <https://www.netacad.com> (при этом необходимо обладать активным статусом пользователя академии). Затем нажав на соответствующий баннер (или выбрав пункт меню **Offerings|Packet Tracer**), перейти к выбору пакета поддерживаемого вашей операционной системой.

Операционная система Windows

Установка программы в Windows довольно проста и понятна. Необходимо найти файл (например с именем «Cisco Packet Tracer 6.2 for Windows Student Version.exe»). Достаточно открыть этот файл для запуска мастера установки, затем принять лицензионное соглашение, выбрать место и начать установку.

Операционные системы из семейства Linux

В зависимости от конкретной операционной системы семейства Linux необходимо загрузить соответствующий файл. Для обеспечения права доступа на исполнение этого файла следует воспользоваться командой `chmod`, а запустить файл на исполнение.

Для выполнения установки рекомендуется следовать инструкциям на экране.

Обзор графического интерфейса

Основное рабочее окно Packet Tracer подобно графическому редактору делится на несколько составляющих (рисунок 1). Необходимые пояснения даются ниже.

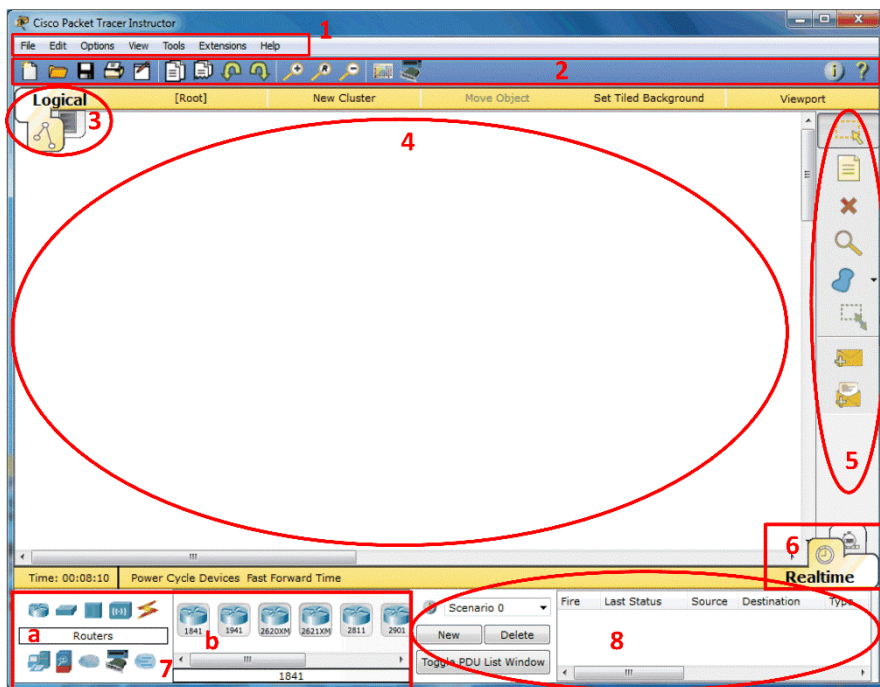


Рисунок 1 – Основное окно Packet Tracer

1 Строка меню (Menu Bar). Этот компонент идентичен для всех программных приложений. Используется для открывания, сохранения, печати, изменения настроек и т.п.

2 Главная панель инструментов (Main Toolbar) содержит ярлыки, обеспечивающие быстрый доступ к наиболее часто используемым пунктам меню, таким как **Открыть (Open)**, **Сохранить (Save)**, **Масштаб (Zoom)**, **Отменить (Undo)**, **Повторить (Redo)** и прочим. В правой части панели находится ярлык для ввода информации о текущей топологии.

3 Переключатель выбора логической или физической топологии (Logical/Physical Workspace Tabs) служат для переключения между логической или физической рабочими областями.

4 Рабочее пространство (Workspace). Это основная область работы в Packet Tracer. Именно здесь создается необходимая топология

(схема сети), и отображается симуляция процесса сетевого взаимодействия.

5 Общая панель инструментов (Common Tools Bar) обеспечивает возможность выбора инструментов манипуляции с схемой сети, таких как выделение и изменение расположения устройств, размещение надписей и заметок, удаление, изменение размера и выбор передачи простого (Simple PDU) или сложного (Complex PDU) пользовательского блока данных.

6 Переключатель выбора режима работы (Realtime/Simulation Tabs) обеспечивает переключение между реальным режимом работы или режимом симуляции сетевого взаимодействия. Данный переключатель также дает возможность контроля времени и захвата пакетов в сети.

7 Окно выбора сетевых компонентов (Network Component Box) содержит доступное в Packet Tracer сетевое оборудование и оконечные устройства. Подразделяет на две области:

7а Окно выбора категории устройства (Device-type Selection Box) содержит основные категории устройств (маршрутизаторы, коммутаторы, концентраторы, беспроводные устройства, сетевые кабели, оконечные устройства и прочие).

7б Окно выбора конкретного типа устройства (Device-specific Selection Box). После выбора категории здесь становятся доступными различные модели устройств.

8 Окно создания пользовательских пакетов (User-created Packet Box) предназначено для создания пользователями подробных тестов сетевой топологии и отображения их результатов.

Для успешного дальнейшего изучения Packet Tracer необходимо уверенно ориентироваться в приведенных названиях инструментов и их расположения в окне программы.

Создание простой схемы сети

После знакомства с интерфейсом программы мы можем приступить к созданию первой топологии. Выполним следующие пункты.

1 В окне сетевых выбора сетевых компонентов найдите категорию **Оконечные устройства (End Devices)** и выберите в соседнем окне **Персональный компьютер ПК (Generic PC)** и **Ноутбук (Generic Laptop)**. Перетащите оба устройства в рабочую область Packet Tracer.

2 Кликните **Подключения (Connections)**, затем выберите **Перекрестный кабель (Copper Cross-Over)**. Вначале кликните на изображении ПК и выберите FastEthernet-интерфейс устройства в открывшемся

списке. После этого кликните на изображении ноутбука и также выберите FastEthernet-интерфейс. При правильном подключении индикаторы статуса устройств должны отображаться зеленым цветом, указывающим, что интерфейсы устройств включены.

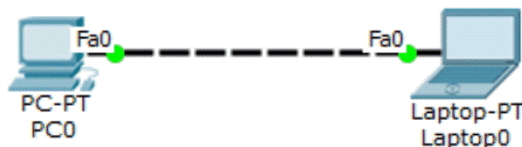


Рисунок 2 – Простая топология сети

3 Для того, чтобы настроить устройство, например ПК, следует кликнуть на его изображении и затем выбрать вкладку **Рабочий стол (Desktop)**. Выберите инструмент **Конфигурация IP (IP Configuration)** и введите IP-адрес (**IP Address**) и маску (**Subnet Mask**) устройства.

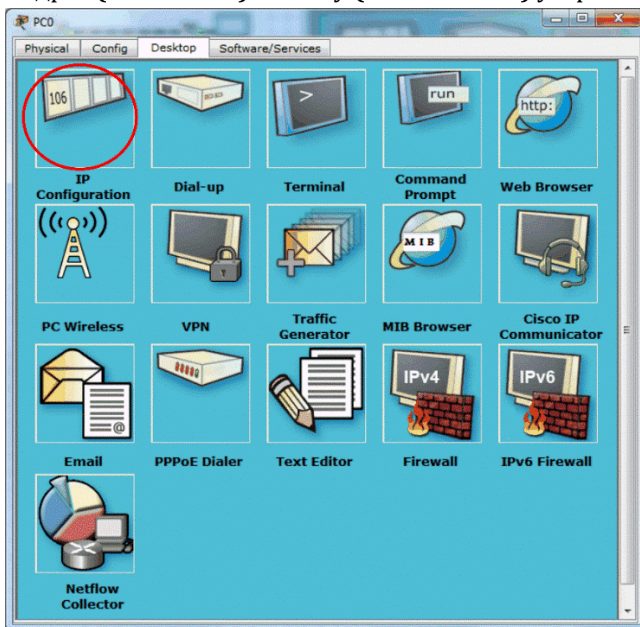


Рисунок 3 – Рабочий стол ПК

Для схемы можно обочиться без IP-адресов шлюза по умолчанию и DNS-сервера, т.к. в этом нет необходимости (схема состоит только из двух компьютеров и не предполагает выход в Интернет или подключение к другим сетям, а также использование символьных имен).

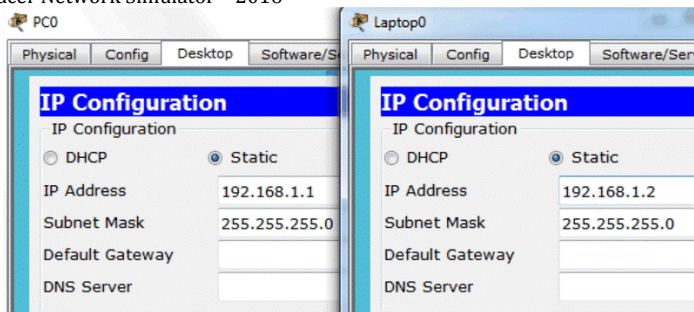


Рисунок 4 – Настройка IP-адреса и маски ПК и ноутбука

4 Закройте окно настройки ПК. Кликните по изображению ноутбука и выполните таким же образом настройку ноутбука.

Убедитесь, что заданные IP-адреса находятся в одной подсети.

5 Закройте окно настройки IP-адреса и затем откройте инструмент **Командная строка (Command Prompt)**. Воспользовавшись утилитой **ping** проведите тест связности, как показано на следующем рисунке.

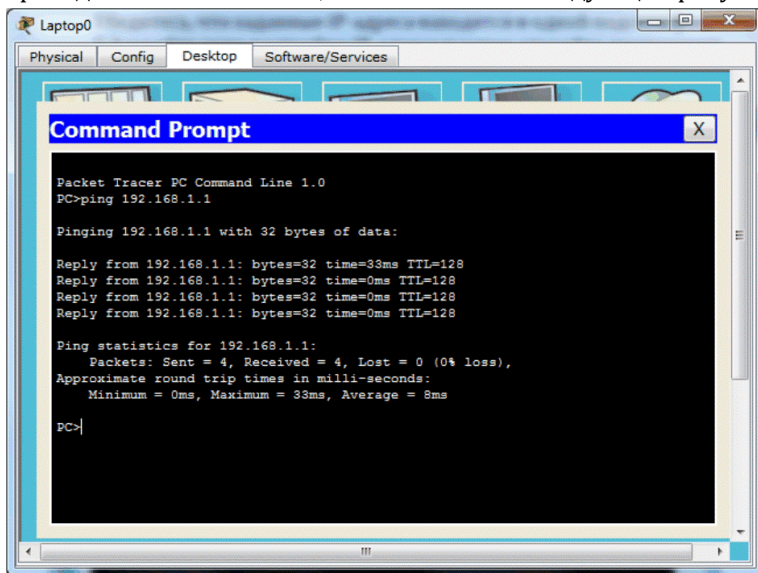


Рисунок 5 – Тест связности между устройствами

Рассмотренная схем сети относительно простая. В действительности современная сеть требует наличия сетевого оборудования. Немного усложним нашу топологию, добавив Ethernet-коммутатор.

1 Кликните на категории устройств **Коммутаторы (Switches)** и перенесите из окна выбора конкретного типа устройства в рабочую область любой тип коммутатора (за исключением Switch-PT-Empty)/

2 Удалите кабель между ПК и ноутбуком, используя инструмент **Удалить (Delete)** из общей панели инструментов.

3 Кликните на категории **Подключения (Connections)**, затем выберите **Прямой кабель (Cooper Straight-Through)** и подключите ПК и ноутбук к коммутатору. Сразу после подключения индикаторы коммутатора будут оранжевого цвета, потому что порты коммутатора находятся в режимах прослушивания и изучения протокола связующего дерева STP (Spanning Tree Protocol).

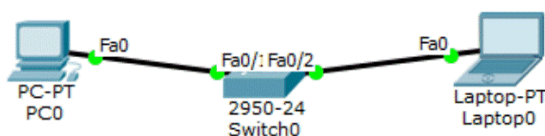


Рисунок 6 – Схема сети с коммутатором

4 Как только индикаторов цвет измениться на зеленый (что свидетельствует о нормальной работе портов коммутатора) проведите тест связности между ПК и ноутбуком с помощью утилиты **ping**. Убедитесь, что тест выполнен успешно.

5 Сохраните измененную топологию под другим именем (меню **File> Save As**). Схема сохраняется в файле с расширением **.pkt**, при этом устройства запоминается текущий статус и настройки устройств.

Резюме

В данной главе вы научились устанавливать Packet Tracer и использовать его для создания простейших схем сети. Поэкспериментируйте с различными вариантами топологий, используя только ПК, ноутбук и коммутаторы, что самостоятельно закрепить принципы работы с программой. Также вы познакомились со списком протоколов поддерживаемых Packet Tracer. Используйте этот список всякий раз, как только вы собираетесь опробовать новую технологию, чтобы убедиться, что необходимые протоколы и соответствующие им настройки полностью поддерживаются программой.

В следующей главе вы узнаете о различных типах сетевых устройств и принципах их настройки под конкретные нужды. Мы также разберем, как настраивать устройства через интерфейс командной строки (CLI), а также с помощью графического интерфейса.

2 СЕТЕВЫЕ УСТРОЙСТВА

Сетевые устройства создают основу для сетевого взаимодействия. В этой главе вы узнаете о всех сетевых устройствах, доступных в Packet Tracer, и модулях, подходящих для конкретных моделей устройств. После этого вы сможете создавать устройства с предпочитаемыми модулями и производить их настройку. В программе также предусмотрено сохранение таких видоизмененных устройств для работы с ними в будущем. Если вы не знаете команд межсетевой операционной системы Cisco IOS, то после чтения пункта «Настройка сетевых устройств» вы будете способны к пошаговой настройке коммутаторов и маршрутизаторов Cisco, используя любые команды.

Сетевое оборудование Cisco и устройства Packet Tracer

Большинство устройств, представленных в Packet Tracer, более-менее соответствуют реальному оборудованию Cisco. Однако имеются устройства, присущие только Packet Tracer. Эти устройства находятся в подразделах категорий **коммутаторы (Switches)** и **маршрутизаторы (Routers)** и имеют в своем названии слово **Общий (Generic)**. Изначально их слоты пусты и допускают установку различных типов модулей.

Маршрутизаторы

Маршрутизаторы обеспечивают взаимодействие между подсетями (логическими сегментами). Любой маршрутизатор в Packet Tracer может быть включен и выключен переключением тумблера «Питание», расположенного на внешнем виде устройства («**Physical Device View**»)

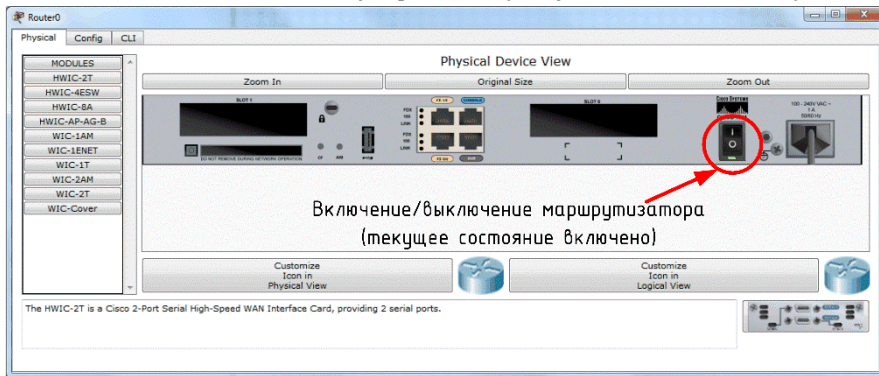


Рисунок 7 – Вкладка «Физический вид устройства»
(указан тумблер «Питание» маршрутизатора)

Возможность включения/выключения питания маршрутизаторов в Packet Tracer симулирует работу реальных устройств. Модуль устройства может быть добавлен и удален только после выключения электропитания устройства. При этом надо помнить, если вы не сохранили текущую конфигурацию, выключение устройства приведет к потере произведенных настроек.

Следующие маршрутизаторы доступны в Packet Tracer:

1) **Cisco 1841.** Маршрутизатор с интегрированными сервисами (Integrated Service Router, ISR) имеет два порта Fast Ethernet и два свободных слота для подключения интегральных карт для высокоскоростного WAN-соединения.

2) **Cisco 1941.** Эта модель подобна предыдущей с той лишь разницей, что функционирует под управлением 15 версии Cisco IOS. Также имеет два Gigabit Ethernet порта.

3) **Cisco 2620XM.** Этот мультисервисный маршрутизатор имеет один Fast Ethernet порт, два слота для установки WAN интерфейсных карт и слот для AIM.

4) **Cisco 2621XM.** Данный маршрутизатор подобен предыдущему, за исключением наличия двух портов Fast Ethernet.

5) **Cisco 2811.** Маршрутизатор с интегрированными сервисами имеет два порта Fast Ethernet, четыре WIC слота и два AIM слота.

6) **Cisco 2901.** Этот маршрутизатор имеет два Gigabit Ethernet порта, четыре WIC слота и два слота для установки DSP.

7) **Cisco 2911.** Данный маршрутизатор имеет три порта Gigabit Ethernet, а в остальном повторяет характеристики предыдущего устройства. Функционирует под управлением 15 версии Cisco IOS.

8) **Genetic Router-PT.** Маршрутизатор с настройкой под пользователя. Имеет 10 слотов и несколько специальных модулей, названия которых начинается с букв **PT**.

Коммутаторы

Коммутатор (ранее называемые многопортовый мост) соединяет более чем одно оконечное устройство в сеть. Каждый порт коммутатора является коллизийным доменом. Следующие коммутаторы доступны в Packet Tracer:

1) **Cisco 2950-24.** Управляемый коммутатор с поддержкой 24 портов Fast Ethernet.

2) **Cisco 2950T-24.** Этот коммутатор принадлежит к семейству интеллектуальных коммутаторов Catalyst 2950 и имеет 24 порта Fast Ethernet и два Gigabit Ethernet с поддержкой модулей GBIC (Gigabit Interface Converter).

2) **Cisco 2960-24TT**. Еще один 24-портовый коммутатор. В отличие от предыдущей модели имеет порты Gigabit Ethernet с поддержкой модулей SFP (Small Form-factor Pluggable). Однако это отличие существенно для реальных коммутаторов и не оказывает никакого влияния при работе в Packet Tracer.

3) **Cisco 3560-24PS**. В отличие от других коммутаторов данное устройство является коммутатором 3 уровня и в дополнении к штатной функции коммутации способно осуществлять маршрутизацию. Две последние буквы **PS** означают поддержку питания по Ethernet PoE (Power over Ethernet), что используется для питания IP-телефонов без отдельного блока питания.

4) **Bridge PT**. Это устройство используется для сегментации сетей и имеет только два порта (потому и называется мостом; если бы портов было больше, тогда более приемлемое название было бы коммутатор).

5) **Generic Switch PT**. Данное устройство существует только в Packet Tracer и представляет собой коммутатор с настройкой под пользователя. Имеет 10 слотов и несколько специализированных модулей.

Точно также как рассмотренный ранее Genetic Router-PT, коммутатор) Generic Switch PT может быть выключен, что необходимо для смены модулей. Все остальные коммутаторы имеют фиксированную структуры и не предполагают кастомизации. Потому не имеют нужды в выключении питания.

Другие устройства

Как можно убедиться, Packet Tracer поддерживает не только коммутаторы и маршрутизаторы, но и другие устройства. Эти устройства настройки и работают как есть.

1) **Hub PT**. Построение сетей на основе концентраторов является достоянием истории. Однако с помощью этого устройства становится возможным познакомиться с ширококвещательным штормом и коллизиями. Имеет 10 слотов для.

2) **Repeater**. Используется для повышения уровня и восстановления формы электрического сигнала. Имеет два слота.

3) **Coaxial Splitter PT**. Предназначено для раздвоения коаксиального подключения. Имеет три порта для подключения коаксиального кабеля и не может быть кастомизировано.

Подключение модулей сетевых устройств

Модули сетевых устройств представляют собой аппаратную реализацию некоторый распространённых интерфейсов. Например, модуль HWIC-4ESW содержит 4 Ethernet-порта (10 Мбит/с). Как и для реального

устройства, так и для устройства, представленного в Packet Tracer, для смены модуля требуется отключение питания.

Для отключения питания сделайте один клик на переключателе питания в правой части устройства. Для установки модуля перетащите любой из доступных в списке модулей и установите его в любой пустой слот. Если модуль не может быть установлен в определенный слот, то он будет автоматически возвращен в список.

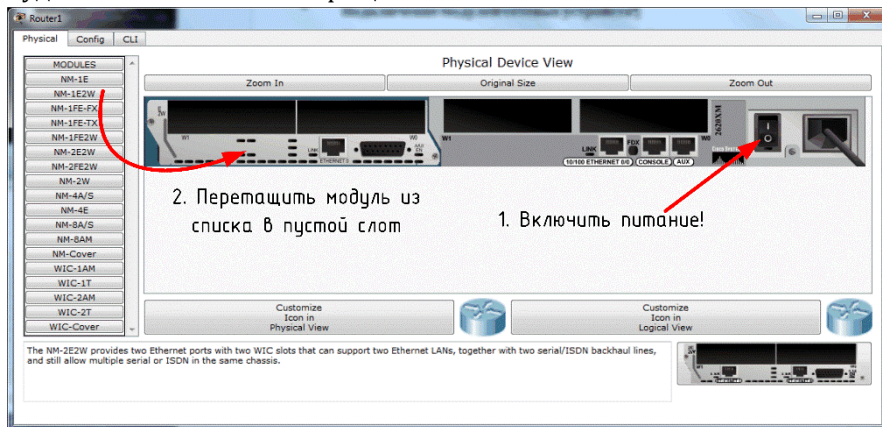


Рисунок 8 – Добавление модуля маршрутизатора

Для удаления модуля также необходимо выключить питание и перетащить его из слота обратно в список.

После смены модуля не забудьте включить питание устройства.

Система наименования модулей

Каждый маршрутизатор имеет более десятка модулей, которые могут быть идентифицированы по их названиям. Ниже перечисляются модули, сгруппированные на основе типа кабельного подключения.

Медный интерфейс Ethernet

Представляет собой стандартные LAN-интерфейс, к которому подключается медная витая пара с разъемом RJ-45. Название таких интерфейсов основано на указании скорости: **Etnernet** (10 Мбит/с), **FastEtnernet** (100 Мбит/с), **GigabitEtnernet** (1000 Мбит/с). Соответственно в названиях модулей имеется сокращенное упоминание об скорости интерфейса: **E**, **FE**, **GE**, **CFE** или **CGE**. Модули с обозначением **SW** предназначены для маршрутизаторов и обеспечивают функции коммутации.

- 1) **HWIC-4ESW** – 4 коммутируемых Ethernet-порта;
- 2) **WIC-1ENET** – одиночный Ethernet-порт;

- 3) **NM-1E** – одиночный Ethernet-порт;
- 4) **NM-1FE-TX** – одиночный Fast Ethernet-порт;
- 5) **NM-4E** – 4 Ethernet-порта;
- 6) **NM-ESW-161** – 16 коммутируемых Ethernet-порта;
- 7) **PT-ROUTER-NM-1CE, PT-ROUTER-NM-1CFE, PT-ROUTER-NM-1CGE** – пользовательские модули Packet Tracer.

Оптический модуль Ethernet

Данный вид модулей схож с предыдущим, за исключением использования оптического кабеля вместо медного. Эти модули можно определить по присутствующей букве **F**.

- 1) **NM-1FE-FX** – одиночный Ethernet-порт для оптической среды передачи;
- 2) **PT-ROUTER-NM-1FFE, PT-ROUTER-NM-1FGE** – пользовательские модули Packet Tracer.

Последовательный интерфейс

В названиях этих модулей присутствует буква **T** или пара символов **A/S**. Модули с буквой **T** являются синхронными, а модули с символами **A/S** – асинхронными. Различия в их работе проявляется в мире реального оборудования, в Packet Tracer между ними нет разницы.

- 1) **WIC-1T, WIC-2T** – одиночный или вдвоенный синхронный последовательный порт;
- 2) **NM-4A/S, NM-8A/S** – четыре или восемь последовательных асинхронно-синхронных портов;
- 3) **PT-ROUTER-NM-1S, PT-ROUTER-NM-1SS** – пользовательские модули Packet Tracer.

Модемный интерфейс

Данный вид модулей имеет RJ-11 интерфейс для подключения телефонных кабелей. Такие модули можно идентифицировать по буквам **AM**, присутствующих в названии после цифры, указывающей количество портов.

- 1) **WIC-1AM** – вдвоенный RJ-11 порт для подключения телефона и модема;
- 2) **WIC-2AM, WIC-8AM** – два или восемь RJ-11 портов;
- 3) **PT-ROUTER-NM-1AM** – пользовательский модуль Packet Tracer.

Модули с поддержкой WIC-модулей

Сетевые модули WIC не занимают слот целиком, для их поддержки используются модули (**WICs within Network Modules(NM)**), имеющие в своем составе дополнительные слоты для поддержки модулей малого

размера. Такие модули можно опознать по букве **W**, присутствующей в конце названия.



Рисунок 9 – Модули с поддержкой WIC-модулей

- 1) **NM-1E2W, NM-1FE2W** – один Ethernet/ два Fast Ethernet порта с поддержкой двух WIC-слотов;
- 2) **NM-2E2W, NM-2FE2W** – два Ethernet/ Fast Ethernet порта с поддержкой двух WIC-слотов;
- 3) **NM-2W** – не имеет портов, предназначен для поддержки двух WIC-слотов.

Заглушки

Packet Tracer обеспечивает заглушку (крышку) для пустых слотов. Заглушка не несет никакой функциональной нагрузки и служит для более приятного вида устройства при просмотре физического вида устройства.

- 1) **NM-Cover** – крышка для сетевого модуля;
- 2) **WIC-Cover** – заглушка для WIC-слота.

Дополнительный модуль HWIC-8A

Модуль HWIC-8A появился в шестой версии Packet Tracer и поддерживает 8 асинхронных EIA-232 подключения к консольному порту. Маршрутизатор, использующий данный модуль, может работать как сервер доступа.

Создание пользовательского устройства

Если вам потребуется маршрутизатор с определенным набором модулей. Создание такого устройства является несколько утомительным занятием, особенно, если выполнять его каждый раз в новой топологии. Packet Tracer обеспечивает возможность сохранить созданное устройство. Для этого надо выполнить следующие шаги.

1 Перетащите сетевое устройство в рабочую область программы. Для примера мы будем использовать коммутатор Generic Switch PT: **Switch-PT-Empty**.

2 Кликните по изображению коммутатора для открытия окна настроек. Окно настроек открывается по умолчанию на вкладке **Физический вид (Physical)**. Отключите питание устройства.

3 Добавьте в пустые слоты необходимые вам модули.

4 Перейдите в меню **Инструменты (Tools)** → **Создание пользовательского устройства (Custom Devices Dialog)** или нажмите *Ctrl+E*.

5 Кликните по кнопке **Выбор (Select)**, а затем кликните по коммутатору, который вы настроили в соответствии с вашими предпочтениями.

6 Укажите имя и описание устройства и нажмите кнопки **Добавить (Add)** и **Сохранить (Save)**.

Пользовательское устройства сохраняется с расширением .ptd в папке %USERPROFILE%\Cisco Packet Tracer\templates\. Для того, чтобы сделать пользовательское устройство доступным для всех пользователей скопируйте полученный файл в папку %PTHOME%\templates\.

Имитация WAN-соединения

Для создания сценариев из реальной жизни Packet Tracer имеет устройства имитирующие WAN-соединения. Кликните в окно выбора сетевых компонентов на категории **Имитация WAN (WAN Emulation)** для просмотра доступных устройств в окне выбора конкретного типа устройства.

1) **Cloud-PT**. Это устройство выглядит как облако, но имеет конфигурационное окно больше похожее на маршрутизатор с несколькими слотами. Для облачного устройства доступны следующие модули.

а) **NM-1AM** – служит для подключения модемов с RJ-11 интерфейсом с использованием телефонного кабеля. При работе с интерфейсом командной строки этот модуль имеет имя *ModemN*, где *N* – номер порта.

б) **NM-1CE, NM-1CFE, NM-1CGE** – все эти модули служат для Ethernet, Fast Ethernet и Gigabit Ethernet интерфейсов соответственно. Через них сетевые устройства подключаются к телефонному или кабельному модему. За исключение скорости, все три модуля выполняют схожие функции.

в) **NM-1FFE, NM-1FGE** – Данные интерфейсы обеспечивают Fast Ethernet и Gigabit Ethernet интерфейсы с волоконно-оптическое средой передачи. Функционально обеспечивают аналогичные функции как и предыдущие модули.

г) **NM-1CX** – Имеет коаксиальный интерфейс для подключения к кабельному модему.

д) **NM-1S** – Последовательный порт поддерживает интерфейс с поддержкой Frame Relay. На вкладки **Настройка (Config)** доступны функции по созданию Frame Relay соединения.

2) **DSL-Modem-PT** – Модем с Ethernet и RJ-11 интерфейсами. Ethernet-интерфейс может выбран с Ethernet, Fast Ethernet или Gigabit Ethernet модулями. Не имеет каких-либо конфигурационных опций.

3) **Cable-Modem-PT** – Этот модем схож с предыдущим, за исключением поддержки коаксиального порта.

Доступ к командному окну CLI

Доступ к интерфейсу командной строке (CLI) может быть получен двумя путями:

- 1) Через вкладку **CLI** окна настройки устройства;
- 2) Через консольный порт устройства.

В Packet Tracer, как и в реальном мире устройств Cisco, обеспечивается доступ к устройству через SSH или Telnet соединение.

Вкладка CLI

Данная опция представляет собой простейший способ доступа к интерфейсу командной строки. Кликните по устройству и перейдите на вкладку **CLI**, где окне командной строки можно, в частности, наблюдать процесс загрузки.

Консольный порт

Использование консольного порта делает работу с устройствами подобной работе с реальными устройствами, хотя в рамках Packet Tracer между предыдущим способом и текущим нет принципиальной разницы.

Для настройки консольного порта следует выполнить следующие пункты.

1 В рабочее пространство добавить ПК (ноутбук) и сетевое устройство (например, маршрутизатор).

2 Выбрать категорию Подключения и кликнуть по консольному кабелю (**Console**).

3 С одной стороны подключите кабель к консольному порту сетевого устройства, с другой же подключите кабель к порту RS-232 компьютера.



Рисунок 10 – Подключение к консольному порту

4 Кликните по изображению компьютера и перейдите на вкладку **Рабочий стол (Desktop)**, откройте утилиту **Терминал (Terminal)** и не изменяя предложенных настроек, нажмите **Ок**.

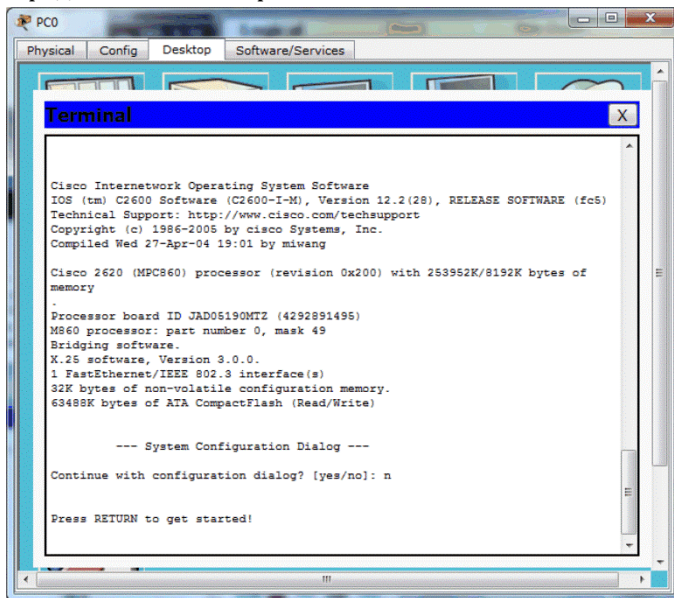


Рисунок 11 – Терминальное подключение через консольный порт

Если на втором шаге вы выбрали **Автоматический выбор типа подключения (Automatically Choose Connection Type)**, то произойдет соединение Ethernet портов сетевого устройства и компьютера.

Конфигурирование сетевых устройств

В этом разделе вы изучите как необходимо конфигурировать маршрутизаторы и коммутаторы Cisco без использования даже простейших команд. Как ни странно, это возможно. Вкладка **Настройка (Config)** окна свойств устройства содержит графический интерфейс для настройки некоторого количества общих опций. Более того, когда вы работаете на скорую руку с графическим интерфейсом, в нижнем окне вкладки отображаются эквивалентные команды Cisco IOS (рисунок 12).

На вкладке **Настройка (Config)** коммутатора произведем следующую последовательность действий: **Интерфейс (Interface)** → FastEthernet0/1 и далее уберите в опции **Статус порта (Port Status)** птичку **Вкл (On)**. В окне эквивалентных команд Cisco IOS (**Equivalent IOS Commands**) отобразятся следующие команды:

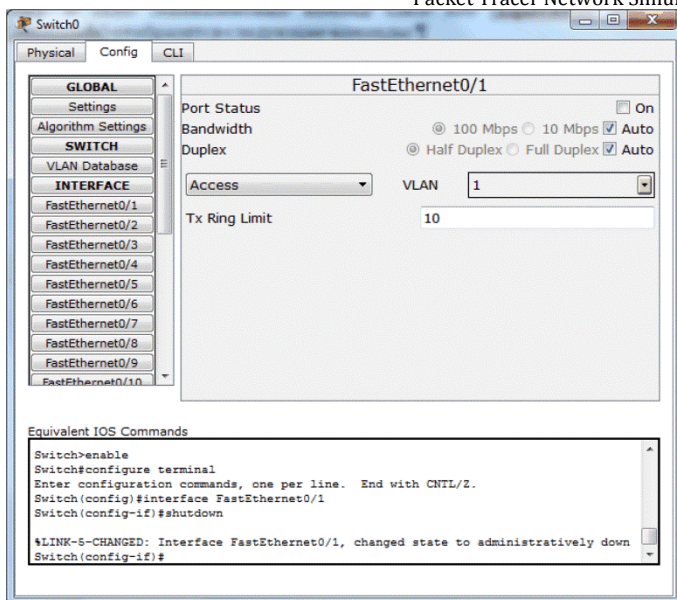


Рисунок 12 – Вкладка Настройка коммутатора

```
Switch>enable
Switch#configure terminal
Switch(config)#interface FastEthernet0/1
Switch(config-if)#shutdown
```

Использование вкладки **Настройка (Config)** позволяет настроить:

- настройки глобального режима конфигурирования;
- маршрутизацию (на маршрутизаторе или коммутаторе третьего уровня);
- базу данных VLAN (на коммутаторе);
- опции интерфейса.

Доступ к этим настройкам осуществляется при выборе соответствующего раздела вкладки.

Глобальные настройки

Настройки глобального режима конфигурирования (**Global settings**) позволяют изменить **Название (Display name)**, отображаемое в рабочем пространстве и **Имя (Hostname)**, используемое в интерфейсе командной строки. Название устройства также можно изменить непосредственно в рабочем пространстве сделав клик на тексте под изображением устройства.

В этом же разделе можно сохранить, удалить или экспортировать конфигурационный файл для дальнейшего использования (рисунок 13).

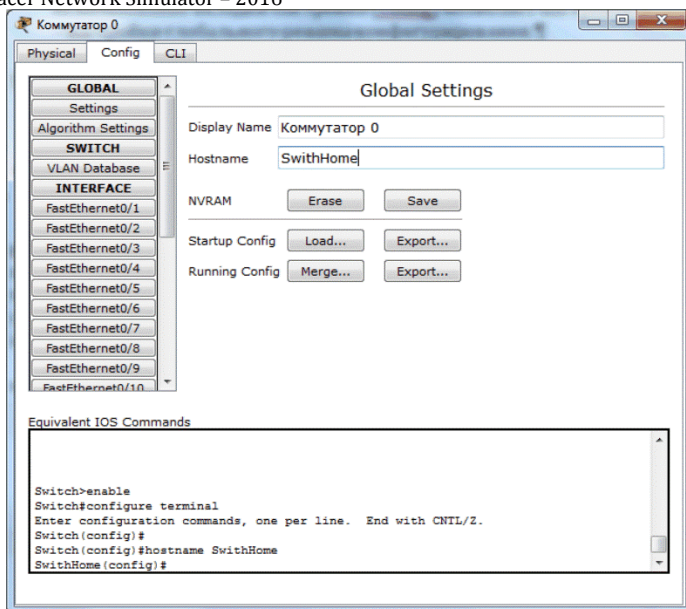


Рисунок 13 – Раздел настройка глобального режима конфигурации

Также здесь можно имеется секция **Параметры алгоритмов (Algorithm Setting)**. Она содержит некоторые опции, представляющие интерес для продвинутых пользователей. Эти опции позволяют точно настроить устройство, чтобы просмотреть его поведения в определенных ситуациях. Эти опции можно определить глобально для всех сетевых устройств, выбрав последовательно пункты меню: **Option→ Algorithm Settings** или используя клавиатурное сокращение: Ctrl+ Shift + M.

Маршрутизация

Этот раздел имеет секции по конфигурации **Статической маршрутизации (Static)** и динамической маршрутизации **RIP**. Для задания статического маршрута необходимо ввести адрес и маску сети назначения и адрес следующего маршрутизатора и нажать кнопку **Добавить (Add)** (рисунок 14). Ниже приведен пример такой настройки маршрутной информации.

Сеть назначения (Network): 192.168.30.0

Маска (Mask) 255.255.255.0

Следующий маршрутизатор (Next Hop) 10.0.0.6

Для конфигурирования протокола маршрутной информации (**Routing Information Protocol, RIP**) будет достаточно добавить IP-адрес сети назна-

чения. Заметим, что графический интерфейс задействует RIP версии 1, который не поддерживает передачу масок и, соответственно, бесклассовые сети. Более подробно этот момент рассматривается в шестой главе. Кроме собственно маршрутизаторов, процесс маршрутизации может быть сконфигурирован на коммутаторе третьего уровня **3560-24PS**.

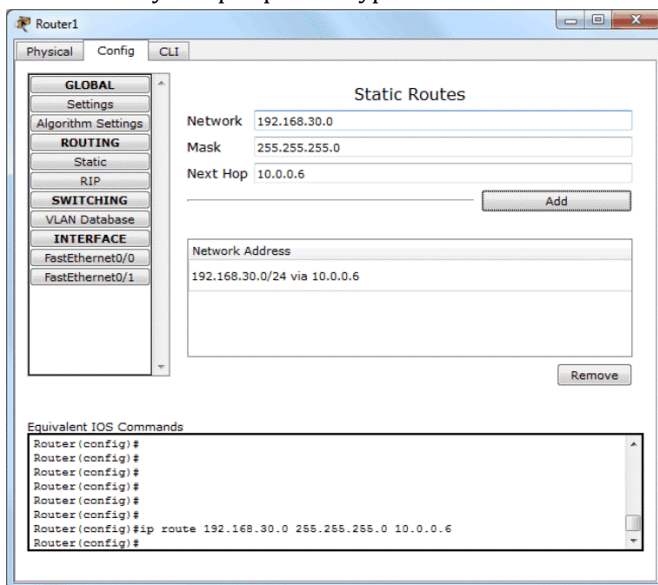


Рисунок 14 – Раздел Маршрутизация

База данных VLAN

Этот раздел позволит создавать или удалять виртуальные локальные сети VLAN (подробно рассматриваются в десятой главе). Здесь производятся изменения самой базы данных, добавление же интерфейсов в конкретную виртуальную сеть (рисунок 15) делается в следующем разделе.

Параметры интерфейсов

Данный раздел различается для коммутаторов и маршрутизаторов. Коммутаторы имеют следующие опции (рисунок 16): выбора скорости и режима работы, а также добавления порта к VLAN.

На маршрутизаторе вместо добавления к VLAN имеется настройка IP-конфигурации.

При изменении скорости и режима работы порта (по умолчанию – **Авто (Auto)**) на одной стороне необходимо установить такую же скорость и режим работы на другой. Например, если на одной стороне вы установите скорость 100 Мбит/с, а на другой 10 Мбит/с, соединение будет находиться в состоянии **Выключено (Down)**.

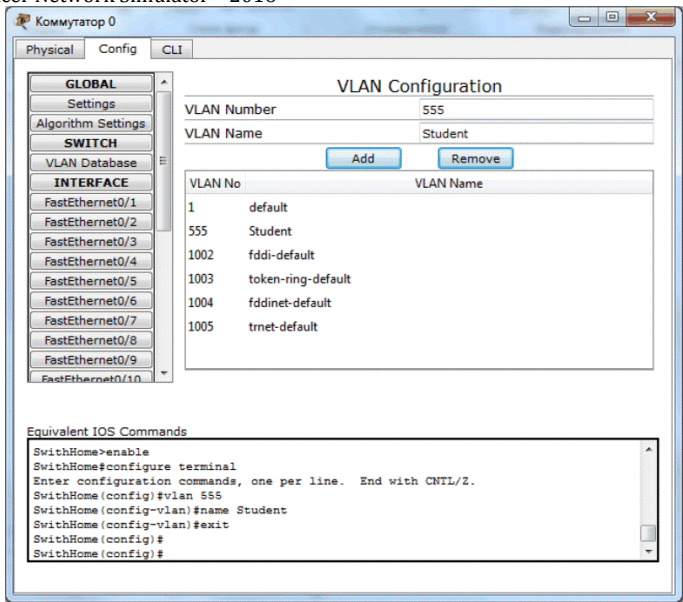


Рисунок 15 – База данных VLAN

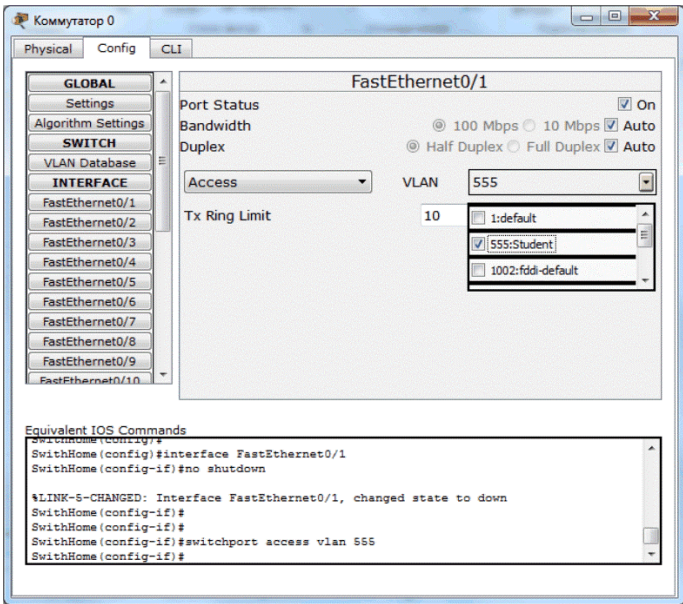


Рисунок 16 – Параметры интерфейсов коммутатора

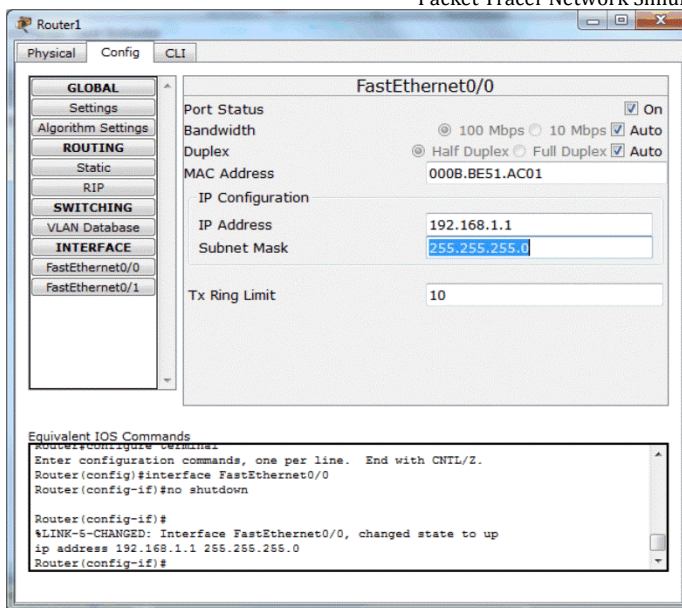


Рисунок 17 – Параметры интерфейсов маршрутизаторов

Резюме

В этой главе мы изучили некоторое количество информации о сетевых устройствах и их модулях с присущими им характеристиками, ограничениями и системой наименования. Ознакомились с методами доступа к интерфейсу командной строки и принципами настройки устройств с помощью интерфейса командной строки (CLI). Теперь мы можем двигаться дальше и сделать попытку создать простую топологию с парой маршрутизаторов и компьютеров, находящихся в разных логических сетях.

В следующей главе, мы познакомимся с оконечными устройствами доступными в Packet Tracer и параметрами их вкладки **Настройка (Config)**. Возможно, вы будете удивлены большому разнообразию устройств доступных в программе.

3 ОБЩАЯ ИНФОРМАЦИЯ ОБ ОКОНЕЧНЫХ УСТРОЙСТВАХ

Сетевые устройства являются основой сети, и оконечные устройства взаимодействуют через них. В Packet Tracer имеется широкий спектр оконечных устройств, начиная с ПК и ноутбуков, планшетных ПК, КПК и заканчивая телевизорами. В этой главе мы изучим каждое устройство и модули, подходящие к ним, а также доступные конфигурационные опции. Вы будете удивлены, как много модулей поддерживаются для оконечных устройств. Как и для сетевых устройств, так и для оконечных имеется множество утилит доступных через вкладку **Рабочий стол (Desktop)**, совпадающие с аналогичными существующими в реально мире.

Персональные компьютеры и ноутбуки

ПК и ноутбуки являются самым высоким уровнем пользовательских устройств. Между ними нет принципиальной разницы (что проявляется в удобстве использования), различия проявляются в политике именования модулей.

Ниже перечисленные модули, доступные для ПК и ноутбуков. Подобно маршрутизаторов, как вы могли убедиться в прошлой главе, эти устройства также нужно выключать, прежде добавления или удаления модулей.

1) **Linksys-WMP300N**. Обеспечивает беспроводной интерфейс для настройки подключения к Wi-Fi сети.

2) **PC-HOST-NM-1AM**. Имеет RJ-11 интерфейс, используемый для подключения телефонного модема.

3) **PC-HOST-NM-1CE, PC-HOST-NM-1CFE, PC-HOST-NM-1CG**. Эти три модуля служат для Ethernet, FastEthernet, GigabitEthernet подключения соответственно.

4) **PC-HOST-NM-1FFE, PC-HOST-NM-1FGE**. Оптические версии предыдущих модулей.

5) **PC-HOST-NM-1W, PC-HOST-NM-1W-A**. Оба этих модулей обеспечивают беспроводной интерфейс. Первый из модулей работает на частоте 2.4ГГц, второй – 5 ГГц (беспроводная сеть стандарта IEEE 802.11a).

6) **PC-HEADPHONE, PC-MICROPHONE, PC-CAMERA, PC-USB-HARD-DRIVE**. Эти модули служат для представления соответствующих устройств (наушники, микрофон, камера, жесткий диск с USB-интерфейсом).

Для ноутбуков эти модули имеют другие названия. Вместо слова HOST используется слово LAPTOP. Так модуль PC-HOST-NM-1AM называется PC-LAPTOP-NM-1AM.

Сервера

Сервера совершенно отличны от других оконечных устройств. У них имеется различная функциональность и предусмотрено место для установки двух сетевых адаптеров. Модули, предназначенные для серверов, такие же как и для ПК, за исключением того, что для серверов не существует модуля PC-HOST-NM-1AM.

Перенесите на рабочее пространство, сервер. Кликните по его изображению и перейдите на вкладку **Службы (Services)**. Вы можете увидеть следующие доступные сервисы и службы.

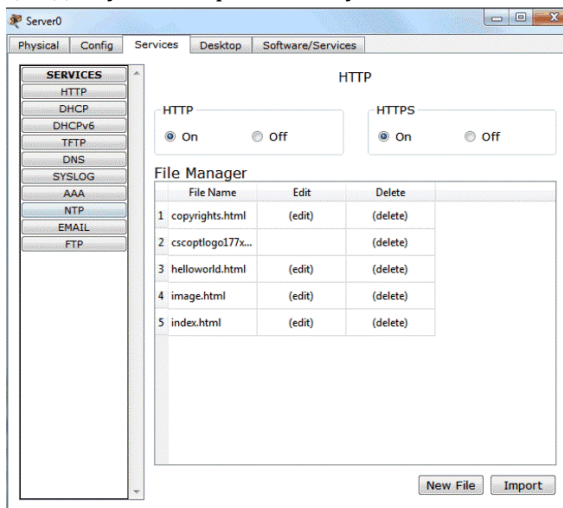


Рисунок 18 – Вкладка «Службы» сервера

HTTP

Служба HTTP предполагает работу веб-сервера с поддержкой протоколов HTTP и HTTPS. Окно этой службы служит для создания и редактирования статических HTML-страниц, которые отображаются при введении адреса в веб-браузер на пользовательском устройстве. Эта служба включена по умолчанию.

DHCP

Служба DHCP может быть использована для автоматического назначения IP-адресов маршрутизаторов. Здесь имеются опции для создания и редактирования пула IP-адресов. По умолчанию пул носит название **serverPool** и не может быть удален или изменен. Данная служба включена по умолчанию. Начиная с шестой версии программы доступна служба DHCPv6.

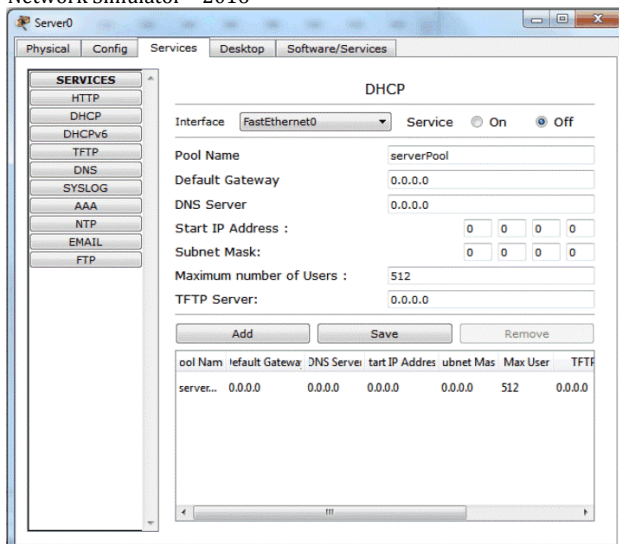


Рисунок 19 – Служба DHCP

TFTP

Служба TFTP очень востребована при изучении резервирования и восстановления образов Cisco IOS и конфигурационных файлов. В этой секции находится список из нескольких образов операционной системы некоторых маршрутизаторов и коммутаторов, работающих в Packet Tracer. При копировании образа любого устройства на TFTP-сервер файл автоматически добавляется к этому списку. Пример работы TFTP-сервера доступен в папке \saves\Server\TFTP\TFTP.pkt. Эта служба включена по умолчанию.

DNS

Служба DNS предназначена для разрешения символьных имен (DNS-имен) в IP-адреса и наоборот. Служба DNS предлагает поддержку следующих типов записей: **A** (адресная запись), **CNAME** (каноническое имя для псевдонима), **SOA** (учетная запись начала полномочий) и **NS** (учетная запись именного сервера). Хотя и интерфейс службы достаточно прост, тем не менее многоуровневая служба DNS может быть настроена через него. Пример такого использования находится в папке \saves\Server\DNS\Multilevel DNS.pkt.

Кнопка **кэш DNS (DNS cache)** позволяет увидеть кэшированные DNS-запросы, а также обеспечивается возможность чистки этого кэша. По умолчанию эта служба отключена.

Syslog

Данный протокол служит основой для централизованного хранения системного журнала. Установка IP-адреса сервера Syslog на вкладке **Настройка (Config)**, а также указание IP-адреса сервера Syslog в настройках сетевого устройства представлена таблица (рисунок 22) будет заполняться системными сообщениями, генерируемыми сетевым устройством. Эта служба включена по умолчанию.

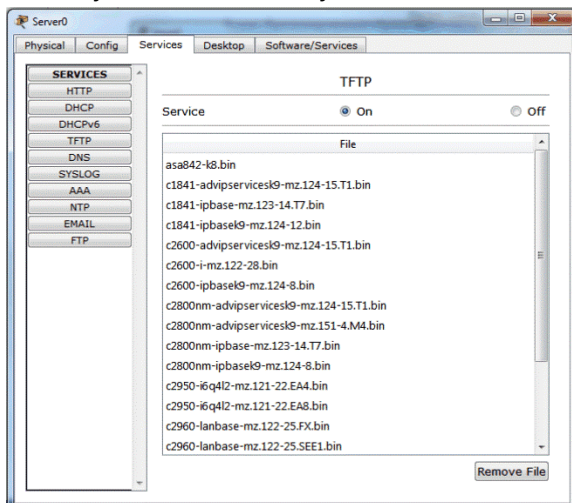


Рисунок 20 – Служба TFTP

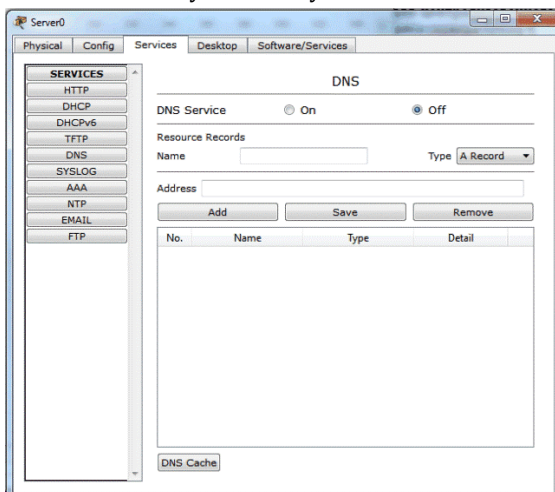


Рисунок 21 – Служба DNS

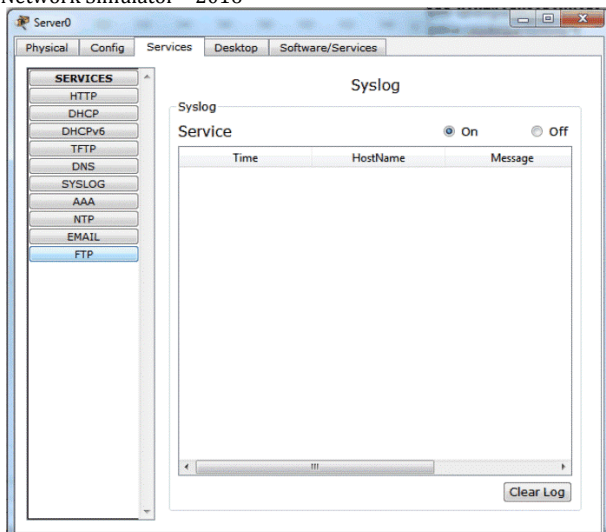


Рисунок 22 – Служба Syslog

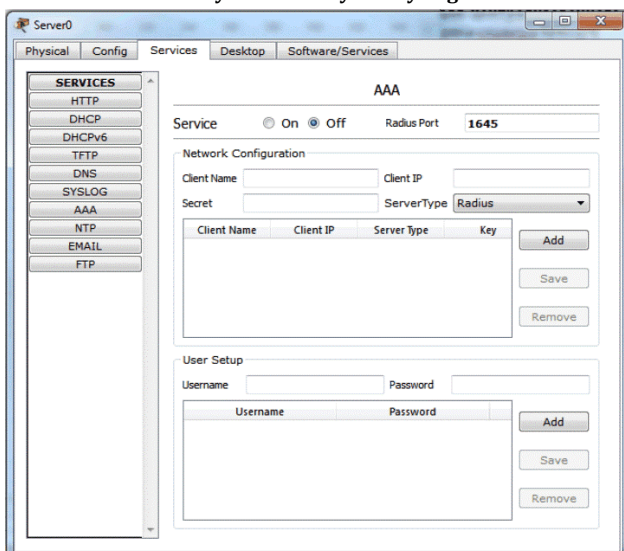


Рисунок 23 – Служба AAA

AAA

AAA расшифровывается как аутентификация (Authentication), авторизация (Authorization) и учет (Accounting.) Этот сервис используется для централизованного управления полномочиями всех сетевых

устройств. Поддерживаются протоколы аутентификации RADIUS и TACACS. Опции этой секции позволяют создавать пользователей и настраивать сетевые разрешения. Пример доступен в \saves\Server\AAA\ . Данная служба отключена по умолчанию.

NTP

Протокол сетевого времени обеспечивает источник и синхронизацию сетевого времени. В этой секции устанавливаются дата и время. Дополнительно можно настроить аутентификацию NTP. После установки времени на сервере все сетевые устройства могут быть сконфигурированы на синхронизацию своих внутренних часов с этим сервером. По умолчанию служба включена.

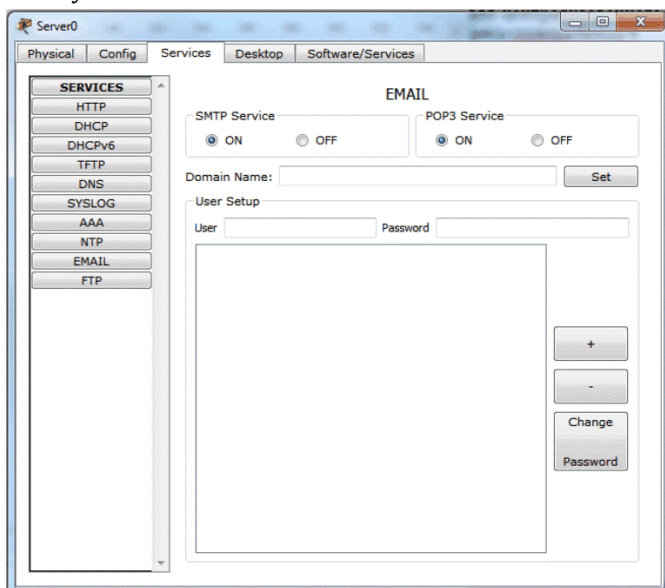


Рисунок 24 – Служба сетевого времени

Email

Эта секция включает настройку почтовых протоколов SMTP и POP3. Здесь можно указать доменное имя и создать пользователей, что позволит этим пользователям взаимодействовать, используя утилиту **Электронная почта (EMAIL)** вкладки **Настройка (Config)** ПК или ноутбука.

Только один почтовый домен разрешен на сервера, и протоколы SMTP или POP3 могут включены или отключены по желанию.

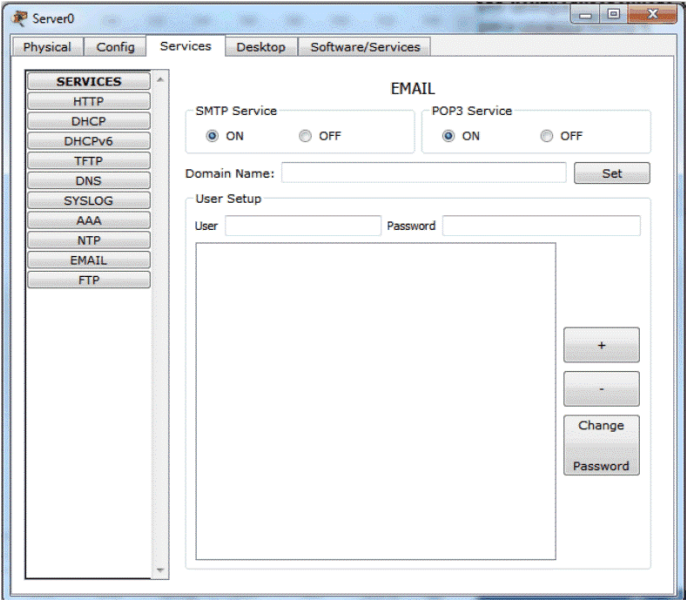


Рисунок 25 – Служба EMAIL

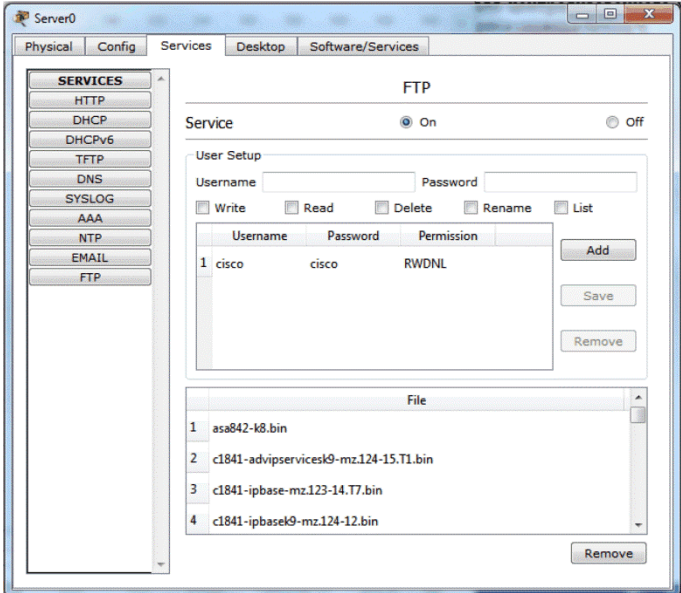


Рисунок 26 – Служба FTP

FTP

FTP имеет гораздо больше возможности TFTP. В этой секции указываются пользователи и разрешения, которые могут быть представлены каждому из них. Также здесь перечисляются файлы, что могут быть загружены. В настройка ПК нет графического интерфейса для взаимодействия с ftp-сервером, и доступ к нему осуществляется через утилиту командной строки вкладки **Настройка (Config)**. Пример доступен в папке `\saves\Server\FTP\FTP.pkt`.

Firewall/IPv6 Firewall

Начиная с шестой версии Packet Tracer поддерживается два вида брандмауэр (IPV4 и IPV6). В этой секции вам доступна настройка правил, основанных на совпадении IP-адреса отправителя или получателя, локального или удаленного номера порта TCP или UDP. Соединение, совпавшие с правилом, может быть разрешено или запрещено.

Другие пользовательские устройства

Кроме ПК, ноутбуков и серверов, Packet Tracer имеет много других пользовательских устройств. Некоторые из них не имеют никакой функциональности, другие предоставляют интересные возможности.

1) **Printer-PT**. Сетевой принтер имеет модули подобные модулем ПК, за исключением PC-HOST-NM-1AM. Единственная доступная опция – назначение IP-адреса.

2) **7960**. Это устройство представляет собой Cisco IP-телефон, имеющий два Ethernet-порта: один подключается к коммутатору, к другому подключается ПК. Единственный доступный модуль **IP_PHONE_POWER_ADAPTER**, необходимый при отсутствии питания по проводке PoE (Power over Ethernet).

3) **Home-VoIP-PT**. Это устройство предназначена для преобразования сигналов аналоговый телефонии в VoIP, не имеет модулей и содержит единственную настройку: IP-адрес сервера. В качестве сервера может использоваться IP-адрес маршрутизатора, на котором запущен коммуникационный менеджер **Communications Manager Express(CME)**. Устройство имеет один Ethernet port, для подключения к сети, и один порт RJ-11, для подключения аналогового телефона.

4) **Analog-Phone-PT**. Телефон для традиционной (аналоговой) телефонии. Имеет интерфейс RJ-11. При подключении к предыдущему устройству позволяет делать вызов на Cisco IP-телефон.

5) **TV-PT**. Устройство представляет собой телевизор с коаксиальным подключением и единственной опцией включения. На экране

устройства (вкладка **Физический вид (Physical)**) отображается слайд-шоу при подключении к облачному устройству **Cloud-PT**.

6) **TabletPC-PT**. Планшетный компьютер по своим опциям аналогичный ПК, но не имеющий никаких модулей. Предполагает подключение к беспроводной сети **WLAN**.

7) **PDA-PT**. КПК – устройство, аналогичное предыдущему.

8) **WirelessEndDevice-PT**. Пользовательское устройство с беспроводным подключением. Имеет графический интерфейс пользователя, с редактируемым HTML-кодом. Вкладка **Графический интерфейс (GUI)** располагает генератором трафика (**Traffic Generator**) таким же как и у ПК и ноутбука.

9) **WiredEndDevice-PT**. Устройство подобное предыдущему, но имеющее проводной подключение.

10) **Sniffer**. Анализатор протоколов – устройство, появившееся в шестой версии, предназначено для захвата и последующего изучения сетевого трафика. Имеет два Ethernet-порта и при подключении к коммутатору требует перекрестного кабеля (Cooper Cross-Over). Отображение захваченного трафика производится на вкладке **Графический интерфейс (GUI)**.

Настройка пользовательских устройств

У пользовательских устройств имеется вкладка **Рабочий стол (Desktop)**, обеспечивающая набор утилит для тестирования и отладки сети. В этой главе мы изучим каждую утилиту.

Следующие утилиты доступны для ПК, ноутбуков, КПК и планшетов.

IP-конфигурация (IP Configuration)

Еще в первой главе мы имели возможность познакомиться с этой графической утилитой, когда создавали простую топологию. Ее функционал используется для выбора динамического (автоматического) или статического (ручного) назначения информации IP протокола. При вводе статического IP-адреса поле маски (**Subnet Mask**) заполняется автоматически в соответствии классом введенного IP-адреса. Также возможно редактировать полученное значение маски. При выборе опции динамическое назначение IP-адреса (**DHCP**) в сети требуется наличие настроенного **Server-PT** с поддержкой протокола DHCP. Начиная с шестой версии Packet Tracer, доступна секция для конфигурирования IP-адресов шестой версии (IPv6).

Коммутируемый доступ (Dial-up)

Коммутируемый доступ станет возможным лишь при установке модуля **PC-HOST-NM-1AM**. Эта утилита доступна только для ПК (PC-PT) и

ноутбука (**Laptop-PT**), прочие пользовательские устройства на предполагают наличия этого модуля (**NM-1AM**). Для обеспечения коммутируемого доступа требуется устройство **Cloud-PT** с соответствующим телефонным номером, на одной стороне которого подключается ПК, с другой – маршрутизатор с модемным интерфейсом. При подключении на ПК требуется ввод имени пользователя и пароля, ранее внесенных в конфигурацию маршрутизатора.

Терминальное подключение (Terminal)

Эту утилиту мы использовали ранее (глава 2) для доступа к интерфейсу командной строки CLI через консольный порт. В большинстве случаев используются настройки по умолчанию (рисунок 27). Если же вы измените скорость доступа к консольному порту через регистр состояния сетевого устройства, то эти же изменения следует ввести и в утилите. Данная утилита недоступна для **Server-PT**, т.к. сервер не имеет интерфейс RS-232.

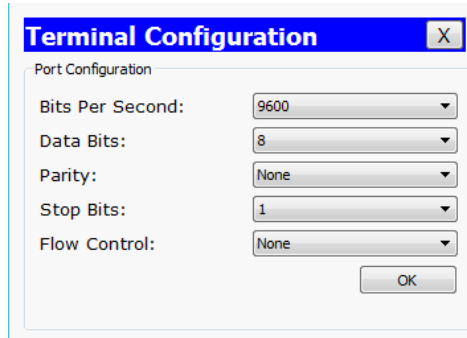


Рисунок 27 – Настройки терминального подключения по умолчанию

Командная строка (Command Prompt)

Эта утилита имитирует командную строку операционной системы Microsoft Windows. Правда, поддерживается ограниченный набор команд, но его вполне достаточно для тестирования сети. Доступны следующие команды:

```
? arp delete dir ftp help ipconfig ipv6config netstat
nslookup ping snmpget snmpgetbulk snmpset ssh telnet tracert
```

Каждая команда поддерживает параметры, которые могут быть выяснены при вводе команды без всякий опций, как показано на рисунке 28.

Веб-браузер (Web Broser)

Веб-браузер – утилита с минимальными возможностями, которые можно применить для настройки серверного компьютера **Server-PT** или

Packet Tracer Network Simulator – 2016

для доступа к веб-интерфейсу беспроводного маршрутизатора Linksys-WRT300N. У этой утилиты есть только четыре кнопки: **Назад (back)**, **Вперед (forward)**, **Перейти (go)**, **Стоп (stop)**. При этом не поддерживается история запрос и кэширование страниц.

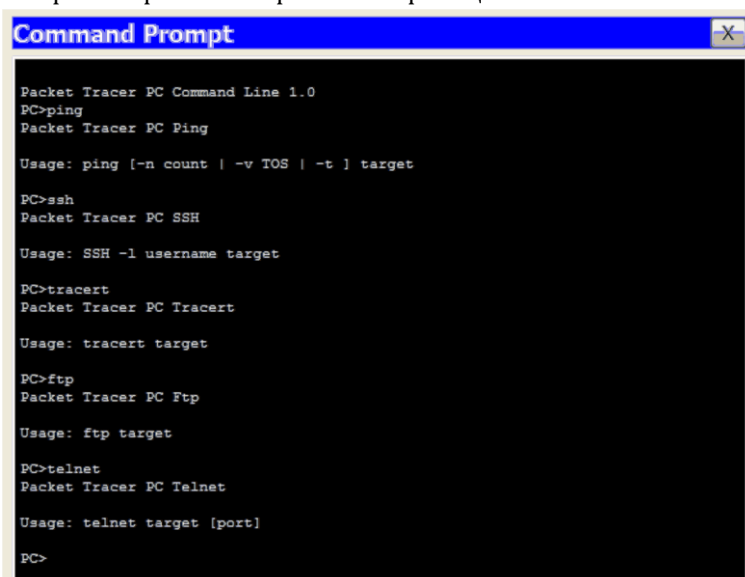


Рисунок 28 – Командная строка

Беспроводное подключение (PC Wireless)

Эта утилита разработана специально для поддержки беспроводного модуля **Linksys-WMP300N**. Она отображает уровень мощности сигнала, а также имеет опции для выбора беспроводной сети и изменения профиля подключения к беспроводному маршрутизатору, который не распространяют широковежательно идентификатор сети SSID. Эти установки могут быть сохранены, импортированы или экспортированы. Более подробно о беспроводных сетях описывается в главе 9. Данная утилита доступна только для ПК или ноутбука, т.к. прочие устройства не имеют беспроводного модуля **Linksys-WMP300N**.

Частная виртуальная сеть (VPN)

Утилита VPN используется для создания VPN-подключения для безопасного взаимодействия. При этом маршрутизатор конфигурируется как VPN-сервер. Пример можно найти в следующей папке:
\\saves\\PC\\VPN\\Vpn_Easy.pkt.

Генератор трафика (Traffic Generator).

Эта утилита функционально подобна инструментам **Add Simple PDU** и **Add Complex PDU** общей панели инструментов. Позволяет создавать пользовательские пакеты и посылать их в сеть с периодическим интервалом. Данная утилита востребована для имитации реальной сетевой среды.

Обозреватель базы данных информации управления (MIB Browser)

Браузер базы данных информации управления MIB (Management Information Base) посылает SNMP-запросы. Это позволяет извлекать данные из маршрутизаторов и коммутаторов или производить изменения в настройках устройств. Get-запрос посылается для получения значения, а set-запрос отправляется для модификации значений параметров. При этом маршрутизатор должен быть настроен с соответствующей строкой сообщения «только чтение» **RO (Read Only)** или «чтение-запись» **RW (Read Write)**. Данная утилита не доступна для серверного компьютера (Server-PT). Пример топологии с использованием SNMP-протокола находится в папке \saves\PC\MIB_Browser\SNMP_Router.pkt.

IP-коммуникатор (Cisco IP Communicator)

Cisco IP Communicator представляет собой образец программного обеспечения Cisco, превращающий компьютер в IP-телефон. Эта утилита, доступная в Packet Tracer, позволяет делать звонок или отвечать на него используя ПК или ноутбук. Кликните для открытия IP-коммуникатора, при этом появится графический интерфейс, который можно использовать для набора номера. Сервер TFTP, настроенный по умолчанию может быть изменен с помощью опции **Настройка (Preference)**, как показано на рисунке 29. Следует заметить, что данная утилита также недоступна для серверного компьютера.

Электронная почта (Email)

Почтовый клиент используется для отправки и приема сообщений электронной почты. Когда вы открываете данную утилиту впервые, вам предлагается настроить сервера входящей (POP3) или исходящей (IMAP) почты, а также некоторые другие настройки. Для того, чтобы в полной мере задействовать работу электронной почты, необходимо наличие серверного компьютера с настроенной секцией электронной почты. Пример доступен в папке \saves\Server\Mail\mail_2Server_2PC.pkt.

Подключение по PPPoE (PPPoE Dialer)

Эта утилита требуется при установлении соединения с использованием устройства DSL-Modem-PT. С одной стороны к модему подключается

ПК с Ethernet-интерфейсом, а другой стороной модем подключается к облаку WAN, с использованием телефонного кабеля. Маршрутизатор должен быть сконфигурирован как PPPoE-сервер с указанием логина и пароля. Пример доступен в папке \saves\Router\PPPOE\client.server.modem.pppoe.pkt.



Рисунок 29 – Опция Настройка (Preference) IP-коммуникатора

Текстовый редактор (Test Editor)

Данный текстовый редактор подобен Блокноту в ОС Windows. Он может создавать, редактировать и сохранять текстовые файлы, которые могут быть перечислены при использовании команды `dir` утилиты командной строки. Созданный текстовый файл также может для тестирования загрузки/ выгрузки файлов по FTP-протоколу с использованием утилиты командной строки (команда `ftp`).

Резюме

В этой главе мы рассмотрели все пользовательские устройства доступные в Packet Tracer. Здесь же и подведем черты этапа изучения устройств программы. Создайте самостоятельно и проверьте каждую

схему, приведенную в этой главе. Далее мы приступаем к использованию устройств доступных в Packet Tracer.

В следующей главе мы будем создавать топологии, которые включают изученные устройства. Мы также изучим, как пакеты перемещаются от одного устройства к другому, используя при этом имитационный режим. Мы также увидим, как создавать кластеры из множества устройств для более чистого вида рабочего пространства.

4 СОЗДАНИЕ ТОПОЛОГИИ СЕТИ

Ранее нами изучена глава об устройствах доступных в Packet Tracer. В этой же главе мы положим начало изучения как их использовать. Разберемся как создавать топологию сети, как подключать устройства и отслеживать состояние линий связи. Проведем тест связности, задействовать для этого вначале инструмент Протокольный блок данных **PDU (Protocol Data Unit)**, вначале простой (**Simplex PDU**), а затем и более сложный (**Complex PDU**). Стоит сделать это однажды, и вы, несомненно, найдете интересным и полезным наблюдение за передвижением блоков данных между устройствами. При этом придется прибегнуть к режиму имитации (**Simulation Mode**). И, наконец, мы обеспечим более чистый вид рабочего пространство, используя объединение устройств в кластер.

Подключение устройств

При выборе категории **Подключения (Connection)** в окне выбора устройств, можно заметить несколько типов кабелей в окне выбора конкретного типа кабеля. Packet Tracer поддерживает следующие типы кабелей, которые могут быть использованы для соединения устройств.

Консольное подключение (Console)

Консольной кабель используется для подключения к сетевому устройству и последующей настройки с помощью ПК или ноутбука. Один конец кабеля подключается к консольному порту сетевого оборудования, другой конец к порту RS-232 ПК или ноутбука.

Прямой кабель (Copper straight-through)

Этот тип кабеля является стандартным Ethernet-кабелем для соединения двух устройств, работающих на разных уровнях модели OSI (разноранговых, таких как хаб и маршрутизатор, ПК и коммутатор). Может быть использован при подключении к Ethernet, Fast Ethernet и Gigabit Ethernet портам. Данный тип кабеля имеет аналог в реальном мире – витая пара UTP.

Перекрестный кабель (Copper straight-through)

Используется для подключения одноранговых устройств (работающих на одном и том же уровне модели OSI, таких как хаб к хабу, ПК к ПК, ПК к маршрутизатору, ПК к принтеру), а также при подключении коммутатора и хаба. Данный тип кабеля также используется при подключении к Ethernet, Fast Ethernet и Gigabit Ethernet портам. Имеет аналог в реальном мире – витая пара UTP с перекрестным подключением.

Оптоволокно (Fiber)

Предполагает подключение к оптическим Ethernet, Fast Ethernet и Gigabit Ethernet портам.

Телефонный кабель (Phone)

Кабель предназначен для подключения аналогового телефона с разъемом RJ-11 к VoIP-телефону или к модему. Также может использоваться к подключения к модемному порту маршрутизатора.

Коаксиальный кабель (Coaxial)

Коаксиальный кабель используется для подключения кабельного модема ил телевизора к облаку.

Последовательный кабель

Последовательный кабель соединяет маршрутизаторы друг с другом или с облаком. Кабель с DCE-окончанием (Data Circuit-terminating Equipment, для аппаратуры передачи данных) является стороной, ответственной за генерацию синхросигнала. Для установки частота синхронизации требуется ввести на маршрутизаторе, подключенном на этой стороне, команды `clock rate <300-4000000>`. При этом линейный протокол окажется в работоспособном состоянии.

При выборе кабеля с DTE-окончанием (Data Terminal Equipment, для оконечного оборудования данных) первое устройство подключается с DTE-окончанием, второй – с DCE-окончанием (и также будет требовать введения соответствующей команды). При выборе кабеля с DCE-окончанием подключение будет противоположным: сначала DCE-подключение, на втором устройстве DTE-подключение.

Консольный кабель-концентратор (Octal)

Данный тип кабеля появился впервые в шестой версии Packet Tracer. Предполагает подключение на одной стороне к одному консольному порту, на другой стороне имеет восемь окончаний с RJ-45 разъемом.

Автоматический выбор типа подключения

Если вы затрудняетесь с необходимым типом кабеля, выбирайте эту опцию и программа автоматически определит наилучший вариант тип подключения. Наилучший тип подключения гарантируется не всегда. В частности, если у вас есть маршрутизатор с последовательными и Ethernet интерфейсами, и вы выбрали именно эту опцию подключения, однако вначале будет выбрано только последовательное подключение (что разумеется не лучший вариант). Также консольное подключение не может быть выбрано автоматически, и требует целенаправленного выбора консольного кабеля.

Статус подключения

После подключения устройств вы обнаружите цветовую индикация на каждом конце кабеля, которая отображает статус подключения.

1) Зеленый цвет говорит о том, что физическое соединение работает, но ничего не говорит работоспособности протокола канального уровня.

2) Зеленый мигающий отображает активность интерфейса при передаче данных.

3) Красный сообщает о том, что физическое соединение не работает. Это может быть по причине выбора неправильного типа кабеля или при административном выключении порта (командой `shutdown`).

4) Янтарный имеет место у коммутаторов и отображает работу порта в соответствии с протоколом связующего дерева STP (Spanning Tree Protocol) по определению резервных связей второго уровня.

Продemonстрируем это на примере топологии, содержащей ПК, ноутбук, коммутатор и маршрутизатор (рисунок 30).

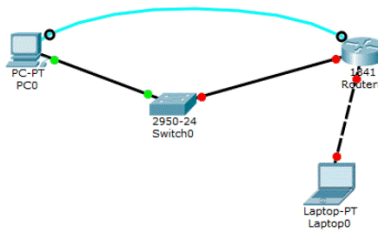


Рисунок 30 – Отображение статусов подключения

После добавления устройств в рабочую область программы переходим к выбору типа кабель (окно выбора типа кабеля). Например для соединения маршрутизатора и ноутбука следует выбрать перекрестную витую пару. Затем кликните по ноутбуку и в контекстном меню вы увидите все доступные для данного устройства интерфейсы. Выберите требуемый интерфейс (например, FastEthernet 0/0), а затем повторите те же действия для маршрутизатора для создания подключения этих устройств между собой.

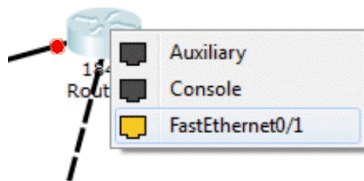


Рисунок 31 – Подключение к порту маршрутизатора

При подключении к маршрутизаторам обратите внимание на красный отображаемый статус портов. Связано это с тем, что порты маршрутизатора по умолчанию выключены. Для устройств, подключаемых к коммутатором, статус подключения будет янтарного цвета, что показывает работу портов коммутатора в соответствии с STP протоколом.

Тест связности

В созданной нами топологии тест связности между устройствами может быть произведен с помощью графических инструментов «Простой PDU» (**simple PDU**) и «Сложный PDU» (**complex PDU**). И хотя тоже самое возможно при использовании утилиты `ping` в командной строке ПК и прочих оконечных устройств, использование этих инструментов, особенно, в больших топологиях позволят быстрее и нагляднее провести тест связности.

Простой PDU (Simple PDU)

Инструмент «Простой PDU» предполагает использование только протокола межсетевых управляющих сообщений **ICMP (Internet Control Message Protocol)**. Создадим сеть, состоящую из ПК и сервера, для демонстрации как этот инструмент работает (рисунок 32):

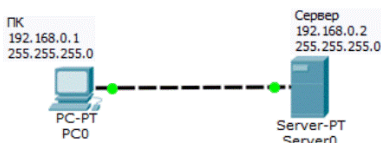


Рисунок 32 – Схема сети для проверки инструмента Simple PDU

- 1) Добавьте ПК и сервер в рабочую область программы и соедините их перекрестным кабелем UTP.
- 2) Присвойте IP-адреса обоим устройствам из одной и той же подсети. Например, для ПК 192.168.0.1/255.255.255.0 и для сервера 192.168.0.2/255.255.255.0.
- 3) На общей панели инструментов кликните по закрытому конверту или используйте клавиатурное сокращение *U*. При этом курсор принимает вид конверта.
- 4) Кликните вначале по ПК, а затем по серверу. Обратите внимание на окно «Пользовательский пакет» (**User Created Packet**). Там (рисунок 33) вы обнаружите статус теста связности «Успешно» (**Successful**), а также указание на источник (**Source**), получатель (**Destination**) и тип пакета (**Type**).

Не правда ли это было очень просто. Посмотрим, что может нам предложить инструмент «Сложный PDU».

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC0	Server0	ICMP		0.000	N	0	(edit)	

Рисунок 33 – Окно «Пользовательский пакет»

Сложный PDU (Complex PDU)

Для демонстрации этого инструмент воспользуемся той же топологией (рисунок 32)

1) Для использования инструмента «Сложный PDU» на общей панели инструментов кликните по открытому конверту или используйте клавиатурное сокращение С.

2) Кликните вначале по ПК, при этом появится диалоговое окно «Создать сложный PDU» (**Create Complex PDU**). Выберите протокол HTTP (**Select Application**), введите IP-адрес сервера в поле «Адрес получателя» (**Destination IP address**), укажите начальное значение порта источника (**Starting Source Port**), укажите временную метку появления пакета (**Time**) и нажмите кнопку «Создать PDU» (**Create PDU**).

Рисунок 34 – Окно «Создать сложный PDU»

3) Посмотрите на окно «Пользовательский пакет». Запись в данном окне свидетельствует об успешном обмене данными TCP-протокола (так называемое трехшаговое рукопожатие TCP). Обратите внимание на красную кнопку в колонке Fire. Кликните по ней дважды и обмен данными будет повторен.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC0	192.168.0.2	TCP		1.000	N	0	(edit)	

Рисунок 35 – Окно «Пользовательский пакет» при трехшаговом квитировании TCP

Работа в режиме имитации (simulation mode)

Все предыдущие примеры мы осуществляли в режиме реального времени (Real-Time), и проверить работоспособность соединения можно только ориентируясь на цветовой статус линии. Режим имитации позволяет отследить как пакеты перемещаются от одного узла к другому. При этом можно дважды кликнуть по пакету для получения детальной информации о пакете с точки зрения модели OSI.

Для перехода в режим имитации используется переключатель выбора режима работы (**Realtime/Simulation Tabs**). В появившемся окне панели режима имитации **Simulation Panel** (рисунок 36) кликните по кнопке «Автозахват/воспроизведение» (**Auto Capture/ Play**) для начала захвата пакетов.

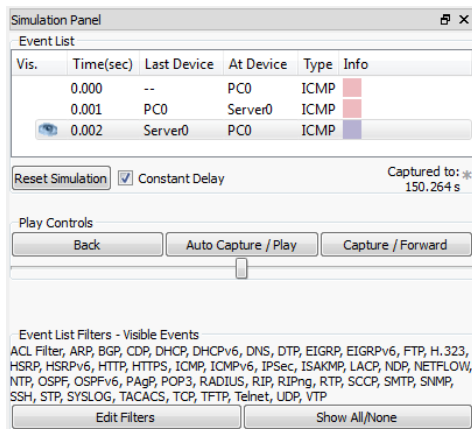


Рисунок 36 – Панель режима имитации

Для примера повторим на предыдущей топологии создание простого PDU. В листе событий (**Event List**) появятся три записи, отображающие этапы создания ICMP-пакета, отправки ICMP-запроса и приема ICMP-ответа.

Если вы кликните по пакету (иконке конверта), вам будет представлена информация о пакете структурированная в соответствии с уровнями модели OSI (рисунок 37). На вкладках «Детализированный входящий/исходящий пакет» (**Inbound PDU Details /Outbound PDU Details**) приводится развернутая информация об заголовках блоков данных каждого из уровней (рисунок 38). Вкладка «Детализированный входящий

Packet Tracer Network Simulator – 2016
пакет» предоставляет информацию о пакете на входе устройства, а вкладка «Детализированный исходящий пакет» – о пакете, покидающем данное устройство.

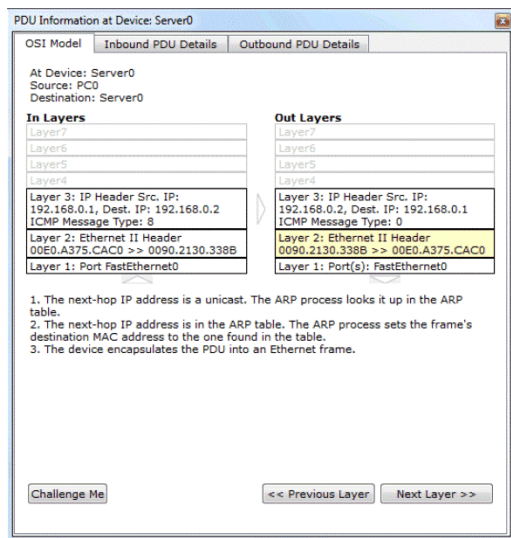


Рисунок 37 – Отображение пакета в соответствии с уровнями модели OSI

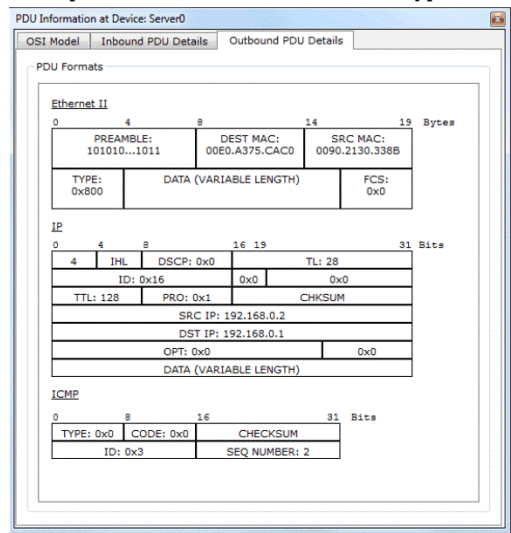


Рисунок 38 – Детализированная информация о исходящем пакете

Для управления режимом имитации в секции «Управление передаче» имеются кнопки, работающие аналогично кнопкам медиа плеера.

– Кнопка «Назад» (**Back**). Нажатие этой кнопки возвращает процесс имитации на один шаг назад.

– Кнопка «Автозахват/воспроизведение» (**Auto Capture/ Play**). Нажатие данной кнопки приводит к автоматическому захвату и отображению процесса передачи пакетов через сеть. Для остановки необходимо повторно нажать кнопку.

– Кнопка «Ручной захват/ Вперед» (**Capture/Forward**). Обеспечивает ручной режим работы. Требуется повторного нажатия для следующего шага продвижения пакетов между устройствами.

Кластеризация схем

При создании топологий большого размера можно столкнуться с ситуацией, когда становится трудно что-либо понять или отследить. В таком случае выручает группировка (кластеризация) некоторых устройств, обеспечивающая объединение этих устройств в одиночное облачное представление. При двойном клике на облаке оно будет раскрываться и отображать сгруппированные устройства в обычном представлении.

Давайте посмотрим как создается кластер устройств.

1) В качестве примера воспользуемся следующей топологией, содержащей 3 коммутатора и 9 ПК (рисунок 39). И хотя эта схема не сильно загромождена, но послужит для демонстрации принципов кластеризации, как следует поступать при будущих затруднениях.

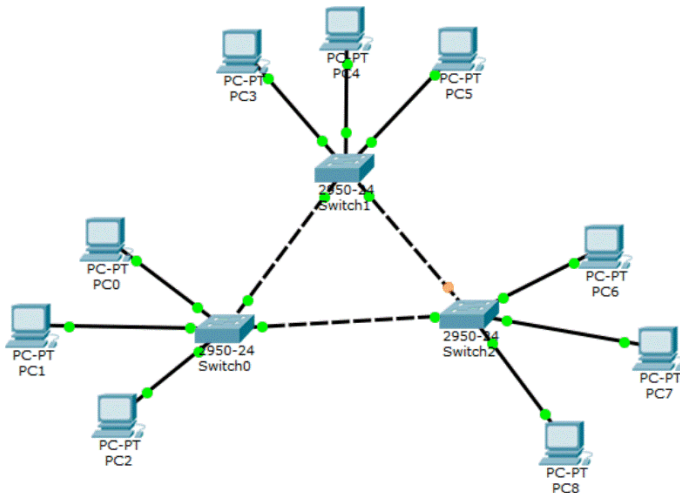


Рисунок 39 – Исходный пример для группировки устройств

2) Кликните в чистом месте около ПК0 и протяните мышкой для выделения ПК0-ПК2 и коммутатора Switch0. Затем нажмите кнопку «Новый кластер» (**New Cluster**), расположенную над рабочим пространством. При этом выделенные устройства будут объединены в кластер. Повторите эти действия для двух оставшихся групп из трех компьютеров и коммутатора.

3) В итоге наша топология после группировки будет выглядеть следующим образом (рисунок 40).

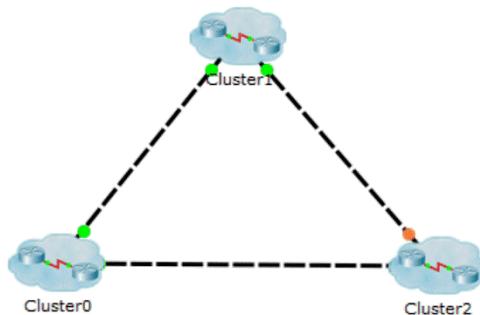


Рисунок 40 – Итоговая схема после кластеризации

4) Двойной щелчок по кластеру развернет группу и покажет только устройства, входящие в него. Для того, чтобы вернуться назад в рабочее пространство следит нажать кнопку «Назад» (**Back**)

Кластеризация также может быть использована для группировки и сокрытия подробностей внешних устройств. Следует заметить, что кластеризация имеет отношение к логическому рабочему пространству и не оказывает влияния на отображение устройств в физическом рабочем пространстве.

Резюме

В этой главе мы изучили принципы создания схемы сети в Packet Tracer, доступные варианты подключения устройств и отображения статуса линии. Мы также увидели, как производится тест связности с использованием графических инструментов простого и сложного PDU. Функция тестирования окажет вам помощь во многих топологиях, которые вы будете строить. Затем вы видели режим имитации, который можно использовать для того, чтобы увидеть разницу между концентраторами и коммутаторами. Наконец, мы изучили принципы создания и управления кластеризации.

В следующей главе мы будем работать с физическим рабочим пространством Packet Tracer и начнем создавать коммуникационные шкафы, рабочие офисы и целые города! Мы будем изучать физические ограничения каждой сетевой технологии и назначения таких устройств как повторители.

5 РАБОТА В ФИЗИЧЕСКОМ ПРОСТРАНСТВЕ

Симулятор, как следует из названия, осуществляет только имитацию работы логического взаимодействия устройств. Однако, Packet Tracer позволяет сделать больше: он также имитирует работу устройств на физическом уровне взаимодействия.

Создание объектов физического рабочего пространства

До сих пор мы использовали логическое рабочее пространство для создания топологий сети. Физическое рабочее пространство делает вашу логическую топологию более осязаемой, придавая ей физическое измерение. Физическое рабочее пространство имеет четыре различных типа сред: междугородное окружение, город, здание и телекоммуникационный шкаф.

Междугородное окружение (Intercity). Самый масштабный вид среды, состоящее из городов. Города, здания и телекоммуникационные шкафы могут быть добавлены на этом уровне с использованием контрольной панели.

Города (Cities). Этот слой включает здания и телекоммуникационные шкафы. По умолчанию город называется «Домашний город» (**Home City**). Домашний город может быть передвинут и размещен в любом месте междугородной карты.

Здания (Buildings). Этот слой содержит телекоммуникационные шкафы. По умолчанию называется «Корпоративный офис» (**Corporate Office**).

Телекоммуникационный шкаф (Wiring closet). Последний слой содержит устройства, размещенные в логической топологии. Его стандартное название «Главный телекоммуникационный шкаф» (**Main Wiring Closet**) и не имеет никаких других подразделений.

Физическое перемещение устройства

Все устройства, задействованные в логическом пространстве, размещаются в главном телекоммуникационном шкафу. В этом разделе мы изучим как перемещать их.

1) Создайте схему сети в логическом рабочем пространстве, состоящую из двух компьютеров. Замените их модули по умолчанию на модуль **PT-HOST-NM-1FGE** (предварительно выключив питание компьютера), т. к. медные кабели Ethernet имеют существенное ограничение по расстоянию. Соедините компьютеры между собой и присвойте им IP-адреса из одной подсети.

2) Переключитесь на физический вид и нажмите кнопку «Новый город» (**New City**) на желтой панели инструментов. Переименуйте вновь созданный город, например, дайте ему имя Удаленный город (**Remote City**). Затем откройте город и создайте в нем новое здание, а в нем создайте новый телекоммуникационный шкаф.

3) Используя кнопку «Навигация» (**Navigation**), перейдите к главному телекоммуникационному шкафу **Home City**→ **Corporate Office**→ **Main Wiring Closet**. В нем находятся оба ПК, которые мы разместили на логическом рабочем пространстве (рисунок 41).

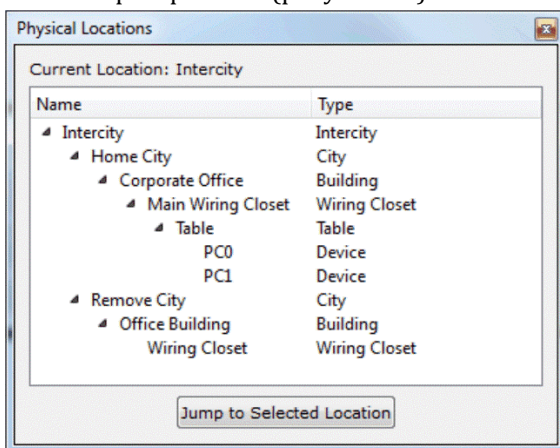


Рисунок 41 – Перемещение между объектами физического рабочего пространства

4) Используя кнопку «Переместить объект» (**Move Object**) (или клавиатурное сокращение Shift+M), а затем кликните на любом ПК и переместите его в «Удаленный город» **Remote City**→ **Office Building**→ **Wiring Closet** (рисунок 42). Эту операцию можно также осуществить в окне навигации перетаскиванием объекта.

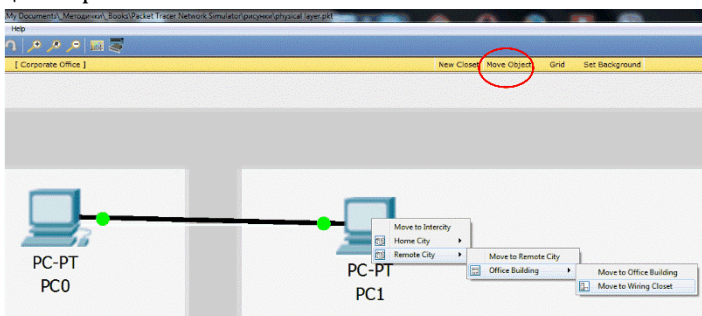


Рисунок 42 – Перемещение объектов на физическом плане

5) Перейдите на междугородный уровень и вы увидите связь между Удаленным и Домашним городами.

Вернитесь в логическое рабочее пространство и вы обнаружите, что изменения, внесенные на физическом плане, не оказывают никакого влияния на топологию сети.

Устройства в физическом рабочем пространстве могут быть перемещены на любой уровень: междугородный, городской, здание и телекоммуникационный шкаф. При этом их изображения будут находиться в соответствующем физическом окружении.

Управление кабеля и расстояниями

На физическом плане может быть определена информация о длине кабеля и расстоянии между устройствами. Такая возможность очень востребована для размещения беспроводных устройств.

Измерение длины кабельной линии

Измерение длины кабеля производится размещением указателя мыши над кабелем (рисунок 43).

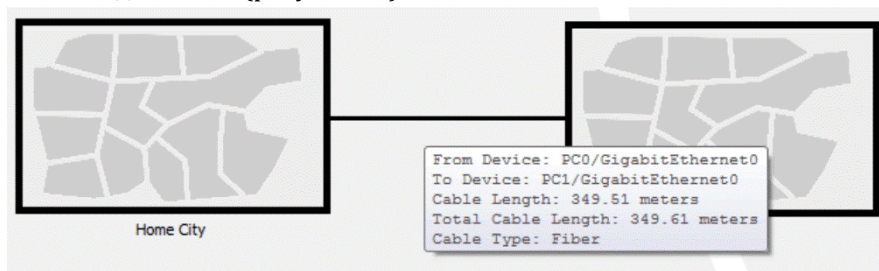


Рисунок 43 – Измерение длины кабельной линии

Стандартный медный кабель можно использовать для подключения устройств, размещенных на расстоянии не более 100 м. Давайте убедимся в этом.

1) Создайте такую же, как и прежде, схему сети из двух компьютеров, но при этом используйте медный кабель вместо оптоволоконного.

2) Перейдите на физический план и разместите оба компьютера в разных городах.

3) Поднимитесь на междугородный уровень и проверьте расстояние между устройствами. Если дистанция меньше 100 м, отодвиньте устройства подальше друг от друга, пока дистанция между ними не превысит 100 м.

4) Вернитесь на логический план и вы обнаружите выключенное состояние портов с обеих сторон (красный цвет индикатора), т. к. соединение между устройствами нарушено из-за превышения максимального расстояния между устройствами для данного типа кабеля (Примечание: в некоторых версиях Packet Tracer может потребоваться сброс по питанию (кнопка **Power Cycle Devices** в нижней части программы)).

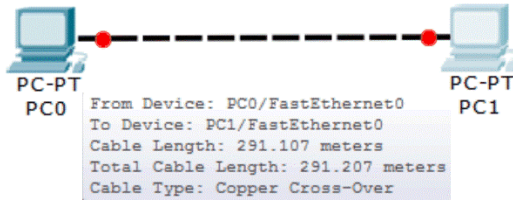


Рисунок 44 – Превышение максимальной длины кабеля

5) Удалите кабельную линию между устройствами и разместите повторитель (**Repeater-PT**) из секции концентраторы (**Hub**). Подключите оба компьютера к повторителю с использованием прямого медного кабеля. Состояние соединения по-прежнему будет выключено, т. к. повторитель по умолчанию помещен в главный телекоммуникационный шкаф и кабельная длина превышает максимально возможную.

6) Перейдите на физический план в главный телекоммуникационный шкаф и переместите повторитель на междугородный уровень между двумя компьютерами. После этого вы обнаружите, что линии находятся в работоспособном состоянии (рисунок 45), т. к. повторитель усиливает сигнал, который падает по причине затухания из-за большой длины кабеля. (Примечание: при слишком большом расстоянии между устройствами может потребоваться подключение нескольких повторителей, т. к. витая пара по-прежнему имеет ограничение максимального расстояния 100 м).

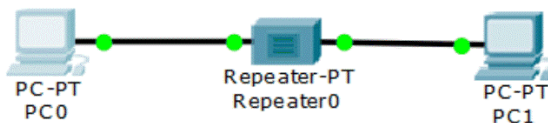


Рисунок 45 – Подключение повторителя

Манипуляция с кабелем

Попробуем произвести кабельные манипуляции на физическом плане. Представим себе ситуацию, когда у вас имеется множество устройств, при этом легко запутаться в кабельных подключениях. Физическое рабочее пространство Packet Tracer имеет возможность, которая разрешает использовать цветовую расцветку кабелей.

Для цветового кодирования кабеля кликните на проводе в физическом рабочем пространстве, выберите пункт меню «Цвет кабеля» (**Color Cable**) и подберите цвет в диалогом окне «Выбор цвета» (**Select Color**). Результат представлен на рисунке 46 (Примечание: для получения аналогичного вида может потребоваться перемещение устройства на уровень корпоративного офиса).

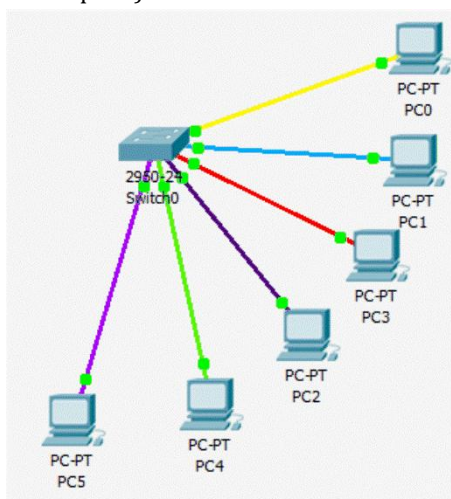


Рисунок 46 – Цветовая расцветка кабеля

На физическом плане также имеется возможность создания точки перегиба для устранения запутанного вида кабеля. Для создания точки перегиба кликните по кабелю и выберите пункт меню «Создать точку перегиба» (**Create bendPoint**). На одной линии можно создать любое количество точек перегиба (рисунок 47)

В дополнение точки перегиба позволяют объединить несколько кабелей в единую группу. Для создания группы совместите точку перегиба с другой точкой. Черный квадрат точки перегиба примет вид желтого квадрата как показано на рисунке 48.

Для удаления группировки используйте инструмент удаления из общей панели инструментов и кликните на групповой точке. Появившиеся

еся контекстное меню позволяет извлечь из группы одну точку или разгруппировать все сразу. При разгруппировке удаляется только объединение точек в группу, сами точки перегиба остаются без изменений.

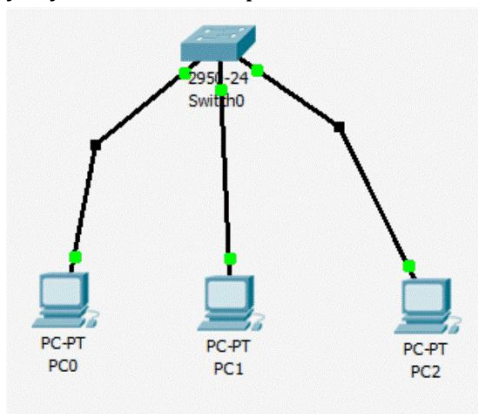


Рисунок 47 – Создание точек перегиба

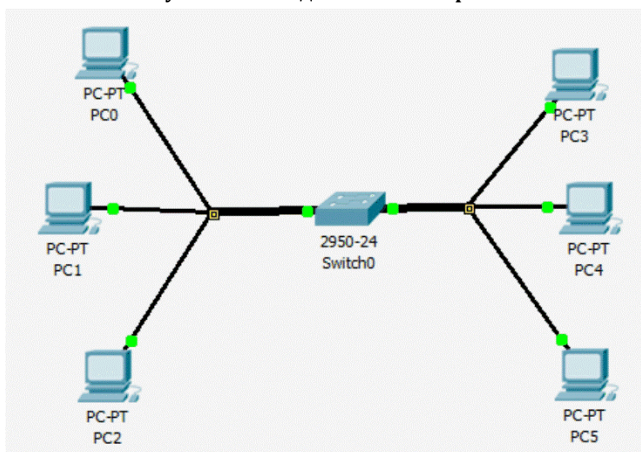


Рисунок 48 – Группировка точек перегиба

Кастомизация изображений устройств и фона

Несмотря на то, что Packet Tracer предлагает собственный набор изображений для каждого устройства, также возможно заменить их на пользовательские изображения. Для изменения изображений устройств кликните по устройству перейдите на вкладку «Физически вид» (**Physical**), а затем кликните по кнопке «Выбор фонового изображения логического плана» (**Customize Icon in Logical View**). Выберите файл

пользовательского изображения и произойдет изменение внешнего вида устройства на логическом плане (рисунок 49).

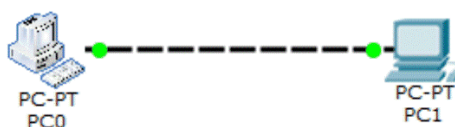


Рисунок 49 – Изменение стандартного изображения

Изменения изображения на физическом уровне становится видимым только при перемещении устройств за пределы телекоммуникационного шкафа.

Фоновое изображение логического и физических рабочих пространств также может быть кастомизировано. Для изменения фона логического плана кликните по кнопке «Выбрать фоновое изображение» (**Set Tiled Background**) и выберите файл изображения. Если выбранный рисунок меньше, чем рабочее пространство вы можете использовать опцию «Замостить фоновым изображением» (**Display Tiled Background Image**).

Для физического рабочего пространства фоновое изображение может быть установлено отдельно для междугородного уровня, города, офиса и телекоммуникационного шкафа.

Резюме

В этой главе мы изучили физическое рабочее пространство, что поможет вам задействовать множество новых возможностей при использовании беспроводных устройства. Кастомизация изображений и фона не только не только улучшает эстетику, но также помогает провести дифференциацию между устройствами, принадлежащими к разным организациям. В следующей главе, мы сфокусируемся больше на межсетевом взаимодействие Cisco-устройств, объяснив принципы IP-маршрутизации, работу статической маршрутизации и динамических протоколов. Режим имитации здесь очень пригодится для того, чтобы увидеть, как все это работает.

6 Настройка маршрутизации с помощью интерфейса командной строки CLI

Наконец-то мы добрались до важнейшей части сетевого взаимодействия – маршрутизации. Маршрутизация обеспечивает взаимодействие между множеством логических подсетей. Настройка маршрутизации с помощью интерфейса командной строки (CLI) Packet Tracer не отличается от конфигурирования реального оборудования. Вы также можете обнаружить в Packet Tracer графический интерфейс, предназначенные для настройки статической маршрутизации и динамической маршрутизации по протоколу RIP. В дополнение к этому, вы также можете наблюдать балансировку нагрузки, что позволит вам понять лучше принципы маршрутизации

Статическая маршрутизация

Статическая маршрутизация – простой метод, работающий в том или ином виде, представленный в большинстве сетей. В Packet Tracer статическая маршрутизация может быть настроена с использованием графического интерфейса. При этом методе конфигурирования мы вводим адрес сети назначения и шлюз, необходимый для достижения данной сети. Каждый маршрутизатор в сети должен знать способ достижения всех получателей в сети. При статической маршрутизации требуется немалая ручная работа. Так если один маршрутизатор добавляется (или удаляется) из сети, на всех оставшихся должно быть проведено ручное обновление этих изменений.

Настройка статической маршрутизации с помощью графического интерфейса

Эта возможность Packet Tracer оказывается очень кстати, если вы не знаете команд Cisco IOS. Для упражнения мы используем следующую топологию (рисунок 50).

В этой сети имеется четыре маршрутизатора, соединенных по кольцевой топологии без использования loopback-интерфейсов или подключения компьютеров. Поэтому здесь мы используем графический интерфейс и такая конфигурация будет иметь минимальное количество инструкций. Выполним следующие шаги.

1) Кликните по изображению маршрутизатора и перейдите на вкладку «Настройка» (**Config**). Далее выберите необходимый интерфейс и настройте IP-адрес. Затем включите интерфейс, выбрав опцию «Включено» (**On**), поставив флажок. В этом примере мы используем следующие IP-адреса, приведенные в таблице 2.

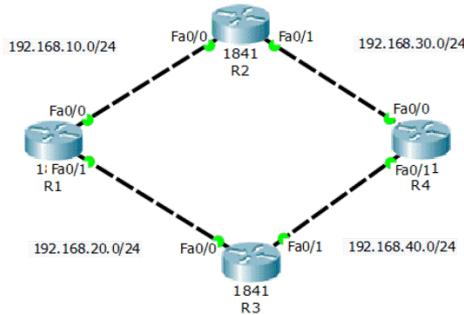


Рисунок 50 – Пример сети для настройки статической маршрутизации
Таблица 2 – Назначение IP-адресов маршрутизаторов

Router	Interface	IP Address
R1	FastEthernet0/0	192.168.10.1
	FastEthernet0/1	192.168.20.1
R2	FastEthernet0/0	192.168.10.2
	FastEthernet0/1	192.168.30.1
R3	FastEthernet0/0	192.168.20.2
	FastEthernet0/1	192.168.40.1
R4	FastEthernet0/0	192.168.30.2
	FastEthernet0/1	192.168.40.2

2) На этой же вкладке в секции «Маршрутизация» (**Routing**) выберите «Статическая маршрутизация» (**Static**), как показано на рисунке 51.

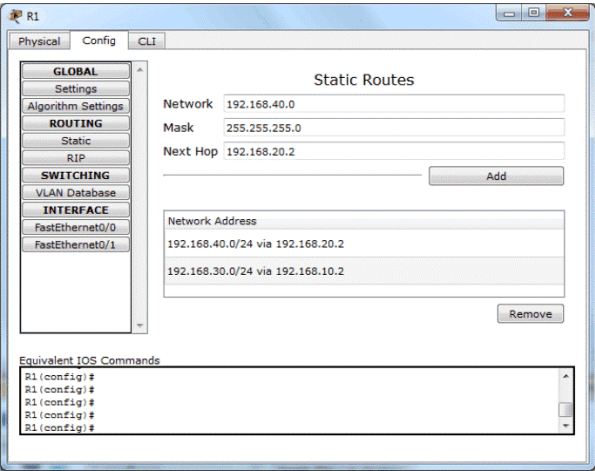


Рисунок 51 – Статическая маршрутизация
3) Настройка статической маршрутизации заключается в ручном вводе в таблицу маршрутизации всех маршрутов, которые не являются

непосредственно подключенными. Следующие установки будут использоваться для настройки статических маршрутов при помощи графического интерфейса.

Таблица 3 – Статические маршруты

Device	Network/Mask	Next Hop
R1	192.168.30.0/255.255.255.0	192.168.10.2
	192.168.40.0/255.255.255.0	192.168.20.2
R2	192.168.20.0 / 255.255.255.0	192.168.10.1
	192.168.4 0.0/255.255.255.0	192.168.30.2
R3	192.168.10.0/255.255.255.0	192.168.20.1
	192.168.30.0/255.255.255.0	192.168.40.2
R4	192.168.10.0/255.255.255.0	192.168.30.1
	192.168.20.0/255.255.255.0	192.168.40.1

4) Сейчас мы используем инструмент «Простой PDU» для проверки связи между всеми маршрутизаторами. При это рекомендуется использовать режим имитации для просмотра маршрута распространения пакетов.

5) Как посмотреть таблицу маршрутизации? Для этого также имеется графический инструмент «Проверка» (**Inspect**), расположенный на панели общих инструментов. Кликните по изображению лупы или нажмите клавишу *I*, а затем выберите маршрутизатор и кликните по нему. Таблица маршрутизации каждого маршрутизатора содержит четыре маршрута (рисунок 52).

Type	Network	Port	Next Hop IP	Metric
C	192.168.10.0/24	FastEthernet0/0	---	0/0
C	192.168.20.0/24	FastEthernet0/1	---	0/0
S	192.168.30.0/24	---	192.168.10.2	1/0
S	192.168.40.0/24	---	192.168.20.2	1/0

Рисунок 52 – Таблица маршрутизация (графический интерфейс)

Мы настроили только два статических маршрута, откуда в таблице маршрутизации еще два? Эти два маршрута связаны с непосредственно подключенными сетями.

В этой топологии будет использоваться только один определенный маршрут для достижения любой сети, несмотря на то, что имеются альтернативные маршруты к каждой сети, т. к. именно такую настройку статических маршрутов мы произвели. В дальнейшем мы изучим, как использовать более чем один маршрут (в раздел «Балансировка нагрузки»).

Настройка статической маршрутизации с помощью интерфейса командной строки CLI

Для настройки статического маршрута с помощью интерфейса командной строки воспользуемся тем же примером, что и в предыдущем

разделе. Процесс ввода команд рассмотрим только на одном устройстве маршрутизаторе R1). Необходимо ввести следующие команды.

1) Присвоить IP-адрес на интерфейсе каждого маршрутизатора, используя следующие команды.

```
R1(config)#interface FastEthernet0/0
R1(config-if)#ip address 192.168.10.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface FastEthernet0/1
R1(config-if)#ip address 192.168.20.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
```

2) Статический маршрут конфигурируется командой `ip route` со следующим синтаксисом.

```
R1(config)#ip route <Destination Prefix> <Destination prefix mask> <Gateway IP>
```

3) Для маршрутизатора R1 используются следующие команды:

```
R1(config)#ip route 192.168.30.0 255.255.255.0 192.168.10.2
R1(config)#ip route 192.168.40.0 255.255.255.0 192.168.20.2
```

При помощи инструмента «Простой PDU» проведем тест связности. Если вы увидите сообщение об ошибке, перейдите режим имитации и определите какой из маршрутизаторов некорректно настроен.

Динамическая маршрутизация

При изучении статической маршрутизации мы столкнулись с большим объемом ручной работы. При этом изменения в топологии сети также требует внесение изменений в настройки вручную. Динамические протоколы маршрутизации позволяют обеспечить автоматическое оповещение каждого маршрутизатора о существующих маршрутах.

Конфигурирование динамических протоколов маршрутизации несколько противоположно статической маршрутизации. Для этого мы разрешаем работу динамическое маршрутизации на нужных интерфейсах. Протоколы маршрутизации позволяют сформировать соседские отношения между маршрутизаторами и обмениваться непосредственно подключенными маршрутами и иными (принятыми) маршрутами. Таким образом, все маршрутизаторы обмениваются обновлениями друг с другом. Когда происходит изменение топологии, эти обновления также рассылаются маршрутизаторами, при этом определяются потери маршрутов.

Настройка протокола маршрутизации RIP с помощью графического интерфейса

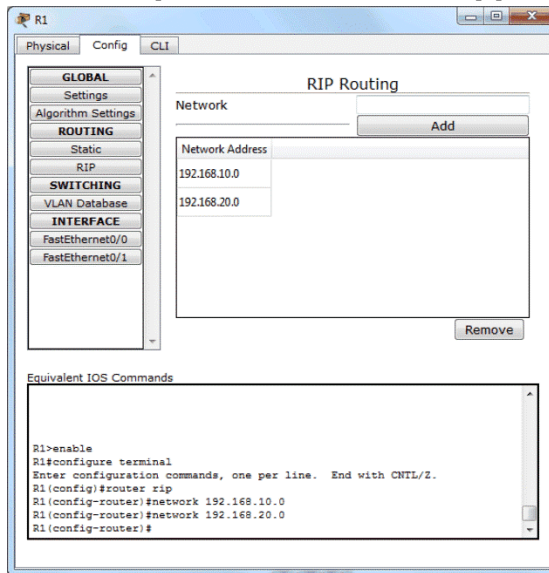
Packet Tracer предлагает графический интерфейс для настройки динамического протокола маршрутизации, называемого протоколом маршрутной информации **RIP (Routing Information Protocol)**. Эта опция несколько похожа на настройку статической маршрутизации. Здесь также имеется одно текстовое окно для ввода сетевого адреса непосредственно подключенной сети.

Можно предположить, что эта настройка похожа на конфигурирование статической маршрутизации, однако это не так. Если для настройки статической маршрутизации вводится маршрут к другим сетям, то для RIP же мы вводим сетевые IP-адреса своих же интерфейсов. Этим действием мы делаем два дела: запускаем на указанном интерфейсе протокол маршрутизации и разрешаем распространять информацию об данной сети.

Для настройки динамической маршрутизации RIP выполним следующие действия.

1) Создайте такую же топология, как и в прошлом примере. Присвойте интерфейсам маршрутизаторов те же самые IP-адреса с помощью вкладки «Настройка» (**Config**).

2) На этой же вкладке перейдите в секцию RIP. Настройка динамической маршрутизации достаточно проста: для каждого маршрутизатора требуется ввести только IP-адрес сети собственного интерфейса (рисунок 53).



**Рисунок 53 – Конфигурирование динамической маршрутизации
с помощью графического интерфейса**

3) Для каждого маршрутизатора необходимо ввести следующие сетевые IP-адреса:

Таблица 3 – Сетевые IP-адреса интерфейсов маршрутизаторов

Router	RIP Network
R1	192.168.10.0
	192.168.20.0
R2	192.168.10.0
	192.168.30.0
R3	192.168.20.0
	192.168.40.0
R4	192.168.30.0
	192.168.40.0

4) По настройки топологии, воспользуйтесь инструментом «Простой PDU» для проведения теста связности. Например, проверьте два несвязанных непосредственно маршрутизаторам (R1 и R4 или R2 и R3). Успешное прохождение свидетельствует о правильной настройке динамической маршрутизации на каждом маршрутизаторе.

5) Следующим шагом проверим, как работают динамические протоколы маршрутизации при изменениях в топологии. Для этого выберем инструмент «Удаление» (**Delete**) с общей панели инструментов и удалим связь между маршрутизаторами R1 и R2 (или R1 и R3). Используем имитационный режим и при помощи инструмента «Простой PDU» проведем тест связности. Вы обнаружите, что тест будет успешным, при этом пакеты проследуют альтернативным (более длинным) путем.

Если вы проделаете пункт 5 в статической маршрутизации, то обнаружите ошибку, т. к. для отработки потери соединения между маршрутизаторами мы не внесли вручную альтернативные маршруты для каждой сети в каждом маршрутизаторе. В этом и состоит большое преимущество динамической маршрутизации.

Настройка протокола маршрутизации RIP при помощи интерфейса командной строки CLI

Давайте настроим ту же топологию при помощи интерфейса командного строки CLI. Команды конфигурирования очень просты, как вы и могли заметить в окне «Эквивалентные IOS-команды» (**Equivalent IOS Commands**), когда работали с графическим интерфейсом. Для настройки динамической маршрутизации перейдем на вкладку **CLI** и выполним следующие шаги.

1) Присвоим IP-адреса интерфейсам маршрутизаторов точно такими же командами, как в случае примера настройки статической маршрутизации при помощи командной строки.

2) Затем вернитесь в режим глобальной конфигурации и оттуда перейдите в режим RIP-маршрутизатора, используя следующую команду:

```
R1(config)#router rip
```

3) Используйте команду `network` для указания IP-адреса сети. Для маршрутизатора R1, это будут следующие команды:

```
R1(config-router)#network 192.168.10.0
```

```
R1(config-router)#network 192.168.20.0
```

4) Аналогичным образом настройте оставшиеся маршрутизаторы. Затем используйте инструмент «Простой PDU» для проведения теста связности.

Таким образом, когда вы знаете как конфигурируется статическая и динамическая маршрутизация, можно перейти к подробному рассмотрению таблице маршрутизации.

Таблица маршрутизация

Таблица маршрутизация содержит список всех предпочтительных маршрутов, известных маршрутизатору. Существует два пути для просмотра таблицы маршрутизации. Первый предполагает использование инструмента «Проверка» (**Inspect**), другой – применение команды Cisco IOS `show ip route`. Вне зависимости от того, что вы выберете, вы увидите таблицу, содержащую некоторое количество столбцов и информацию, содержащуюся в них. Что конкретно в ней отображается, мы узнаем позже, ниже приводится сокращенный пример вывода команды:

```
R1#show ip route
C    192.168.10.0/24 is directly connected, FastEthernet0/0
C    192.168.20.0/24 is directly connected, FastEthernet0/1
R    192.168.30.0/24 [120/1] via 192.168.10.2, 00:00:13,
FastEthernet0/0
R    192.168.40.0/24 [120/1] via 192.168.20.2, 00:00:22,
FastEthernet0/1
```

Первая колонка описывает причину появления записи в таблице маршрутизации: C – непосредственно подключенная сеть, R – динамический протокол маршрутизации RIP.

Вторая колонка указывает сеть назначения.

Первое значение в квадратных скобках описывает административное расстояние **AD (administrative distance)**, указывающее приоритет протокола маршрутизации, второе – отображает значение метрики (**metric**) динамического протокола маршрутизации (для протокола RIP – хопы, количество маршрутизаторов на пути к сети назначения). В данном случае, административное расстояние для протокол RIP равно 120, для статического маршрута – 1.

Если маршрутизатор имеет два маршрута к одной и той же сети – статически и RIP, то будет использоваться статический маршрут, т. к. у него меньшее значение административного расстояния.

IP-адрес, записанный после слова *via*, является адресом шлюзом, т. е. следующим маршрутизатором на пути к сети назначения. Временная метка, записанная в конце динамического маршрута, называется таймер удержания (**Holddown timer**). Также в любом протоколе маршрутизации рассылка сообщений происходит с определенным интервалом (**Hello timer**). Для протокола RIP он составляет 30 с. Если в течении трех Hello-интервалов (180 с или Holddown timer) маршрутизатор не получает сообщений о маршруте, то такой маршрут удаляется из таблицы маршрутизации и происходит поиск альтернативного маршрута.

Последний столбец указывает на исходящий интерфейс самого маршрутизатора, с которого можно достичь шлюз.

Распределение нагрузки

В топологии, настройку которой мы рассматривает на протяжении этой главы, мы можем обнаружить, что каждый маршрутизатор имеет два пути для достижения каждой сети назначения. Неплохо бы посмотреть как маршрутизаторы используют альтернативные пути и производят распределение нагрузки при передачи трафика по ним.

Балансировка нагрузки в протоколе RIP

Вначале рассмотрим протокол RIP, потому что в этом случае нам и делать ничего не надо. Если альтернативные пути для достижения сетей назначения имеют одинаковые метрики, RIP автоматически осуществляет распределение нагрузки.

В примере мы будем использовать тип интерфейса, известный как *loopback* в качестве сети назначения. *Loopback* – виртуальный интерфейс, которые ведет себя как реальный интерфейс и использует IP-адрес.

В той же самой топологии добавим этот интерфейс на маршрутизаторе R4, руководствуясь следующими шагами.

1) К сожалению, это не удастся сделать с помощью графического интерфейса, поэтому воспользуемся вкладкой «Интерфейс командной строки» (**CLI**) и вводом следующих команд:

```
R4(config)#interface loopback 0  
R4(config-if)#ip address 192.168.100.1 255.255.255.0
```

2) На этом же маршрутизаторе необходимо запустить процесс маршрутизации на *loopback*-интерфейсе. Переходим в режим глобальной конфигурации и вводим сетевой IP-адрес *loopback*-интерфейса. Распространение маршрутной информации произойдет автоматически.

```
R4(config)#router rip
R4(router-if)#network 192.168.100.0
```

3) Затем для тестирования воспользуемся инструментом «Сложный PDU», установим временной интервал, равный 2 с.

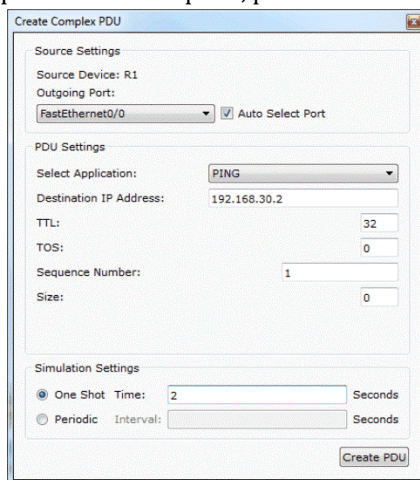


Рисунок 54 – Использование инструмента «Сложный PDU»

4) Переходим в имитационный режим, при этом вы обнаружите, что первый пакет проследует по пути **R1-R2-R4**, а следующий – **R1-R3-R4**!

Кроме того, также можно убедиться, что механизм распределения трафика работает, если взглянуть в таблицу маршрутизации.

```
Router>show ip route
R 192.168.30.0/24 [120/1] via 192.168.10.2, 00:00:12,
FastEthernet0/0
R 192.168.40.0/24 [120/1] via 192.168.20.2, 00:00:14,
FastEthernet0/1
R 192.168.100.0/24
[120/2] via 192.168.20.2, 00:00:08, FastEthernet0/1
[120/2] via 192.168.10.2, 00:00:08, FastEthernet0/0
```

В отображенной таблице маршрутизации оставлены только RIP-маршруты для лучшего понимания. Запись маршрута 192.168.100.0/24 имеет два шлюза, что говорит о том, что трафик к этой сети будет распределяться между ними.

Балансировка нагрузки для статических маршрутов

Статическая маршрутизация требует дополнительной настройки для балансировки нагрузки. Присваиваем IP-адреса для всех физических интерфейсов и loopback-интерфейс, как было указано ранее. Для настройки распределения нагрузки выполним следующие шаги.

1) На маршрутизаторах R2 и R3 конфигурируем маршрут к loopback-интерфейсу маршрутизатора R4.

```
R2(config)#ip route 192.168.100.0 255.255.255.0 192.168.30.2
```

```
R3(config)#ip route 192.168.100.0 255.255.255.0 192.168.40.2
```

2) На маршрутизаторе R1 мы настраиваем два маршрута к сети 192.168.100.0/24. Мы нуждаемся в том, чтобы сообщить маршрутизатору, что имеется 2 пути достижения loopback-интерфейса маршрутизатора R4. Для этого используем следующие команды.

```
R1(config)#ip route 192.168.100.0 255.255.255.0 192.168.10.2
```

```
R1(config)#ip route 192.168.100.0 255.255.255.0 192.168.20.2
```

3) Для проверки работоспособности механизма распределения при статической маршрутизации задействуем «Сложный PDU», как и в предыдущем разделе.

После настройки этой конфигурации при просмотре таблицы маршрутизации можно обнаружить два маршрута к сети 192.168.100.0/24, также как было и при RIP-маршрутизации.

Резюме

В этой главе мы увидели как настраивают статическую маршрутизацию и динамическую маршрутизация RIP в Cisco Packet Tracer. Теперь вы можете понять разницу между ними и увидеть и плюсы и минусы каждого из них. Мы также произвели настройку балансировки нагрузки как RIP и статической маршрутизации.

В следующей главе, мы будем говорить только об одном протоколе маршрутизации, который называется протокол внешнего шлюза **BGP (Border Gateway Protocol)**. Хотя это также протокол динамической маршрутизации, он отличается в значительной степени от других протоколов динамической маршрутизации.

7 Протокол внешнего шлюза BGP

Интернет представляет собой гигантскую сеть, собранную во едино из множества других сетей. Для того, чтобы изучить маршруты к другим сетям, в каждой сети работают протоколы маршрутизации. Такие протоколы как расширенный протокол маршрутизации внутреннего шлюза EIGRP (Enhanced Interior Gateway Routing Protocol), открытый протокол поиска первого кратчайшего маршрута OSPF (Open Shortest Path First), и протокол маршрутной информации RIP (Routing Information Protocol) хорошо работают для большинства сетей, но они не подходят для такой составной сети как Интернет из-за плохой масштабируемости и не достаточного уровня административного разграничения. Протокол внешнего шлюза BGP (Border Gateway Protocol) используется интернет-провайдерами ISP (Internet Service Provider) и большими предприятиями для оповещения о существующих маршрутах между ними.

В этой главе мы будем изучать протокол BGP и его характеристики в сравнении с другими протоколами. Мы также изучим команды Cisco IOS, используемые при конфигурировании BGP, и научимся настраивать его.

Что такое BGP?

BGP очень мощный протокол маршрутизации, используемый для обмена маршрутной информацией между множеством автономных зон (Autonomous Systems, AS). Это определение влечет за собой еще один вопрос: что такое автономная зона. Автономная зона – набор IP-префиксов (читай, IP-сетей), что находятся под единым административным управлением. Сетевым оператором, управляющим автономной зоной может быть предприятие или интернет-провайдер.

Каждая автономная зона имеет номер, называемый номером автономной зоны **ASN (Autonomous System Number)**. Открытые номера автономных зон присваиваются региональными интернет-регистраторами **RIRs (Regional Internet Registries)**, которым это право делегируется Администрацией адресного пространства Интернет **IANA (Internet Assigned Numbers Authority)**.

Настройка BGP в большой степени зависит от того, как организация подключается к интернет-провайдеру. Есть 4 возможных типа подключения.

1) Одиночное подключение (**Single homed**). Это простейший вариант дизайна, предполагающий один канал ко одному интернет-провайдеру (рисунок 55). Такое подключение не обеспечивает резервирование или отказоустойчивость.

2) Двойное подключение (**Dual homed**). Такая схема подключения также предполагает использование одного провайдера, но имеет два или более каналов к нему (рисунок 56). Это обеспечивает некоторое повышение надежности в случае проблем с одиночным каналом.

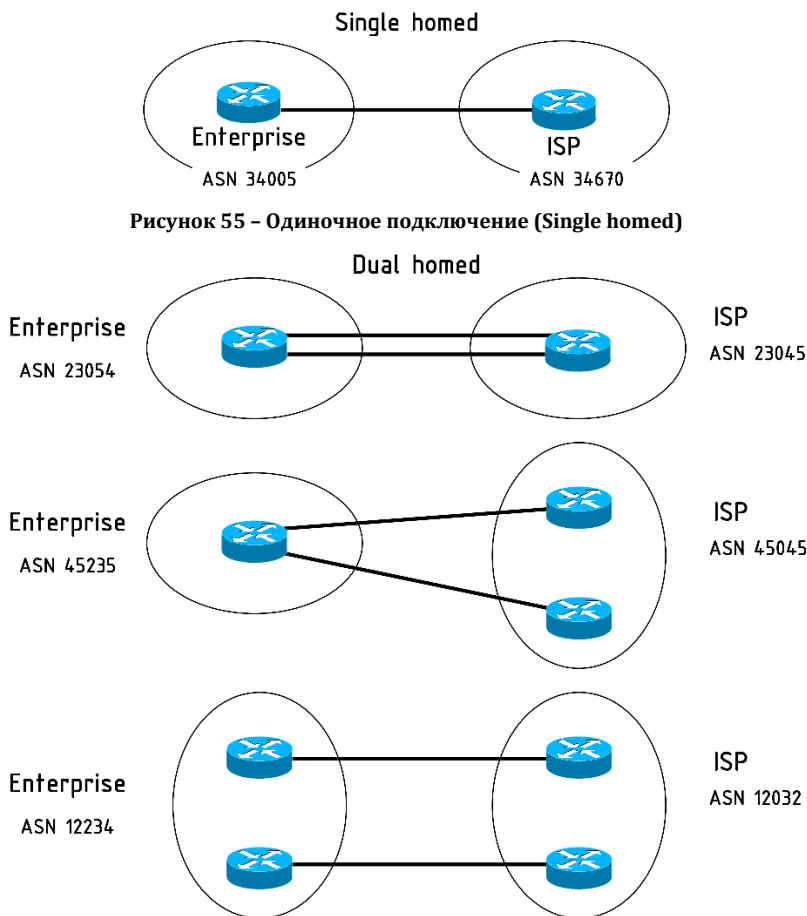


Рисунок 56 – Варианты двойного подключения (Dual homed)

3) Одиночное многосетевое подключения (**Single multihomed**). В этом случае имеется несколько интернет-провайдеров, к каждому подключается по одному каналу связи (рисунок 57).

4) Двойное многосетевое подключение (**Dual mutihomed**). Такая схема подключения обеспечивает наибольший уровень надежности и

доступности. В этом случае имеет два и более провайдеров, и к каждому подключается по два и более каналов связи (рисунок 58).

Single Multihomed

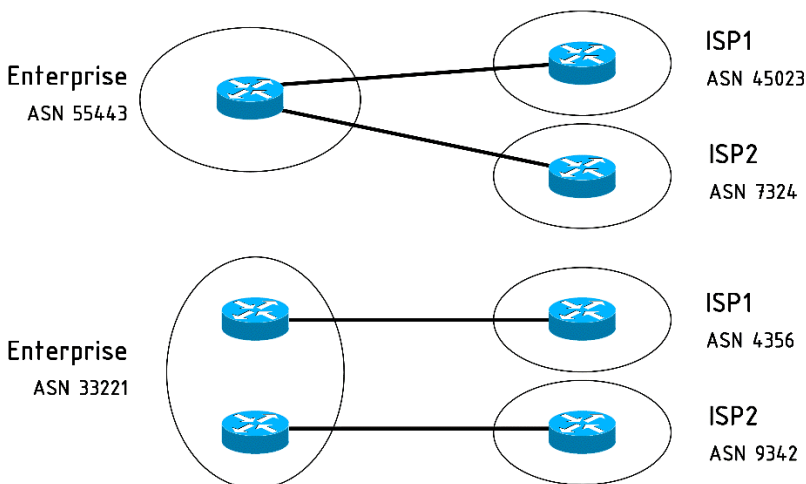


Рисунок 57 – Варианты одиночного многосетевое подключения (Single multihomed)

Dual Multihomed

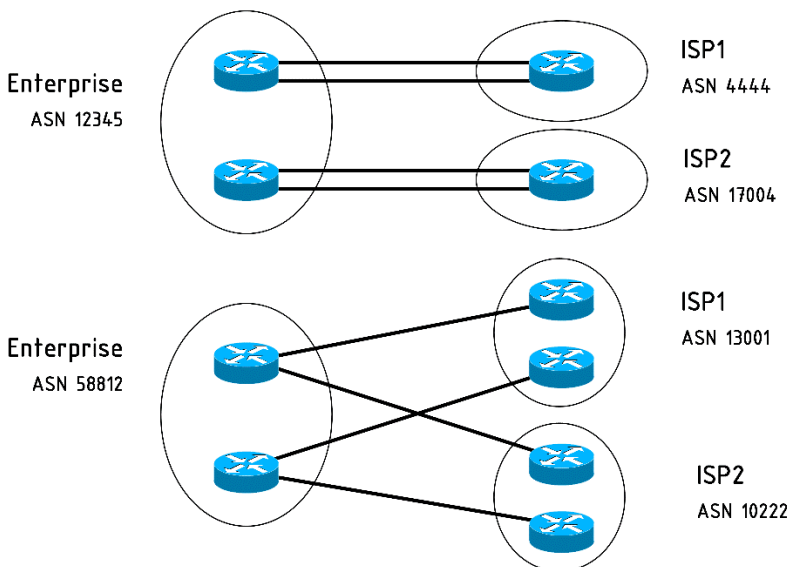


Рисунок 58 – Варианты двойного многосетевое подключения (Dual multihomed)

BGP может не соответствовать предложенным вариантам топологий. В некоторых случаях одиночного подключения предпочтительно иметь статический маршрут по умолчанию к провайдеру, и другой статический маршрут на стороне провайдера к сети предприятия. Однако реализация BGP в варианте многосетевого подключения гарантирует более эффективную маршрутизацию.

Существуют два типа BGP:

- 1) внешний BGP (External BGP, eBGP);
- 2) внутренний BGP (Internal BGP, iBGP).

Внешний BGP

Этот тип BGP используется для обмена маршрутами между автономными зонами. Административное расстояние для eBGP равно 20. По умолчанию при отправлении пакетов обновлений в eBGP время жизни TTL (Time-to-Live) устанавливается в 1, т. е. их получит только непосредственно подключенный BGP-маршрутизатор. Такое поведение можно изменить при помощи соответствующих команд. Маршрутизатор eBGP объявляет все действительные маршруты, полученные от eBGP- и iBGP-маршрутизаторов. Когда eBGP-сосед объявляет маршрут, то в поле следующего маршрутизатора объявляемого маршрута указывает собственный адрес.

Внутренний BGP

Этот тип BGP используется для обмена маршрутами внутри автономной зоны. Административное расстояние iBGP равно 200. Обновления в iBGP не имеют ограничение по TTL-значению. Маршрутизаторы iBGP не объявляют маршруты, изученные от других iBGP-маршрутизаторов. Этот механизм защищает от появления маршрутных петель внутри автономной зоны. В поле адреса следующего маршрутизатора в маршрутных объявлениях iBGP-маршрутизатор оставляет без изменения. Такое поведение также можно изменить с помощью соответствующих команд.

Cisco Packet Tracer версии 5.3.3 не поддерживает iBGP.

BGP как протокол динамической маршрутизации

И хотя BGP работает подобно другим протоколам динамической маршрутизации, имеются некоторые отличия. Внутренние протоколы маршрутизации **IGP (Interior Gateway Protocols)**, как RIP, OSPF и EIGRP, имеют развитый интерфейс. В объявлении сети при настройке протокола маршрутизации указывается сетевой IP-адрес, и те интерфейсы,

чий IP-адреса попадают в диапазон объявленной сети, участвуют в процессе маршрутных объявлений. Через эти интерфейсы происходит широковещательная или групповая рассылка маршрутных сообщений. Для того, чтобы это работало, требуется непосредственное соединения двух соседних маршрутизаторов, с запущенными на них процессами IGP-протоколов. В качестве метрик, на основе которых IGP-протоколы определяют оптимальный путь, используются количество хопов, полоса пропускания, временная задержка и т. д.

С другой стороны, BGP не использует концепции интерфейсов, т. к. весь маршрутизатор соответствует автономной зоне. Соседи BGP не определяются автоматически и должны быть назначены вручную при помощи команды `neighbor`. После этого BGP-сообщения пересылаются однонаправленными пакетами. BGP работает через TCP-протокол и прослушивает 179 порт. Соседи необязательно должны быть непосредственно подключены и могут быть расположены на расстоянии нескольких хопов. При надо помнить, что по умолчанию значение времени жизни TTL для GP-сообщения равно 1. И если точка обмена не подключена непосредственно, то это значение должно быть скорректировано в сторону увеличения. Принципы выбора оптимального маршрута для BGP отличаются от IGP-протоколов. Используются различные атрибуты **PA (path attributes)**, такие как достижимость следующего маршрутизатора (**next hop reachability**), вес маршрута (**weight**) и путь к автономной зоне (**AS_PATH** – число автономных зон на пути к сети назначения). Кроме того, BGP предназначен для обработки сотен тысяч IP-маршрутов, которые потребляют значительное количество ресурсов, если работают через IGP – протоколы.

Настройка BGP в Packet Tracer

В начале рассмотрим команды, используемые в BGP:

```
router bgp <asn>
```

Например,

```
R1(config)# router bgp 120
```

Эта команда включает BGP-процесс на маршрутизаторе и переводит маршрутизатор в режим настройки маршрутизации. Номер автономной зоны ASN может принимать значения в диапазоне от 1 до 65535. BGP-процесс требует присвоения идентификатора маршрутизатора (router ID). По умолчанию BGP использует методы выбора идентификатора маршрутизатора в следующем порядке приоритета:

- 1) Настроенный в ручную. Идентификатор конфигурируется при помощи команды `bgp router-id` в режиме настройки маршрутизации.

2) Наибольшее значение loopback-интерфейса. В этом случае идентификатором маршрутизатора становится наивысший IP-адрес любого доступного loopback-интерфейса при инициализации BGP-процесса.

3) Наибольшее значение другого интерфейса. Идентификатор маршрутизатор выбирается наивысший IP-адрес, настроенный на любом доступном интерфейсе, кроме loopback-интерфейса при инициализации BGP-процесса.

Идентификатор маршрутизатора можно задать явно следующей командой:

```
bgp router-id X.X.X.X
```

Например, мы используем следующую команду для назначения идентификатора маршрутизатора:

```
R1(config-router)#bgp router-id 1.1.1.1
```

Для настройки BGP-соседа воспользуемся следующей командой:

```
R1(config-router)#neighbor X.X.X.X remote-as <asn>
```

Например:

```
R1(config-router)#neighbor 10.0.0.2 remote-as 130
```

В данном примере значение номера автономной зоны введенное после опции `remote-as` должно соответствовать автономной зоны, подключенной к соседнему маршрутизатору. Здесь имеется различие между внешним (eBGP) и внутренним (iBGP) протоколом.

Для внешнего BGP-протокола мы воспользуемся следующими командами:

```
R1(config)#router bgp 120
```

```
R1(config-router)#neighbor 10.0.0.2 remote-as 130
```

Для внутреннего BGP-протокола мы командами примут следующий вид:

```
R1(config)#router bgp 120
```

```
R1(config-router)#neighbor 192.168.1.20 remote-as 120
```

Как упоминалось ранее, при обмене маршрутной информацией внутри автономной зоны внутренний BGP-протокол не изменяет поле следующего маршрутизатора. Этот может быть проблемой, т. к. может быть не доступна редистрибуция через IGP-протоколы, т. к. эти протоколы будут отклонять такие маршруты из-за неверно указанного (с точки зрения IGP-протоколов) адреса следующего маршрутизатора. Следующая команда устанавливает свой собственный IP-адрес в качестве адреса следующего маршрутизатора:

```
R1(config-router)#neighbor X.X.X.X next-hop-self
```

BGP-протокол также имеет команду `network`. Она используется для указания специфического маршрута, объявляемого через протокол BGP, при этом такой маршрут должен существовать в таблице маршрутизации.

```
R1 (config-router) #network 10.20.20.0 mask 255.255.255.0
```

При указании только классового маршрута опция `mask` может быть опущена.

Полный набор команд BGP-протокола не поддерживается в Packet Tracer, так что дальнейшие примеры мы рассмотрим с использованием указанных ранее команд.

Для упражнения мы будем использовать одиночную многосетевую топологию (рисунок 59), т. к. Packet Tracer не поддерживает iBGP.

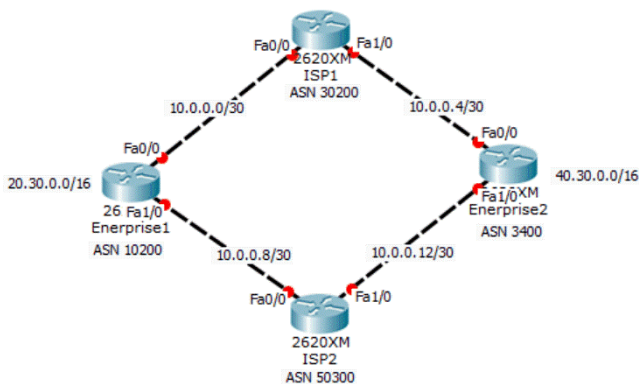


Рисунок 59 – Пример для настройки BGP в Packet Tracer

В данной сети имеет 4 маршрутизатора – два из них принадлежат разным предприятиям, а два – различным Интернет-провайдерам. У маршрутизаторы предприятий имеются loopback-интерфейсы с настроенными IP-адреса. Это продемонстрирует как появляются маршруты, изученные через BGP, в таблице маршрутизации.

В ниже перечислены (таблица 4)

Таблица 4 – IP-адреса интерфейсов маршрутизаторов

Устройство	Интерфейс	IP-адрес	Маска
Enterprise1	Loopback0	20.30.0.1	255.255.0.0
	FastEthernet0/0	10.0.0.1	255.255.255.252
	FastEthernet1/0	10.0.0.9	255.255.255.252
Enterprise2	Loopback0	40.30.0.1	255.255.0.0
	FastEthernet0/0	10.0.0.5	255.255.255.252
	FastEthernet1/0	10.0.0.13	255.255.255.252
ISP1	FastEthernet0/0	10.0.0.2	255.255.255.252
	FastEthernet1/0	10.0.0.6	255.255.255.252
ISP2	FastEthernet0/0	10.0.0.10	255.255.255.252
	FastEthernet1/0	10.0.0.14	255.255.255.252

Для настройки BGP-протокола в данной топологии выполним следующие шаги.

1) Начнем настройку с производственных маршрутизаторов:

Packet Tracer Network Simulator – 2016

```
Enterprise1(config)#router bgp 10200
Enterprise1(config-router)#bgp router-id 0.0.0.1
Enterprise1(config-router)#neighbor 10.0.0.2 remote-as 30200
Enterprise1(config-router)#neighbor 10.0.0.10 remote-as 50300
Enterprise1(config-router)#network 20.30.0.0 mask 255.255.0.0

Enterprise2(config)#router bgp 3400
Enterprise2(config-router)#bgp router-id 0.0.0.2
Enterprise2(config-router)#neighbor 10.0.0.6 remote-as 30200
Enterprise2(config-router)#neighbor 10.0.0.14 remote-as
50300
Enterprise2(config-router)#network 40.30.0.0 mask
255.255.0.0
```

2) Затем настроим маршрутизаторы интернет-провайдеров:

```
ISP1(config)#router bgp 30200
ISP1(config-router)#bgp router-id 1.1.1.1
ISP1(config-router)#neighbor 10.0.0.1 remote-as 10200
ISP1(config-router)#neighbor 10.0.0.5 remote-as 3400

ISP2(config)#router bgp 50300
ISP2(config-router)#bgp router-id 2.2.2.2
ISP2(config-router)#neighbor 10.0.0.9 remote-as 10200
ISP2(config-router)#neighbor 10.0.0.13 remote-as 3400
```

3) При правильной настройке появятся консольные сообщения об установлении соседских отношений

```
%BGP-5-ADJCHANGE: neighbor 10.0.0.9 Up
%BGP-5-ADJCHANGE: neighbor 10.0.0.13 Up
```

4) Сейчас сделаем попытку пинга loopback-интерфейса маршрутизатора Enterprise2 от маршрутизатора Enterprise1.

```
Enterprise1>ping 40.30.0.1
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 40.30.0.1, timeout is 2
seconds:
```

```
.....
```

```
Success rate is 0 percent (0/5)
```

5) Мы видим, что попытка теста связности оказалась неудачной. Так происходит потому, что пакет ICMP-запроса в качестве отправителя используется адрес 10.0.0.1, так, что когда пакет принимается маршрутизатором Enterprise2, он не может послать ICMP-ответ, т. к. не имеет маршрута к сети 10.0.0.0/30. Для достижения указанной сети loopback-интерфейса Enterprise1 воспользуемся расширенной версией утилиты ping, в которой можно явным образом указать исходящий интерфейс.

```

Enterprisel#ping
Protocol [ip]:
Target IP address: 40.30.0.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 20.30.0.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 40.30.0.1, timeout is 2
seconds:
Packet sent with a source address of 20.30.0.1
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
0/0/1 ms 6)

```

6) Таким образом мы успешно настроили eBGP. Теперь посмотрим BGP-маршруты таблицы маршрутизации.

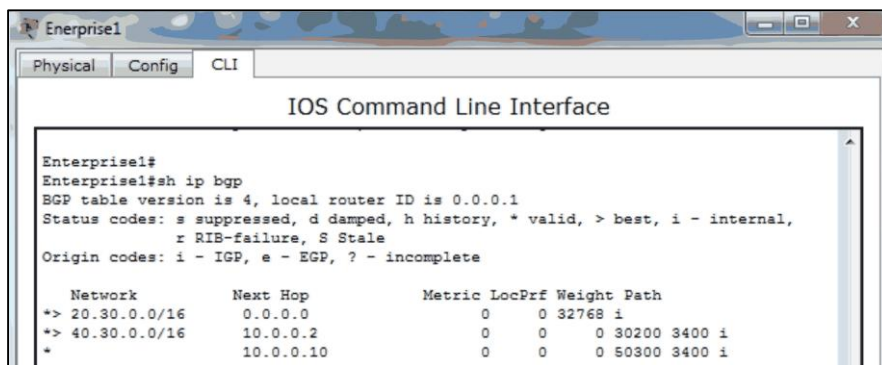


Рисунок 60 – Результат применение команды sh ip bgp

Резюме

В этой главе мы изучили принципы дизайна отличные от ранее изученных, которые используются для подключения к Интернет. Затем мы увидели широкое использование протокола маршрутизации BGP, его характеристики в сравнении с внутренними протоколами IGP и принципы

его настройки. К сожалению, Packet Tracer не поддерживает iBGP, но с ним можно познакомиться при работе на реальном оборудовании или при использовании симулятор **dynamips**.

В следующей главе, мы изучим о последней забаве сетевиков – IPv6. Мы начнем с изучения как присваиваются IPv6-адреса, затем продолжим настройку маршрутизации. И, наконец, мы узнаем о совместной работе IPv4 и IPv6 в сети.

8 IPv6 в Packet Tracer

Протокол IPv4 предполагает наличие свыше 4,3 млрд адресов, что кажется невероятно большим числом. Однако потребовалось всего лишь два десятилетия, чтобы они закончились. IPv6 – ожидаемый спаситель, имеет формат адреса в размере 128 бит (16 байт). Packet Tracer поддерживает многие возможности IPv6. Мы начнем изучение IPv6 с присвоения IP-адресов различным устройствам и настройки маршрутизации между ними. В конце главы мы создадим IPv6 взаимодействие через устройства с IPv4.

Присвоение IPv6-адресов

Начиная с шестой версии Packet Tracer, инструмент «Конфигурация IP» (**IP Configuration**), расположенная на вкладке «Рабочий стол» пользовательских устройств, имеет опции для ввода данных IPv6-адреса. Давайте создадим простую топологию из двух ПК и маршрутизатора, подключенных к коммутатору (рисунок 61).

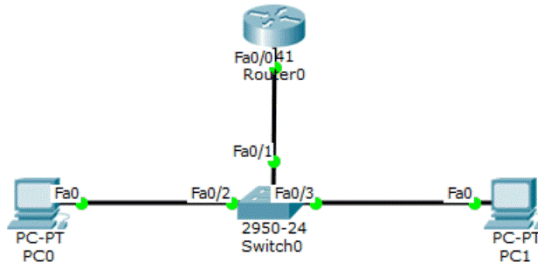


Рисунок 61 – Пример для назначения IPv6-адресов

Имеет три варианта присвоения IPv6-адресов, и мы рассмотрим каждый по отдельности.

Автоконфигурация (Autoconfiguration)

Автоконфигурация предполагает минимум настроек, но делает трудным запоминание IPv6-адресов. Этот метод использует MAC-адрес устройства для создания IPv6-адреса с префиксом FE80::: Проделаем следующие шаги по назначению IPv6-адресов с использованием автоконфигурацией.

1) Начнем с настройки маршрутизатора. Входим в режим глобальной конфигурации и разрешим использование IPv6 на интерфейсе.

```

R0(config)#interface FastEthernet0/0
R0(config-if)#ipv6 enable
  
```

2) Следующим шагом мы настроим локальный канальный и глобальный уникальный адрес для этого интерфейса. Мы будем использовать формат eui-64 для сокращения количества настроек.

```
R0(config-if)#ipv6 address autoconfig
R0(config-if)#ipv6 add 2000::/64 eui-64
R0(config-if)#no shutdown
```

3) Проверим, что этому интерфейсу назначены два IPv6-адреса.

```
R0#sh ipv6 interface brief
FastEthernet0/0 [up/up]
FE80::2D0:58FF:FE65:E701
2000::2D0:58FF:FE65:E701
```

4) Указанные IPv6-адреса могут быть не похожи на ваши, т. к. они зависят от конкретного MAC-адреса. Разрешим маршрутизацию, чтобы этот маршрутизатор мог стать шлюзом по умолчанию на других устройствах.

```
R0(config)#ipv6 unicast-routing
```

5) Настройка маршрутизатора окончена, переходим к настройке ПК. На вкладке «Рабочий стол» (**Desktop**), открываем инструмент «Конфигурация IP» (IP Configuration) и в секции «Настройка IPv6» (**IPv6 Configuration**) выбираем опцию «Автоконфигурация» (**Autocoffiguration**). IPv6-адрес и шлюз по умолчанию будут автоматически освоены (рисунок 62).

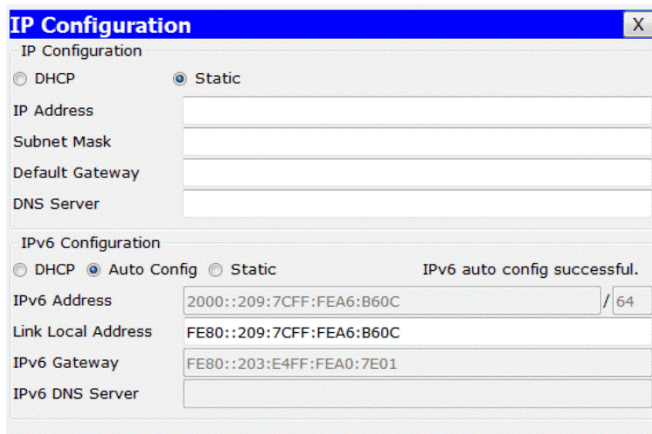


Рисунок 62 – Автоконфигурация IPv6-адреса на ПК0

6) Используйте инструмент «Простой PDU» (**Simple PDU**) для проведения теста связности. Мы увидим ICMPv6-пакеты перемещающиеся между узлами. Для просмотра IPv6-адресов на ПК используйте утилиту командной строки `ipv6config`.

Статический IPv6

IPv6-адрес может быть назначен статически на всех устройствах. Используем ту же топологию, что и в предыдущем примере. Прделаем следующие шаги для статического назначения IPv6.

1) Начнем с присвоения статического IPv6-адреса маршрутизатору.

```
R0(config)#interface fastethernet0/0
R0(config-if)#ipv6 enable
R0(config-if)#ipv6 address 2000::1/64
R0(config-if)#no shutdown
```

2) Переходим на вкладку «Рабочий стол» (**Desktop**), открываем инструмент «Конфигурация IP» (**IP Configuration**) и вводим IPv6-адрес с тем же самым префиксом, например 2000::10/64 или 2000::20/64.

3) Проведем тест связности с использование инструмента «Простой PDU». Убедимся, что оба метода (автоконфигурация и статическое назначение адреса) прекрасно работают, воспользовавшись просмотром таблицы IPv6-соседей, которая соответствует ARP-таблицы для IPv4.

```
R0#sh ipv6 neighbor
IPv6 Address    Age    Link-layer Addr    State    Interface
2000::2         0      00E0.A39E.05C4     REACH    Fa0/0
2000::3         0      0001.43B9.0268     REACH    Fa0/0
```

Сейчас, когда мы имеем сконфигурированные IPv6-адреса в простой сети, давайте добавим еще одну простую сеть и настроим маршрутизацию между ними.

IPv6 статическая и динамическая маршрутизации

Как и IPv4, так и IPv6 также поддерживает оба типа маршрутизации: статическую и динамическую. Команды настройки статической IPv6-маршрутизации аналогичны IPv4-настройке.

Статическая маршрутизация

Модифицируем предыдущую топологию, добавив в схему маршрутизатор, коммутатор и два ПК, и таким образом, создадим разделенную сеть (рисунок 63).

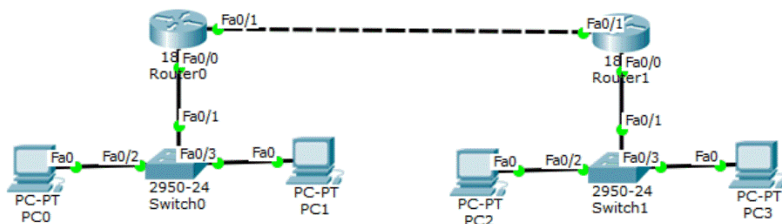


Рисунок 63 – Пример сети для поддержки IPv6 статической маршрутизации

В первой подсети мы будем использовать сеть 2000:1::/64, во второй – сеть 2000:2::/64. Интерфейсы в канале между маршрутизаторами получат адреса 2001::10/64 и 2001::20/64.

В таблице 5 приведено описание топологии для нашего примера.

Таблица 5 – IPv6-адреса примера с статической маршрутизацией

Устройство	Интерфейс	IPv6-адрес
R0	FastEthernet0/0	2000:1::1/64
	FastEthernet0/1	2001::10/64
PC0	FastEthernet	2000:1::2/64
PC1	FastEthernet	2000:1::3/64
R1	FastEthernet0/0	2000:2::1/64
	FastEthernet0/1	2001::20/64
PC2	FastEthernet	2000:2::2/64
PC3	FastEthernet	2000:2::3/64

После настройки необходимых IPv6-адресов и шлюзов по умолчанию, откроем вкладку **CLI** маршрутизатора R0 и введите следующие команды для настройки статической маршрутизации.

```
R0(config)#ipv6 unicast-routing
R0(config)#ipv6 route 2000:2::/64 2001::20
```

Затем откройте вкладку **CLI** маршрутизатора R1 и настройте статическую маршрутизацию на нем.

```
R1(config)#ipv6 unicast-routing
R1(config)#ipv6 route 2000:1::/64 2001::10
```

Воспользовавшись инструментом «Простой PDU», проведем тест связности. Можно также использовать команду `tracert` на ПК для того, чтобы отследить путь прохождения пакетов.

```
PC>tracert 2000:2::3
Tracing route to 2000:2::3 over a maximum of 30 hops:
 1 63 ms 63 ms 47 ms 2000:1::1
 2 94 ms 78 ms 94 ms 2001::20
 3 156 ms 109 ms 129 ms 2000:2::3
Trace complete.
```

Динамическая маршрутизация

Packet Tracer также предоставляет работу с некоторыми протоколами маршрутизации с поддержкой IPv6: RIPv6 (RIPng), EIGRP и OSPF. В данном разделе мы настроим RIPv6. Заметим, что название RIPv6 не предполагает 6 версии протокола маршрутной информации RIP, а лишь говорит о поддержке IPv6.

Для упражнения мы будем использовать следующую топологию (рисунок 64). Детали присвоения IPv6-адресов представлены в таблице 6.

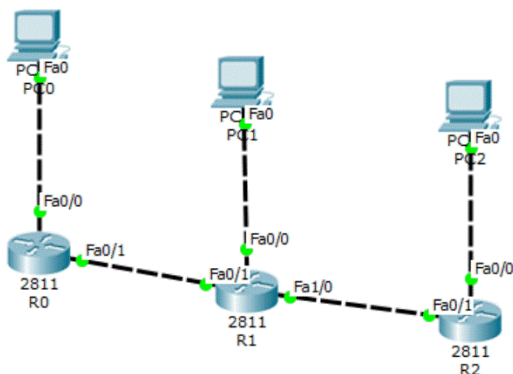


Рисунок 64 – Пример сети с поддержкой IPv6 динамической маршрутизации

Таблица 6 – IPv6-адреса примера с динамической маршрутизацией

Устройство	Интерфейс	IPv6-адрес
R0	FastEthernet0/0	2000:1::1/64
	FastEthernet0/1	2001:1::1/64
PC0	FastEthernet	2000:1::2/64
	FastEthernet0/0	2000:2::1/64
	FastEthernet0/1	2001:2::2/64
R1	FastEthernet0/0	2000:2::1/64
	FastEthernet1/0	2002:2::2/64
PC1	FastEthernet	2000:2::2/64
R2	FastEthernet0/0	2000:3::1/64
	FastEthernet0/1	2002:1::1/64
PC2	FastEthernet	2000:3::2/64

Мы будем настраивать протокол динамической маршрутизации сначала на одном маршрутизаторе, а затем такими же командами, но с своими адресами на других.

```

R0(config)# ipv6 unicast-routing
R0(config)# interface FastEthernet0/0
R0(config-if)# ipv6 address 2000:1::1/64
R0(config-if)# ipv6 rip Net1 enable
R0(config-if)# ipv6 enable
R0(config-if)# interface FastEthernet0/1
R0(config-if)# ipv6 address 2001:1::1/64
R0(config-if)# ipv6 rip Net1 enable
R0(config-if)# ipv6 enable

```

Команда `ipv6 rip` используется для разрешения RIP- маршрутизации на выбранном интерфейсе. Введя команду `ipv6 rip Net1 enable` на интерфейсе `fa0/1` запускаем процесс PIRv6. Вместо названия для RIP-процесса `Net1` можно использовать любое имя.

После окончания процесса конфигурирования использует обычный инструмент теста связности («Простой PDU»). Для просмотра базы данных RIP предназначены следующие команды.

```
R1#sh ipv6 rip database
RIP process "Net1" local RIB
2000:2::/64, metric 2, installed
FastEthernet0/1/FE80::201:97FF:FE87:E5A9, expires in 173 sec
2000:3::/64, metric 3, installed
FastEthernet0/1/FE80::201:97FF:FE87:E5A9, expires in 173 sec
2001::/64, metric 2
FastEthernet0/1/FE80::201:97FF:FE87:E5A9, expires in 173 sec
2001:1::/64, metric 2, installed
FastEthernet0/1/FE80::201:97FF:FE87:E5A9, expires in 173 sec
RIP process "LINK" local RIB
```

Проверим маршрут продвижения пакетов на ПК0

```
PC>tracert 2000:3::2
Tracing route to 2000:3::2 over a maximum of 30 hops:
 1 31 ms 32 ms 31 ms 2000:1::1
 2 50 ms 50 ms 63 ms 2001::20
 3 94 ms 94 ms 94 ms 2001:1::20
 4 125 ms 109 ms 125 ms 2000:3::2
Trace complete
```

Совместное использование IPv4 и IPv6

В этой секции мы увидим, как обеспечить взаимодействие хостов, настроенный на использование IPv6, через устройства, работающие только с IPv4. Существует несколько методов обеспечивающие такое взаимодействие. Здесь же мы обсудим IPv6-туннелирование через IPv4-сеть при помощи общей инкапсуляции маршрутов **GRE (Generic Routing Encapsulation)**.

GRE является методом, при котором IPv6-пакеты инкапсулируются в IPv4-пакеты и в таком виде транспортируются через IPv4-сеть. На принимающей стороне происходит деинкапсуляция таких пакетов и хосту-получателю отправляются только IPv6-пакеты В качестве упражнения мы будем использовать следующую топологию (рисунок 65).

Для обеспечения маршрутизации пакетов, мы настроим протокол EIGRP на IPV4-интерфейсах всех трех маршрутизаторов и сконфигурируем статическую маршрутизацию на маршрутизаторах R2 и R3. Вначале настроим маршрутизатор R1, который будет поддерживать IPv4.

```
R1(config)#int fa0/0
R1(config-if)#no shutdown
R1(config-if)#ip add 10.0.0.1 255.255.255.0
R1(config)#int fa0/1
```

```

R1(config-if)#no shutdown
R1(config-if)#ip add 10.2.0.1 255.255.255.0
R1(config)#router eigrp 1
R1(config-router)#network 10.0.0.0
R1(config-router)#no auto-summary

```

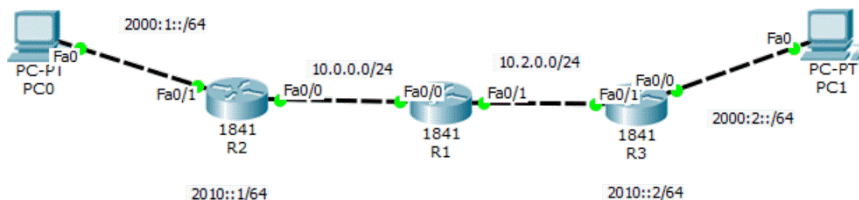


Рисунок 65 – Пример для обеспечения GRE-инкапсуляции

Затем переходим к маршрутизатору R2, настраиваем его с одновременной поддержкой как IPv4 и IPv6-адресов и соответствующих типов маршрутизации.

```

R2(config)#ipv6 unicast-routing
R2(config-router)#int fa0/0
R2(config-if)#ip add 10.0.0.2 255.255.255.0
R2(config-if)#no shutdown
R2(config)#int fa0/1
R2(config-if)#no shutdown
R2(config-if)#ipv6 add 2000:1::1/64
R2(config)#router eigrp 1
R2(config-router)#network 10.0.0.0

```

Тоже самое делаем с маршрутизатором R3.

```

R3(config)#ipv6 unicast-routing
R3(config)#int fa0/0
R3(config-if)#no shutdown
R3(config-if)#ipv6 add 2000:2::1/64
R3(config)#int fa0/1
R3(config-if)#no shutdown
R3(config-if)#ip add 10.2.0.2 255.255.255.0
R3(config)#router eigrp 1
R3(config-router)#network 10.0.0.0 0.0.0.255

```

На маршрутизаторе R2 создаем туннелирование с помощью следующих команд.

```

R2(config)#int tunnel 0
R2(config-if)#tunnel source f0/0
R2(config-if)#tunnel destination 10.2.0.2
R2(config-if)#tunnel mode ipv6ip
R2(config-if)#ipv6 address 2010::1/64

```


Заметим, что адресом назначения является IPv4-адрес интерфейса fa0/0 маршрутизатора R3. Завершаем создание туннеля на маршрутизаторе R3.

```
R3(config)#int tunnel 0
R3(config-if)#tunnel source f0/1
R3(config-if)#tunnel destination 10.0.0.2
R3(config-if)#tunnel mode ipv6ip
R3(config-if)#ipv6 address 2010::2/64
```

На крайних маршрутизаторах настроим статический IPv6-маршрут с префиксами 2000:1::/64 и 2000:2::/64.

Используем инструмент «Простой PDU» для проведения теста связности между ПК0 и ПК1. Для определения пути следования пакетов воспользуемся утилитой `tracert`.

```
PC>tracert 2000:2::2
Tracing route to 2000:2::2 over a maximum of 30 hops:
 1 0 ms 0 ms 0 ms 2000:1::1
 2 0 ms 0 ms 0 ms 2010::2
 3 0 ms 0 ms 0 ms 2000:2::2
Trace complete.
```

Как показано выше, IPv6-пакеты следуют через туннель.

Резюме

В этой главе мы изучили, как работает IPv6 в Packet Tracer. Мы увидели как настраивается статическая и динамическая маршрутизации с поддержкой IPv6. Также разобрались как настроить взаимодействие IPv6-устройств через IPv4-сеть при помощи туннелирования трафика.

В следующей главе, мы войдем в мир беспроводных устройств и изучим, как использовать физическое рабочее пространство для влияния на диапазон этих устройств.

9 Настройка беспроводной сети

Беспроводные сети распространены повсеместно. Каждый может найти точку доступа в большинстве публичных мест. Packet Tracer имеет ограниченное количество устройств, но обеспечивает неограниченное число возможностей. При создании беспроводной сети следует учитывать диапазон действия беспроводных устройств. Несмотря на то, что Packet Tracer только программа-симулятор реальных устройств, можно проверить диапазон действия беспроводной связи, используя возможность перемещения устройств в физическом пространстве программы. В конце главы мы настроим Radius-сервер для обеспечения аутентификации беспроводных устройств.

Беспроводные устройства и их модули

Packet Tracer поддерживает беспроводные модули для ПК, ноутбуков и маршрутизаторов. Доступны следующие модули.

1) **Linksys-WMP300N**. Этот модуль предназначен для серверов, ПК и ноутбуков. Обеспечивает работу в одном радиочастотном диапазоне (2,4 ГГц) и имеет один Ethernet-порт. Настройка данного модуля производится через утилиту «PC Wireless» на вкладке «Рабочий стол» (**Desktop**).

2) **PC-HOST-NM-1W**. Базовый беспроводной интерфейс, работающий в диапазоне 2,4 ГГц и имеющий один Ethernet-интерфейс. Не предусматривает какой-либо настройки.

3) **PC-HOST-NM-1W-A**. Этот модуль аналогичен предыдущему, за исключением поддержки радиодиапазона 5 ГГц.

4) **HWIC-AP-AG-B**. Модуль для маршрутизаторов серий 1841 и 2811. Его функциональность включает интегрированную точку доступа с поддержкой однополосного диапазона 802.11b/g или двухполосного диапазона 802.11 a/b/g.

Далее остановим свой взгляд на устройствах. Packet Tracer обеспечивает такую же поддержку беспроводных оконечных устройств, как и точек доступа.

1) **TabletPC-PT/PDA-PT/WirelessEndDevice-PT**. Данные три устройства обеспечивают схожую функциональность представленную в разных устройствах. Все имеют встроенный беспроводной интерфейс.

2) **AccessPoint-PT/ AccessPoint-PT-A/ AccessPoint-PT-N**. Простые точки доступа с минимумом конфигурационных опций. Все устройства имеют антенну и порт для подключения к таким устройствам, как маршрутизатор или DHCP-сервер.

3) **Linksys-WRT300N**. Данное беспроводное устройство имеет веб-интерфейс аналогичный реальному беспроводному маршрутизатору Linksys для ввода идентификатора беспроводной сети SSID, беспроводной аутентификации, порт глобальной сети WAN и многие другие опции. Это устройство имеет 4 Ethernet-порта для локальной сети LAN и один Ethernet-порт глобальной сети WAN, предназначенный для Интернет-подключения.

Зная беспроводные устройства, доступные в Packet Tracer, приступим к настройке беспроводной сети. Мы будем использовать две точки доступа с двумя различными SSID (рисунок 66).

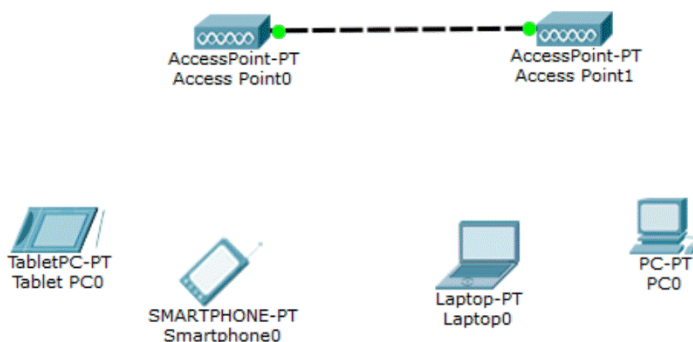


Рисунок 66 – Пример простой беспроводной сети

В качестве беспроводных устройств используем **TabletPC-PT** и **PDA-PT**. Как только сеть создана, вы можете обнаружить, что эти устройства подключаются к какой-либо беспроводной точке доступа. Установим SSID точки доступа Access Point0 как Office, а точки доступа Access Point1 как Guest. Для ПК и ноутбука замените стандартные интерфейсы на беспроводные (Linksys-WMP300N).

Откройте каждую из точек доступа, перейдите на вкладку «Настройка» (**Config**), выберите порт **Port1** и измените поле **SSID** (рисунок 67).

Затем настроим оконечные устройства. Для этого переходим на вкладку «Настройка» (**Config**), выберите опцию Wireless секции INTERFACE и измените SSID, как показано на рисунке 68.

Вы можете видеть беспроводное подключение каждого оконечного устройства к соответствующей точке доступа. Назначьте каждому оконечному устройству IP-адреса из одной и той же подсети. Используйте инструмент «Простой PDU» для проведения теста связности и проверки работоспособности сети.

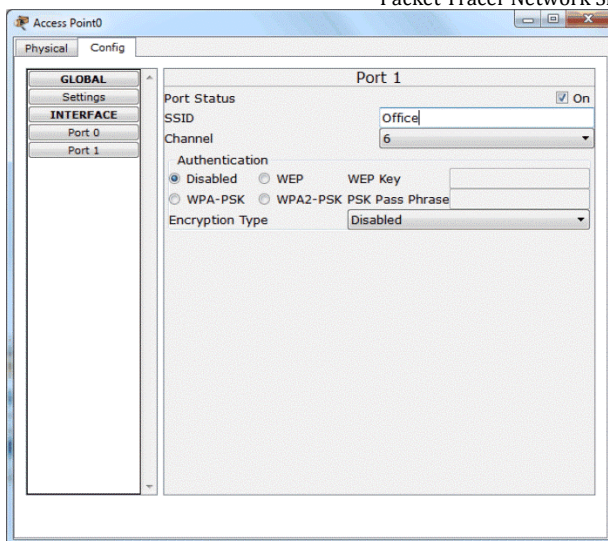


Рисунок 67 – Вкладка «Настройка» точки доступа

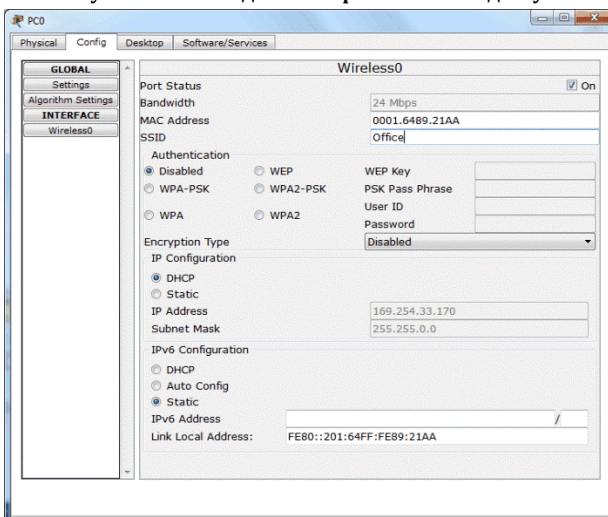


Рисунок 68 – Настройка беспроводного интерфейса оконечного устройства

Беспроводные сети в физическом рабочем пространстве

В реальном мире каждое беспроводное устройство имеет ограничение по расстоянию, на котором обеспечивается связность. Packet Tracer

имитирует это ограничение при работе в физическом рабочем пространстве. Мы можем увидеть, как это случается, когда передвигаем ноутбук с беспроводным интерфейсом во вне зоны действия беспроводной сети. В качестве упражнения будем использовать следующую топологию (рисунок 69).

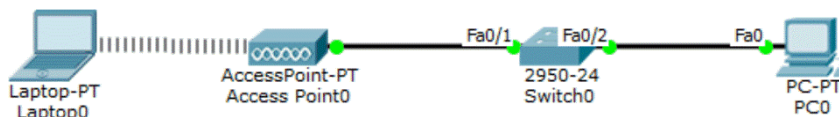


Рисунок 69 – Пример беспроводной сети с ограничением зоны доступа

В этой топологии имеются беспроводная точка доступа (Access Point0) подключенная к коммутатору (Switch), к которому также подключен ПК (PC). Предполагается подключение ноутбука (Laptop) к точке доступа.

Настроим IP-адреса на обоих компьютерах: 10.0.0.1 для ноутбука и 10.0.0.2 для ПК. После этого проведем тест связности при помощи утилиты ping, он должен быть успешным. Теперь переключаемся на физическое рабочее пространство, перемещаемся «Домашний город» (Home Sity)| «Корпоративный офис» (Corporate Office). Вы обнаружите сетку, что показывает зону действия беспроводной связи.

Передвиньте ноутбук из зоны действия беспроводной связи (рисунок 70) и проверьте тест связности между ноутбуком и ПК. Тест связности покажет ошибку, т. к. ноутбук оказался перемещенным вне зоны действия беспроводной точки доступа.

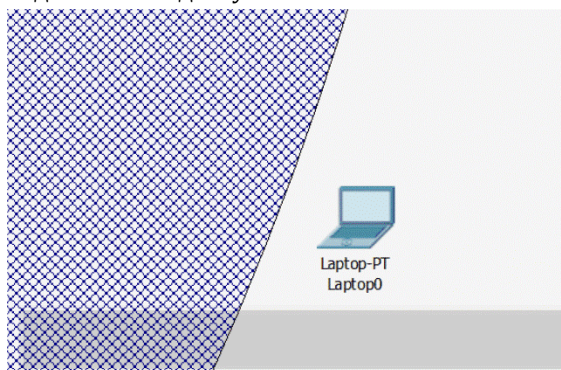


Рисунок 70 – Перемещение ноутбука во вне зоны действия беспроводной связи

Вернемся в логическое рабочее пространство и обнаружим, что также исчезло символическое изображения беспроводной связи между ноутбуком и точкой доступа.

Если вы не смогли передвинуть ноутбук за пределы действия точки доступа, необходимо переместить ноутбук на уровень корпоративного офиса (Navigation→Home City→ Corporate Office→ Move to Corporate Office).

Настройка беспроводной точки доступа Linksys

Мы создавали беспроводную сеть без таких дополнительных возможностей, как служба DHCP. В этом разделе мы будем использовать беспроводной маршрутизатор Linksys-WRT300N, доступный в Packet Tracer и создадим сеть с этой дополнительной возможностью (рисунок 71).

Мы также добавим RADUIS-сервер в эту сеть и разрешим аутентификацию по протоколу RADUIS. При этом на маршрутизаторе выберем режим аутентификации **WPA2-PSK enterprise**. После создания этой топологии необходимо заменить стандартный модуль ноутбука (Laptop0) на беспроводной модуль **Linksys-WMP300N**. Откроем Linksys-маршрутизатор, переходим на вкладку «Графический интерфейс пользователя» (**GUI**), там выбираем вкладку «Беспроводная связь» (**Wireless**) и производим замену стандартного имени в поле **SSID** на имя Linksys.

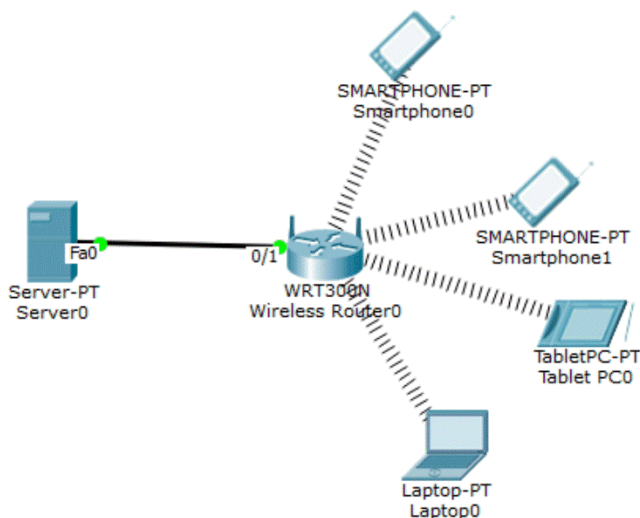


Рисунок 70 – Беспроводная сеть на основе Linksys-WMP300N

Откроем сервер, перейдём на вкладку «Службы» (**Services**), выбираем секцию **AAA** и настраиваем RADIUS-аутентификацию (таблица 7) и вводим 4 четыре пользователя (таблица 8).

Таблица 7 – Опции настройка AAA на RADIUS-сервере

ClientName	ClientIP	ServerType	Key
Linksys	192.168.0.1	Radius	password

Таблица 8 – Настройка RADIUS-аутентификации на сервере

User Name	Password
alice	pwd
bob	s3rec
john	secr3t
user1	passwd

Присваиваем серверу статический IP-адрес 192.168.0.50. На вкладке **GUI** Linksys-маршрутизатора переходим «Беспроводная сеть» (**Wireless**)→ «Безопасность» (**Wireless security**) и вводим следующие настройки (таблица 9).

Таблица 9 – Настройки безопасности беспроводной сети

Security Mode	WPA2 Enterprise
Encryption	AES
RADIUS Server	192.168.0.50
RADIUS Port	1645
Shared Secret	password

Далее переходим к пользовательским устройствам, открываем вкладку «Настройка» (**Config**), выбираем «Беспроводное соединение» (**Wireless**) и вводим следующие значения:

SSID: Linksys

Authentication: WPA2

User ID: john

Password: secr3t

На каждом из устройств необходимо ввести свои значения пары логин/пароль (см. таблица 8). Как только введены данные аутентификации, беспроводные устройства получают IP-адреса, и вы можете увидеть отображение беспроводного подключения.

Вслед за этим настроим Linksys-модуль ноутбука. Переходим на вкладку «Рабочий стол» (**Desktop**), открываем утилиту «Беспроводное подключение» (**PC Wireless**), переходим на вкладку «Профили» (**Profiles**) и нажмите кнопку «Новый профиль» (**New**). Введите здесь любое имя профиля и нажмите **OK**, за этим вы увидите отображаемое значения SSID. Затем нажмите «Дополнительные настройки» (**Advanced Setup**) и пройдите все этапы мастера настройки последовательно до конца. После создания профиля вернитесь на вкладку «Профиль», выберите созданный вами профиль и нажмите кнопку «Подключение» (**Connect**).

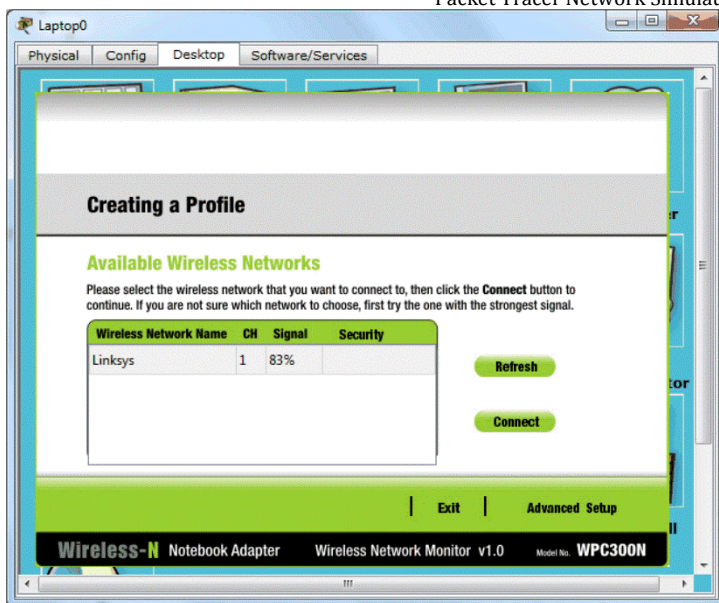


Рисунок 71 – Создание нового профиля

Воспользуйтесь инструментом «Простой PDU» для проведения теста связности. Если вы перейдете в режим имитации до установления беспроводной связи между пользовательскими устройствами и точкой доступа, то увидите RADIUS-сообщения, пересылаемые от сервера к маршрутизатору.

Резюме

Эта глава вводит вас в мир беспроводных устройств Packet Tracer. Вы также настроили простую беспроводную топологию без какой-либо аутентификации и использовали физическое рабочее пространство для демонстрации зоны действия беспроводных устройств. Наконец мы смешали такие технологии как WPA2, RADIUS и DHCP и создали сеть с использованием Linksys-устройств.

В следующей главе, мы рассмотрим сегментацию на втором уровне с настройкой виртуальных локальных сетей VLAN, а также настроим маршрутизацию между VLAN-сетями.

10 Настройка VLAN и магистральных каналов

Коммутаторы разбивают коллизийный домен на множество мелких, а также представляют собой единый широковещательный домен. Почему так происходит? Виртуальные локальные сети VLAN (Virtual LAN) делают возможным так, что на одном коммутаторе мы получаем множество широковещательных доменов. Однако создав на одном коммутаторе множество VLAN, мы столкнемся с утомительной работой по распространению этой конфигурации на все другие коммутаторы. Таким образом мы получаем множество коммутаторов с разрозненными настройками VLAN. Здесь пригодится протокол VTP (VLAN Trunking Protocol). Теперь имея VLAN и протокол VTP, мы делаем управление простым. Но как мы обеспечим взаимодействие между устройствами различных VLAN? Для этого мы рассмотрим маршрутизацию между виртуальными сетями (InterVLAN).

Создание VLAN и VTP-домена

Виртуальные локальные сети VLAN – технология, предусматривающая разбиение простой сети второго уровня на множество широковещательных доменов. Это ограничивает сетевое взаимодействие только устройствами, которые находятся в одном и том же широковещательном домене. При этом устройства все-таки могут взаимодействовать, но при помощи устройства третьего уровня, таких как маршрутизаторы или коммутаторы третьего уровня. В общем случае это напоминает подключение пользовательских устройств к разным коммутаторам, а затем соединение коммутаторов через маршрутизатор как отдельных широковещательных доменов (подсетей).

Чем больше и больше создается VLAN, тем более утомительным становится репликация (распространение) конфигурации на все коммутаторы сети. Именно поэтому и был создан магистральный протокол VLAN (VLAN Trunking Protocol, VTP).

Вначале мы изучим создание и присвоение портов VLAN. Сеть управления (VLAN 1) имеется сразу на всех коммутаторах, и все порты коммутатора приписаны к этой виртуальной сети.

Для создания VLAN используется следующая команда:

```
Sw1(config)#vlan 2
```

Идентификатор (номер) VLAN может принимать значения в диапазоне от 1 до 1001. Номера 1002 – 1005 зарезервированы. При вводе указанной команды вы оказываетесь в режиме конфигурирования VLAN. Здесь можно присвоить имя для VLAN.

```
Sw1(config-vlan)#name finance
```

Присвоение имени необязательно. Если не присваивать имя вручную, то система сама сгенерирует имя на основе номера сети, для нашего случая (VLAN2) это будет VLAN0002.

Далее необходимо добавить несколько портов в эту VLAN. Для присвоения сразу нескольких портов в одну виртуальную сеть можно воспользоваться опцией `range`, после которой указав диапазон портов.

```
Sw1(config)#interface range f0/10-20
```

Для назначения этих портов к VLAN2 используем следующую команду:

```
Sw1(config-if-range)#switchport access vlan 2
```

Наконец, следует убедиться, что порты действительно присвоены к правильной VLAN.

```
Sw1#show vlan
```

```
Sw1#show vlan
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/21, Fa0/22, Fa0/23 Fa0/24
2	finace	active	Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

Рисунок 72 – Результат работы команды `show vlan`

Некоторые строки, выводимые при выполнении данной команды, для краткости были опущены.

Создадим новую топологию с тремя коммутаторами для демонстрации принципов работы протокола VTP. Магистральный протокол виртуальных локальных сетей имеет три режима работы: серверный (`server`), клиентский (`client`) и прозрачный (`transparent`).

1) Серверный режим работы включен по умолчанию. В этом режиме коммутаторам разрешено модифицировать их VLAN и посылать VTP-объявления.

2) В клиентский режим работы коммутаторы прослушивают VTP-объявления от других коммутаторов, работающих в серверном режиме. Коммутаторы, работающие в режиме клиента VTP, не имеют возможности локально изменять собственную базу данных, такое возможно только на основе принимаемых VTP-объявлений.

3) Прозрачный режим работы предполагает независимость от других коммутаторов. В это режиме коммутатор только продвигает VTP-

объявления, которые были им приняты, но никаких объявлений не генерирует, ни изменяет собственную базу данных VLAN на основе VTP-объявлений.

Следующая топология (рисунок 73) послужит для демонстрации принципов работы VTP-протокола.

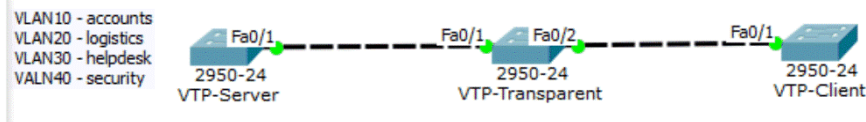


Рисунок 73 – Пример, демонстрирующий режимы работы протокола VTP

1) На первом коммутаторе (VTP-Server) необходимо создать имеем 4 VLAN с различными именами, как указано на рисунке 73. Затем мы создаем между коммутаторами магистральную связь, для этого переводим порты между коммутаторами в транковый режим работы.

```
VTP-Server(config)#interface Fa0/1
VTP-Server(config-if)#switchport mode trunk
VTP-Transparent(config)#interface range Fa0/1-2
VTP-Transparent(config-if-range)#switchport mode trunk
VTP-Client(config)#interface Fa0/1
VTP-Client(config-if)#switchport mode trunk
```

2) Т.к. по умолчанию используется серверный режим работы VTP, следует изменить имя VTP-домена и установить пароль.

```
VTP-Server(config)#vtp domain My-Office
Changing VTP domain name from NULL to My-Office
VTP-Server(config)#vtp password s3cRet
Setting device VLAN database password to s3cRet
```

3) Переходим к второму коммутатору (VTP-Transparent) и переводим его в прозрачный режим/

```
VTP-Transparent(config)#vtp mode transparent
```

4) Наконец переходим к третьему коммутатору (VTP-Client) и переводим его в режим клиента.

```
VTP-Client(config)#vtp mode client
```

5) Вы не должны изменять имя VTP-домена на этом коммутаторе. Данный коммутатор присоединится к VTP-домену под влиянием VTP-объявлений сервера (VTP-Server). При этом необходимо установить пароль, такой же как на сервере.

```
VTP-Client(config)#vtp password s3cRet
```

Настройка сети закончена. Теперь воспользуемся командой `show vlan` на коммутаторе VTP-Client для просмотра новых VLAN.

В данном примере демонстрируются принципы работы VTP. Такая топология не имеет смысла, т. к. между коммутатором VTP-Server и коммутатором VTP-Client не обеспечивается нормальное взаимодействие.

Между ними находится коммутатор VTP-Transparent, работающий в прозрачном режиме и не имеющий ни одной VLAN—сети, что мы сконфигурировали.

Настройка маршрутизации между VLAN (Inter-VLAN)

Хотя VLAN создаются с целью разбиения широкополосного домена на более мелкие, для взаимодействия между собой они нуждаются в ведении сетевого уровня с поддержкой IP-маршрутизации. Это называется Inter-VLAN (маршрутизация между виртуальными локальными сетями) и может быть выполнено с использованием как и маршрутизаторов, так коммутаторов третьего уровня. Inter-VLAN маршрутизация требует выделения отдельной подсети для каждой подсети.

Мы настроим Inter-VLAN маршрутизацию, подключив маршрутизатор к коммутатору одним каналом. Весь трафик разных VLAN проходит через этот канал связи. Такой метод конфигурации называется маршрутизатор на палочке (router-on-a-stick), т. к. для передаче всего трафика используется одиночный канал маршрутизатора.

Настройка Inter-VLAN на маршрутизатора

Используем следующую топологию для настройки маршрутизации между виртуальными сетями (рисунок 74).

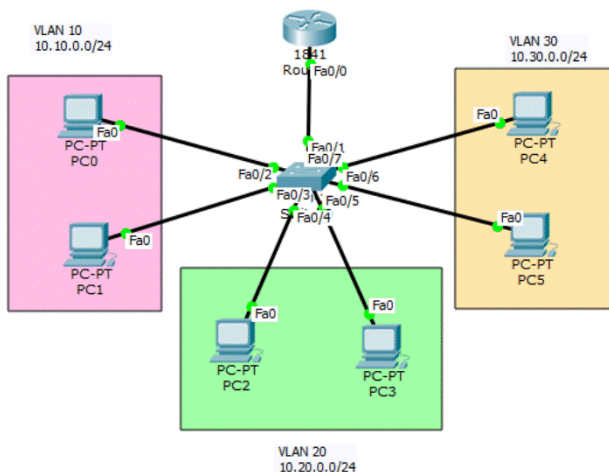


Рисунок 74 – Inter-VLAN маршрутизация

Напомним, что каждая VLAN будет иметь отдельную IP-подсеть, и маршрутизатор должен иметь три IP-адреса, соответствующих каждой VLAN.

1) После присвоения IP-адресов всем компьютеров (IP-адреса подсетей приведены на рисунке 74, в качестве шлюзов по умолчанию используем первые IP-адреса соответствующих подсетей) создадим на коммутаторе необходимые виртуальные сети и присвоим его порты к определенным VLAN.

```
Sw1(config)#int range f0/2-3
Sw1(config-if-range)#switchport access vlan 10
Sw1(config-if-range)#int range f0/4-5
Sw1(config-if-range)#switchport access vlan 20
Sw1(config-if-range)#int range f0/6-7
Sw1(config-if-range)#switchport access vlan 30
```

2) Настроим порт коммутатора, подключенный к маршрутизатору, как магистральный порт (trunk). Более подробно о магистральных портах будет разъяснено далее.

```
Sw1(config)#int f0/1
Sw1(config-if)#switchport mode trunk
```

3) Далее приходим на маршрутизатор и включаем порт, соединенный с коммутатором.

```
R1(config)#int f0/0
R1(config-if)#no shutdown
```

4) Создадим на интерфейсе fa0/0 подинтерфейсы. Каждый из подинтерфейсов будет иметь собственный IP-адрес, соответствующий определенной VLAN.

```
R1(config-subif)#int f0/0.10
R1(config-subif)#encapsulation dot1Q 10
R1(config-subif)#ip address 10.10.0.1 255.255.255.0
R1(config-subif)#int f0/0.20
R1(config-subif)#encapsulation dot1Q 20
R1(config-subif)#ip address 10.20.0.1 255.255.255.0
R1(config-subif)#int f0/0.30
R1(config-subif)#encapsulation dot1Q 30
R1(config-subif)#ip address 10.30.0.1 255.255.255.0
```

5) Обратите внимание на команду *encapsulation*. Она определяет номер виртуальной сети, в которой будет находится данный подинтерфейс.

6) Настройка окончена, осталось только провести тест связности между компьютерами различными VLAN с использованием инструмента «Простой PDU» или утилиты *ping*. Первый пакет может быть потерян из-за некоторой задержки, связанной с выполнением ARP-запроса. Для просмотра пути следования пакетов используем утилиту *tracert*.

Настройка Inter-VLAN на коммутаторе третьего уровня

В Packet Tracer присутствует только один коммутатор третьего уровня 3560-24PS. В качестве упражнения используем такую же топологию, заменив в ней маршрутизатор на коммутатор третьего уровня (рисунок 75).

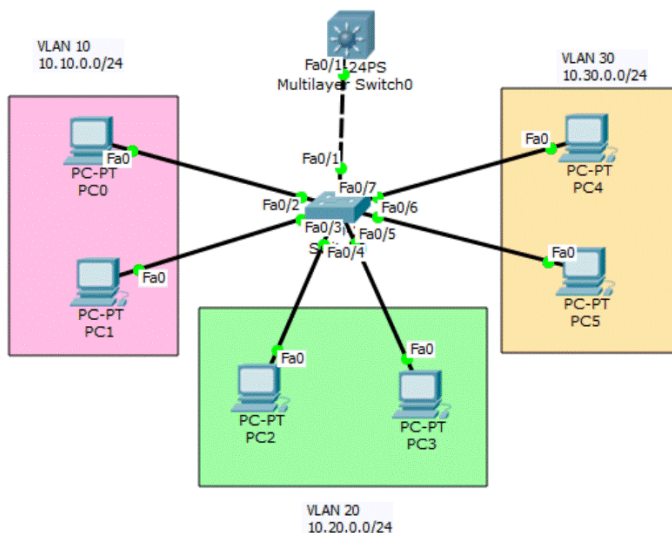


Рисунок 75 – Inter-VLAN маршрутизация на коммутаторе третьего уровня

Т. к. в данном упражнении создание VLAN и сопутствующих на коммутаторе второго уровня совпадает с предыдущим примером, эту часть настроек опускаем и переходим к конфигурированию коммутатора третьего уровня. Обратите внимание, что интерфейс fa0/1 этого коммутатора окажется в режиме магистрального порта, как можно убедиться при помощи следующей команды:

```
MSW1#show interface trunk
```

```

Multilayer Switch0
Physical Config CLI
IOS Command Line Interface

MSW1#
MSW1#show interfaces trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/1     auto      n-802.1q       trunking    1

Port      Vlans allowed on trunk
Fa0/1     1-1005

Port      Vlans allowed and active in management domain
Fa0/1     1

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     1
  
```

Рисунок 76 – Результат выполнения show interface trunk

Значение поля статуса trunking указывает на магистральный режим работы данного порта. Каким образом этот порт автоматически переходит в режим транка будет разобран далее в этой главе.

2) Для коммутатора третьего уровня необходимо настроить так называемый виртуальный коммутирующий интерфейс **SVI (Switch Virtual Interface)**, который позволяет задействовать интерфейс третьего уровня для каждой VLAN

```
MSw1(config)#int vlan 10
MSw1(config-if)#ip add 10.10.0.1 255.255.255.0
MSw1(config-if)#int vlan 20
MSw1(config-if)#ip add 10.20.0.1 255.255.255.0
MSw1(config-if)#int vlan 30
MSw1(config-if)#ip add 10.30.0.1 255.255.255.0
```

3) Эти интерфейсы будут находиться в выключенном состоянии, т. к. коммутатор не имеет виртуальных локальных сетей VLAN 10, VLAN 20, VLAN 30. Создадим их при помощи следующих команд

```
MSw1(config)#vlan 10
MSw1(config-vlan)#vlan 20
MSw1(config-vlan)#vlan 30
```

4) После ввода каждой из команд соответствующие SVI-интерфейсы станут активными. Необходимо также разрешить IP-маршрутизацию на коммутаторе третьего уровня.

```
MSw1(config)#ip routing
```

5) В конце концов воспользуемся инструментом «Простой PDU» для проведения теста связности.

Заметим, что первый пакет также будет потерян из-за временной задержки, связанной с выполнением ARP-запроса.

Магистральные каналы коммутаторов

Когда два коммутатора подключены друг к другу, должен существовать механизм для идентификации принадлежности кадров к определенной VLAN. Это не имеет отношение к физическому уровню, а всецело лежит в плоскости канального уровня. При подключении двух коммутаторов друг к другу каждый из них должен знать для какой VLAN предназначен передаваемый трафик. При этом используется тегирования кадров. Когда кадры передаются по межкоммутаторному каналу связи, исходящий коммутатор вставляет в кадр дополнительные поля, связанные с идентификатором VLAN. Канал между коммутаторами называется магистральным или транком (trunk).

На следующем рисунке (рисунок 77) представлены детали входящего и исходящего кадров, захваченных в режиме имитации, когда ПК из сети VLAN 10 пингует ПК из сети VLAN 30.

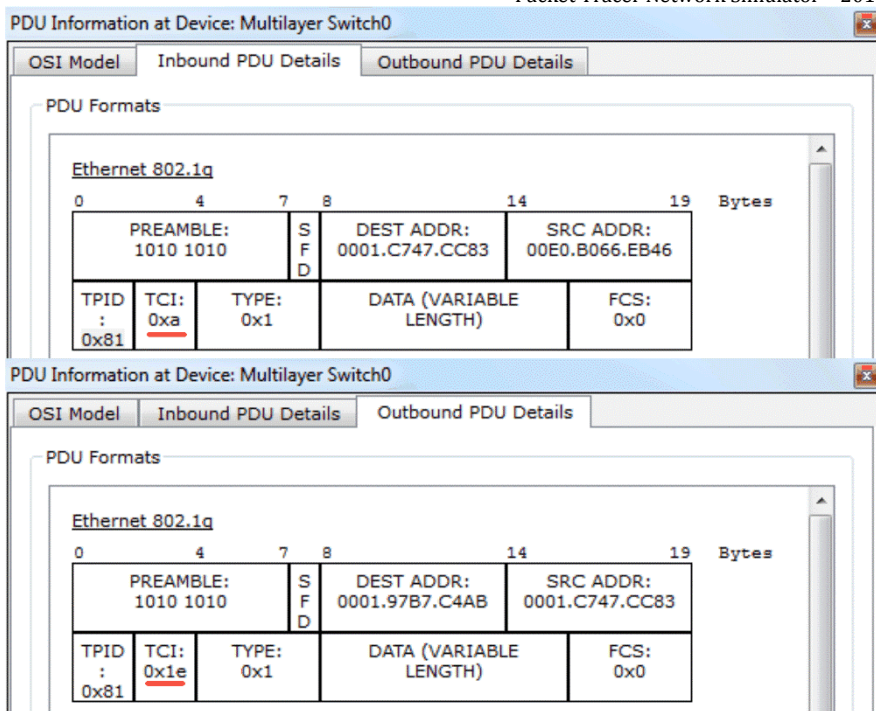


Рисунок 77 – Тегированные кадры с разными идентификаторами VLAN

Заметим, что поле **TCI (Tag Control Information)** содержит шестнадцатеричное значение VLAN ID. Для входящего кадра оно равно 0xA, что соответствует VLAN 10; для исходящего кадра – 0x1E, что, в свою очередь, соответствует VLAN 20.

Анализ работы VLAN в режиме имитации

Концепция VLAN предполагает разбиение широковещательного домена. В последнем разделе этой главы мы рассмотрим в режиме имитации как обрабатываются широковещательные кадры, принадлежащие разным VLAN. Воспользуемся предыдущей топологией. При помощи инструмента «Сложный PDU» и создадим ICMP-пакет от ПК к всей сети, указав в качестве IP-адреса получателя 255.255.255.255. Такой адрес устанавливает широковещательный адрес на канальном уровне (FFFF.FFFF.FFFF). Перейдите в режим имитации и посмотрите, что будет происходить. Коммутатор принимает от ПК0 ICMP-пакет и посылает только две копии этого пакета: один к коммутатору третьего уровня (или маршрутизатору) и к ПК1, находящемуся в той же VLAN 10. Если бы

не было бы разбивка на VLAN, такой пакет должен быть доставлен всем ПК подключенным к коммутатору.

Резюме

В этой главе мы изучили, как использовать устройства в Packet Tracer для создания VLAN и настраивать протокол VTP для простого управления VLAN. Мы также настроили InterVLAN-маршрутизацию с использованием как маршрутизатора, так и коммутатора третьего уровня. Таким образом вы познакомились с виртуальными коммутируемыми интерфейсами, присущими коммутаторами третьего уровня. Наконец, мы изучили различия между каналами доступа (связь ПК-коммутатор) и магистральными каналами (коммутатор-коммутатор, называемых также транком). Имитационный режим Packet Tracer здесь окажет неоценимую пользу, обеспечивая визуализацию потока пакетов в VLAN-окружении.

В следующей и последней главе мы покажем, как создавать практические экзаменационные задания в Packet Tracer, чтобы вы могли распространять и использовать их для проведения тестирования ваших студентов или кандидатов на рабочее место.

11 Создание практических тестов в Packet Tracer

Наконец-то мы достигли последней главы. До сих пор мы использовали Packet Tracer для самостоятельного изучения сетевых вещей, но в этой главе мы создадим оценочный тест для проверки, как другие люди учатся. Packet Tracer, будучи симулятором реального оборудования, в дополнение объединяет функции оценочного инструмента с большим потенциалом. Создание оценочных тестов также просто, как и создание начальной или конечной (или иначе финальной) сетей

Мастер активации (Activity Wizard) является руководством для вас при создании оценочной сети. Он запускается при помощи меню «Расширения» (**Extensions**)| «Мастер активации» (**Activity Wizard**) или при помощи клавиатурного сокращения Alt+W. В этой главе мы создадим простой оценочный тест в виде сети, состоящей из ПК, маршрутизатора, коммутатора и сервера, и настроим в ней простой список управления доступом **ACL (Access Control List)**.

Экран приветствия и окно инструкции

Экран-приветствия (**Welcome**) предлагает вам ввести информацию об авторе и добавить комментарии (**Author Information**). В окно инструкций (**Instructions**) мы описываем вопросы и задачи для пользователя. В этом окне используется HTML-синтаксис для форматирования инструкций. Набор поддерживаемых тегов можно найти в файле помощи Packet Tracer.

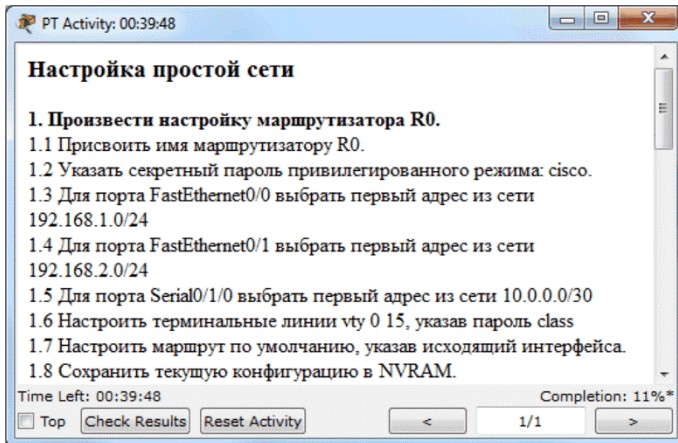


Рисунок 78 – Окно инструкций

В этом примере используются HTML-теги для создания упорядоченных списков `<ol>` и `<li>`.

Начальная сеть

Первое окно, которое видит экзаменующийся, представляет собой начальную сеть. Нажмите «Показать начальную сеть» (**Show Initial Network**) и вы попадете в логическое пространство, где можно добавлять устройства. Добавьте только устройства, показанные на рисунке 79, без взаимного подключения друг с другом и без присвоения IP-адресов.



Рисунок 79 – Начальная сеть

Затем откроем вкладку CLI маршрутизатора и изменим имя устройства, а также установим пароль, используя следующие команды:

```
Router>en
Router#conf t
Router(config)#hostname R1
R1(config)#enable secret cisco
```

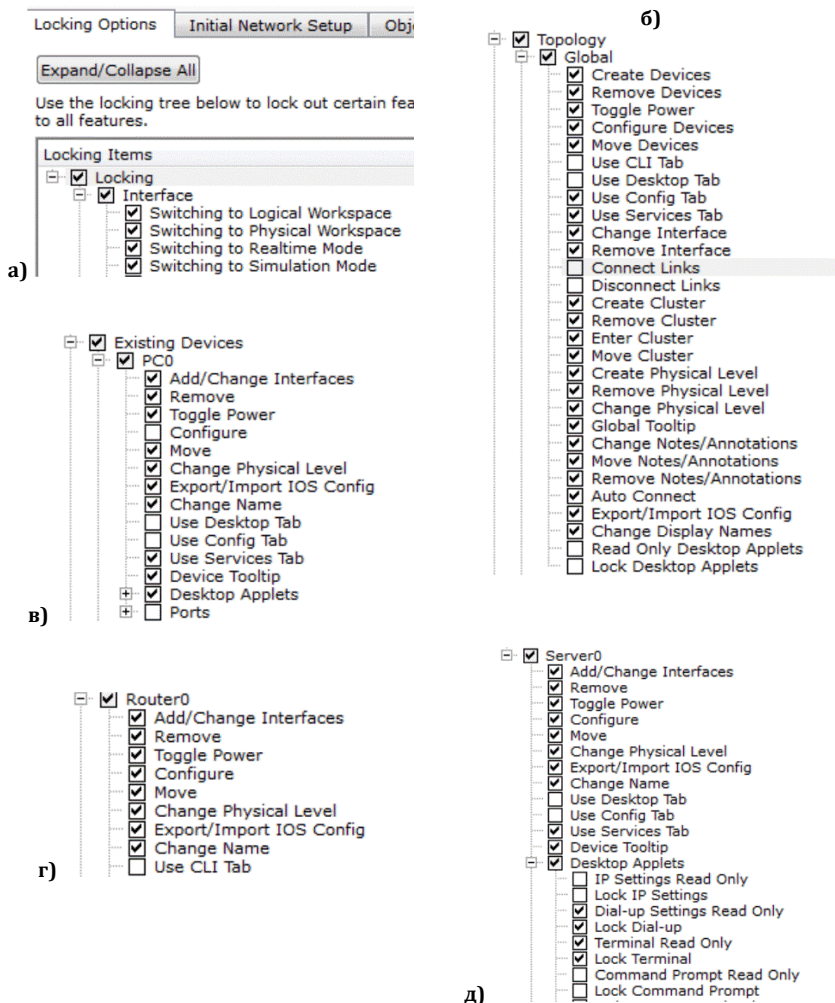
На этом мы заканчиваем создание начальной сети. Кликните по значку «Мастера активаций» (волшебной шляпе и палочке, расположенных в нижнем левом углу рабочего пространства) для возврата в мастер настройки. Сохраните топологию, нажав на «Экспорт начальной сети в файл» (**Export Initial Network to File**). Сохраненный файл послужит нам для создания сети-ответа.

Сейчас мы укажем характеристики, что будут заблокированы в главном интерфейсе так, что пользователи не смогут получить помощь от некоторых инструментов Packet Tracer. Некоторое множество пунктов может быть отмечено на вкладке «Опции блокировки» (**Locking Item**). Следующий рисунок (рисунок 80, а) показывает выбранные пункты в секции «Интерфейс» (**Interface**).

На рисунке 80, б отображены заблокированные опции из секции «Топологи» (**Topology**)

В секции «Существующие устройства» (**Existing Devices**) необходимо отметить опции в соответствии с рисунками 80, в (для ПК), 80, г (для маршрутизатора), 80, д (для сервера).

Вот и все с настройками начальной сети (уточните, чтобы «Режим имитации» был отмечен как заблокированный).



**Рисунок 80 – Опции блокировки в секциях:
а) Interface; б) Topology; в) PC0; г) Router; д) Server**

Сеть ответов

Перейдем к созданию сети ответов. Откроем секцию «Сеть ответов» (**Answer Network**) и импортируем файл, что был предварительно сохранен. Необходимо закончить настройку этой сети. Финальная сеть – это та сеть, которую вы желаете, чтобы конечные пользователи создали. Кликните «Показать сеть ответов» (**Show Answer Network**) и вы увидите ту же сеть, что создали на начальном этапе. Наше конечная сеть должна будет выглядеть в соответствии с рисунком 81.

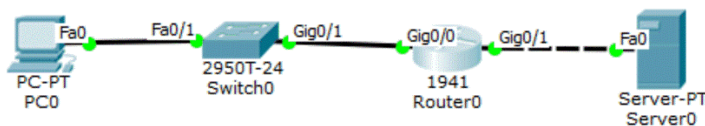


Рисунок 81 – Финальная сеть

Мы используем следующие настройки:

1) ПК

- IP-адрес: 10.10.0.2
- Маска: 255.255.255.0
- Шлюз по умолчанию: 10.10.0.1

2) Маршрутизатор:

- GigabitEthernet0/0: 10.10.0.1/24 (подключен к ПК)
- GigabitEthernet0/1: 30.10.0.1/24 (подключен к серверу)

2) Сервер

- IP-адрес: 10.10.0.2
- Маска: 255.255.255.0
- Шлюз по умолчанию: 10.10.0.1

После присвоения указанных адресов ПК и серверу тоже следует сделать и для маршрутизатора.

```

R1(config)#int g0/0
R1(config-if)#ip add 10.10.0.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#int g0/1
R1(config-if)#ip add 30.10.0.1 255.255.255.0
R1(config-if)#no shut
  
```

Далее настраиваем на маршрутизаторе список управления доступом ACL с разрешениями только для ICMP (Internet Control Message Protocol) и HTTP трафика.

```

R1(config)#ip access-list extended 100
R1(config-ext-nacl)#permit icmp any host 30.10.0.10
R1(config-ext-nacl)#permit tcp any host 30.10.0.10 eq www
R1(config)#int g0/0
  
```

```
R1(config-if)#ip access-group 100 in
```

Протестируем работу списка управления доступом. Откроем ПК и пропиnguем сервер. Затем проведем тест связности с использованием команды ftp с указанием адреса сервера (рисунок 82).

Как и следовало ожидать FTP-соединение завершилось с ошибкой.

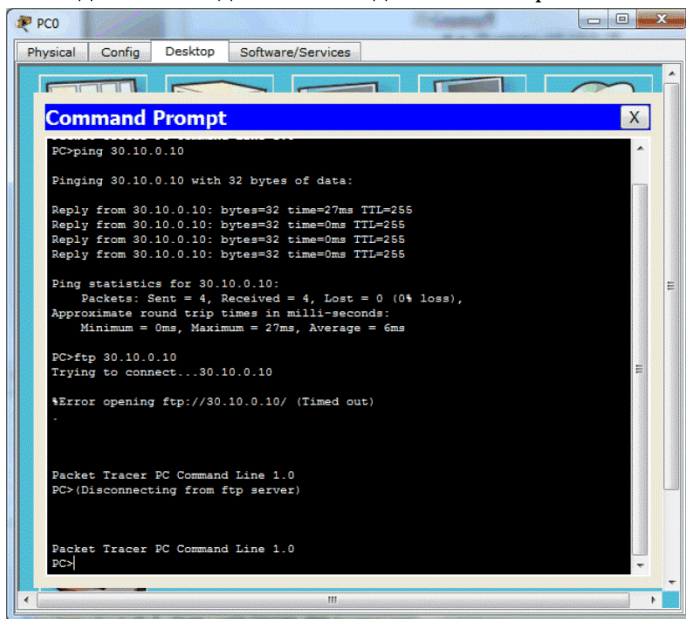


Рисунок 82 – Проверка работы ACL

Далее откроем утилиту «Веб-браузер» (**Web Broser**) и проверим доступность веб-сервера.

Для внедрения в наше задание проверочных запросов, мы нуждаемся в создании таких же тестов с использованием PDU-инструментов. При этом необходимо создать следующие тесты связности:

- ICMP-тест с использованием инструмента «Простой PDU» (успешное завершение);
- HTTP-тест с использованием инструмента «Сложный PDU» (успешное завершение);
- FTP-тест с использованием инструмента «Сложный PDU» (завершиться с ошибкой).

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	PC0	Server0	ICMP		0.000	N	0	(edit)
	Successful	PC0	30.10.0.10	TCP		2.000	N	1	(edit)
	Failed	PC0	30.10.0.10	TCP		3.000	N	2	(edit)

Рисунок 83 – Выполнение тестов связности

Далее необходимо установить критерии успешности прохождения теста. Кликните по волшебным предметам для возврата в мастер настройки. Для сохранения финальной сети кликните «Экспорт начальной сети в файл» (**Export Initial Network to File**).

Затем нам надо определиться с выбором критериев оценки. Мы будем требовать оценку назначения IP-адресов ПК, маршрутизатора и сервера, соединений между ними и теста связности между ПК и сервером. Следующие списки необходимо отметить в Assessment Item:

ПК/Сервер:

- Шлюз по умолчанию (**Default Gateway**)
- Порты→ **FastEthernet0**:
 IP-адрес (**IP address**)
 Статус порта (**Port Status**)
 Маска (**Subnet Address**)
 Подключение к коммутатору/ маршрутизатору
 (**Link to switch/ router**): поле тип (**Type**)

Маршрутизатор:

- Список управления доступом (**ACL**)
- Порты
GigabitEthernet0/0:
 Входящий список (**Access group In**)
 IP-адрес (**IP Address**)
 Маска (**Subnet Mask**)
 Подключение к коммутатору (**Link to switch**):
 поле тип (**Type**)
GigabitEthernet0/1:
 IP-адрес (**IP Address**)
 Маска (**Subnet Mask**)
 Подключение к коммутатору (**Link to switch**):
 поле тип (**Type**)

После завершения конфигурирования критериев оценки, надо проверить связность. Переходим к вкладку «Тест связности» (**Connectivity Test**); там обнаруживаем три PDU, сгенерированных ранее нами. Поле «Состояние теста» (**Test Condition**) для двух первых пакетов (ICMP и HTTP) показано как успешное (success), а для третьего – ошибка (failure). Это является следствием встроенной проверки, чтобы убедиться, что список управления доступом настроен правильно.

Переходим на вкладку «Настройки» (**Settings**) и задаем таймер обратного счета. Установка обратного отсчета автоматически появиться в

всплывающем окне финальной сети, как только время истечет. Установим значение таймера равным 20 мин.

Кликните на кнопке «Пароль» (**Password**) и назначьте пароль защиты. Как только пользователи при прохождении теста попытаются получить доступ к мастеру активности, им будет предложено ввести этот пароль.

Тестирование созданной оценочной работы

После того, как мы подготовили оценочную работу, следует протестировать и убедиться в ее работоспособности. Нажмите кнопку «Тестирование» (**Test Activity**). Выполните тест, обращая внимание на то, как увеличивается процент успешной сдачи. Также попытайтесь осуществить доступ к функциям Packet Tracer, которые были заблокированы нами ранее.

Как только вы будете удовлетворены результатом, вернитесь назад к мастеру активации и кликните «Сохранить» (**Save**). Файл теста будет сохранен с расширением .pka. Этот файл может быть предложен всем, кто будет участвовать в тестировании. Если пользователи попытаются открыть мастер активации, потребуется ввод пароль.

Резюме

В этой главе вы получили начальную информацию по созданию в Packet Tracer оценочного теста. Механизм тестирования также предоставляет множество возможностей для работы с переменными. Переменные обеспечивают гибкость в обслуживании широкого спектра пользовательских операций. Packet Tracer также поддерживает скриптовый механизм. Используя свои навыки программирования, вы можете создавать более интерактивные оценочные тесты.