МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра космического приборостроения и систем связи

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О. Г. Локтионова
«__» _____ 2020 г.

КОММУТАЦИЯ И МАРШРУТИЗАЦИЯ В CISCO PACKET TRACER

Методические указания
по выполнению лабораторных работ
для студентов, обучающихся по направлению подготовки
11.03.02 Инфокоммуникационные технологии и системы связи

Курск 2020

УДК 654:004.7 (075.8)

Составитель: И. Г. Бабанин

Рецензент
Кандидат технических наук, доцент кафедры *Е.О. Брежнева*

Коммутация и маршрутизация в Cisco Packet Tracer: методические указания по выполнению лабораторной работы / Юго-Зап. гос. ун-т; сост.: И.Г.Бабанин. – Курск, 2020. – 61 с.

Методические указания по выполнению лабораторных работ содержат краткие теоретические сведения о сетевом эмуляторе Cisco Packet Tracer, первоначальной настройке сетевых устройств, протоколе покрывающего дерева (STP), организации виртуальных сетей (VLAN), статической и динамической маршрутизации, технологии NAT, сетевой фильтрации ACL, функции Zone-Based Policy Firewall, задания по выполнению работ, а также перечень вопросов для самопроверки изучаемого материала.

Полученные знания в результате выполнения работы дадут возможность сформировать целостную картину информационного взаимодействия в современных сетях, что является фундаментом для изучения остальных дисциплин профессионального цикла учебного плана, а также могут быть использованы в будущей профессиональной деятельности выпускника, связанной с сетевыми технологиями.

Предназначены для студентов, обучающихся по направлению подготовки 11.03.02 Инфокоммуникационные технологии и системы связи.

Текст печатается в авторской редакции

Подписано печать 15.09. Формат 60x841/16.
Усл. печ. л. 3,55. Уч.-изд. 3,21 л. Тираж 100 экз. Заказ 285. Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94

1 Лабораторная работа №1 «Основы работы в Cisco Packet Tracer»

1.1 Цель работы

Изучение принципов работа в сетевом эмуляторе Cisco Packet Tracer для построения вычислительных сетей.

1.2 Краткие теоретические сведения

1.2.1 Обзор сетевого эмулятора Cisco Packet Tracer

Для освоения сетевых технологий и получения начального уровня навыков работы с сетевым оборудованием, фирмой Cisco разработан программный продукт Cisco Packet Tracer. **Пакет Cisco Packet Tracer – это инструмент, предоставляющий возможность имитировать как работу некоторого набора сетевых устройств** (маршрутизаторы, коммутаторы, точки беспроводного доступа, персональные компьютеры, сетевые принтеры, IP-телефоны и т. д.), **так и сетевое взаимодействие между ними** (распространение пакетов по сети). Так как данное программное обеспечение лишь имитирует функционирование реальных устройств и сетевое взаимодействие между ними, то существуют определенные ограничения и условности в работе поддерживаемых устройств и сетевых протоколов (доступны не все команды Cisco IOS). Вместе с тем Packet Tracer предоставляет пользователю определенную возможность изменения аппаратной части имитируемых устройств, например, для маршрутизаторов и коммутаторов существует возможность установки дополнительных сетевых модулей (HWIC, WIC и NM), а для компьютеров – выбора сетевого адаптера с поддержкой той или иной среды передачи. В зависимости от типа устройства программа предоставляет определенные возможности по его конфигурированию и соответствующий набор программного обеспечения, например, для маршрутизаторов и коммутаторов единственное доступное ПО – это Cisco IOS, для ПК – это командная строка, простейший web-браузер и т. п.

Cisco Packet Tracer поддерживает два режима работы: режим реального времени (Real-Time Mode) и имитационный (Simulation Mode). В первом режиме пользователь работает с сетью в реальном масштабе времени. Режим имитации позволяет пользователю «замораживать» сеть, наблюдать перемещение

данных по сети, изменение параметров IP-пакетов при прохождении их через сетевые устройства. Анализ событий, происходящих в сети, в этом режиме позволяет изучать алгоритмы функционирования сетевых устройств и протоколов и обнаруживать узкие места и проблемы. Помимо этого **с помощью Cisco Packet Tracer пользователь может разработать не только логическую организацию сети, но и ее физическую модель**, а, следовательно, получить навыки проектирования ее топологических связей. Схему компьютерной сети можно разрабатывать с учетом плана реально существующего здания или даже города, проектировать ее кабельную систему с учетом физических ограничений, таких как длина и тип прокладываемого кабеля или радиус зоны покрытия беспроводного сегмента сети [1].

1.2.2 Элементы пользовательского интерфейса

Главное окно программы Cisco Packet Tracer с основными элементами пользовательского интерфейса, обозначенными цифрами, представлено на рисунке 1.1.

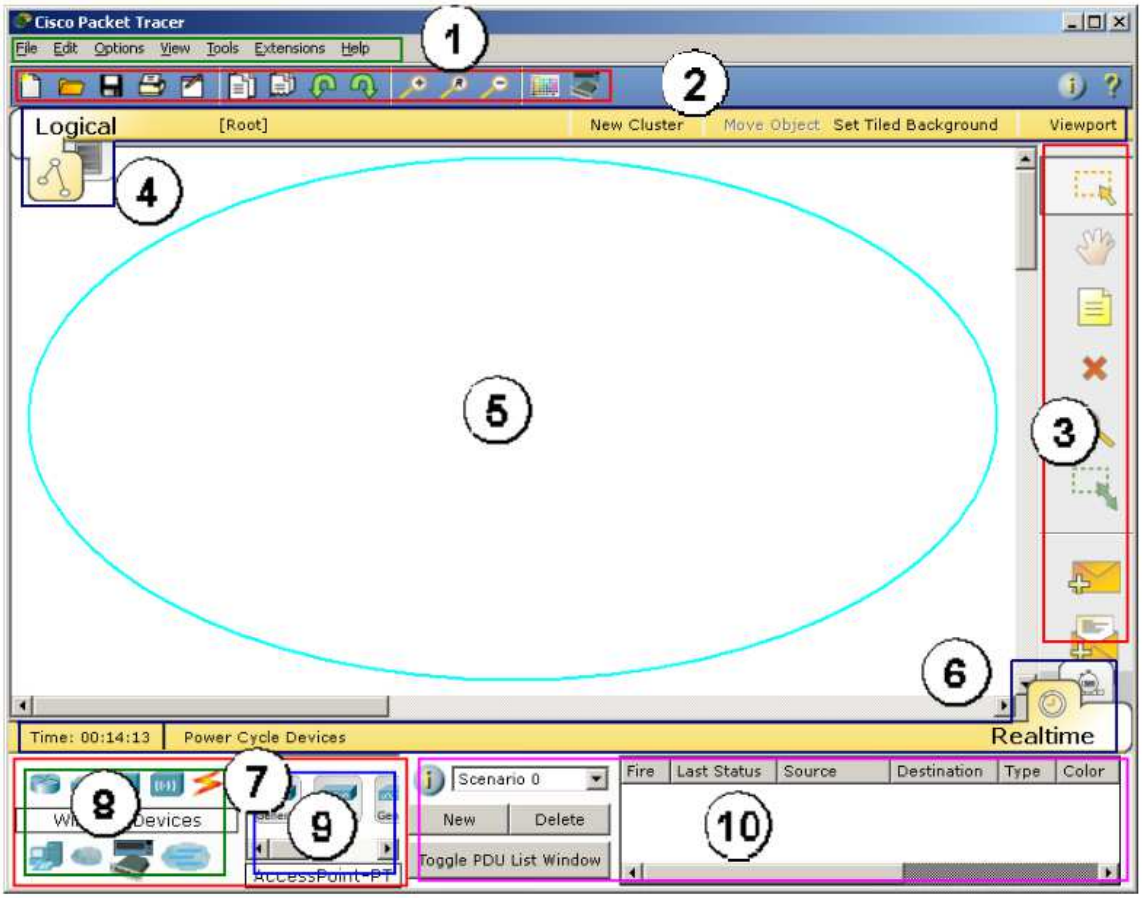

Рисунок 1.1 – Главное окно Cisco Packet Tracer

Пользовательский интерфейс программы включает в себя следующие элементы:

- **Menu Bar** (1) – меню с пунктами File, Edit, Options, View, Tools, Extensions, Help для доступа к функциям программы;

- **Main Tool Bar** (2) – панель инструментов, содержащая пиктограммы для доступа к часто используемым элементам меню;

- **Common Tools Bar** (3) – панель инструментов рабочей области: кнопки сверху вниз: Select, Move Layout, Place Note, Delete, Inspect, Resize Shape, Add Simple PDU и Add Complex PDU;

- **Logical/Physical Workspace and Navigation Bar** (4) – переключатель вида рабочей области: физический или логический. В зависимости от используемого вида на панели располагаются дополнительные кнопки: для логической схемы сети – кнопки для создания кластеров (New Cluster), позволяющих объединить устройства в один объект, и навигации между ними; для физического представления – кнопки, позволяющие создать новые объекты типа город, здание, серверная, и отобразить координатную сетку;

-**Workspace** (5) – основное рабочее пространство, в котором происходит создание сети, визуализация передачи сетевого трафика между устройствами и т. д.;

- **Realtime/Simulation Bar** (6) – переключатель между режимами Realtime и Simulation. В обоих режимах на соответствующей панели присутствуют часы, отображающие относительное время, и кнопка сброса питания (Power Cycle Devices). В режиме имитации добавляются кнопки управления сетевым трафиком (Play Controls): Back, Auto Capture/Play и Capture/Forward и кнопка Event List, позволяющая просматривать события в сети (отправку, получение пакетов и т. п.);

-**Network Component Box** (7) – область, в которой выбираются устройства и кабели для размещения их в рабочем пространстве. В ней в свою очередь находятся панели Device-Type Selectionи Device-Specific Selection;

- **Device-TypeSelectionBox**(8) – панель выбора типа устройств и соединений, содержащая доступные типы устройств и кабелей в Packet Tracer;

- **Device-Specific Selection Box**(9) – панель выбора устройства, используемая для выбора конкретного устройства или соединения, необходимого для создания сети в рабочем

пространстве. Вид панели изменяется в зависимости от выбранного типа устройств;

-**User Created Packet Window** (10) – окно управления сетевым трафиком пользовательского сценария[1].

1.2.3 Основные приемы создания схемы и конфигурированияустройств

Для создания логической схемы компьютерной сети необходимо добавить сетевые устройства в рабочую область. Чтобы это сделать, следует на панели выбора типа устройств (Device-Type Selection) указать категорию добавляемого устройства, затем пиктограмму необходимого устройства можно либо переместить с панели выбора конкретного устройства (Device-Specific Selection)в рабочую область, либо, выбрав ее, нажать левую кнопку мыши в рабочей области программы. На рисунке 1.2 приведен пример, когда в качестве добавляемых устройств выбраны маршрутизаторы (Routers).

Рисунок 1.2 – Список устройств в категории Routers

Для быстрого создания нескольких экземпляров одного и того же устройства следует, удерживая кнопку Ctrl, нажать на пиктограмму устройства в области выбора конкретного устройства и отпустить кнопку Ctrl. После этого нажатие левой кнопки мыши в рабочей области будет приводить к добавлению нового устройства или соединения. После того как устройства добавлены, их необходимо соединить друг с другом кабелем соответствующего типа. Выбор типа кабеля, осуществляется аналогично выбору устройства, используя категорию «соединения» (connections). Далее необходимо указать, какие два устройства будут соединены. При подключении кабеля программа попросит выбрать доступный порт. Существует специальный тип соединения, который автоматически выбирает тип кабеля, но с ним связаны определенные проблемы:

при соединении пользователь не может указать порты, а программа сама выбирает их согласно приоритетам, например, **если на маршрутизаторах есть Serial и Ethernet порты, то предпочтительным будет соединение через Serial порты**.

Как отмечалось ранее, у большинства добавляемых устройств может быть дополнительно сконфигурирована аппаратная часть. Кроме этого, Packet Tracer предоставляет интерфейс для конфигурирования сетевой части устройств (назначение IP-адресов, включение выключение интерфейсов, назначение ID VLAN и т. п.).

Для доступа к параметрам конфигурации устройства необходимо щелкнуть левой кнопкой мыши на его пиктограмме: появится окно с вкладками, содержимое которых зависит от типа выбранного устройства. Пример окна конфигурирования маршрутизатора приведен на рисунке 1.3.

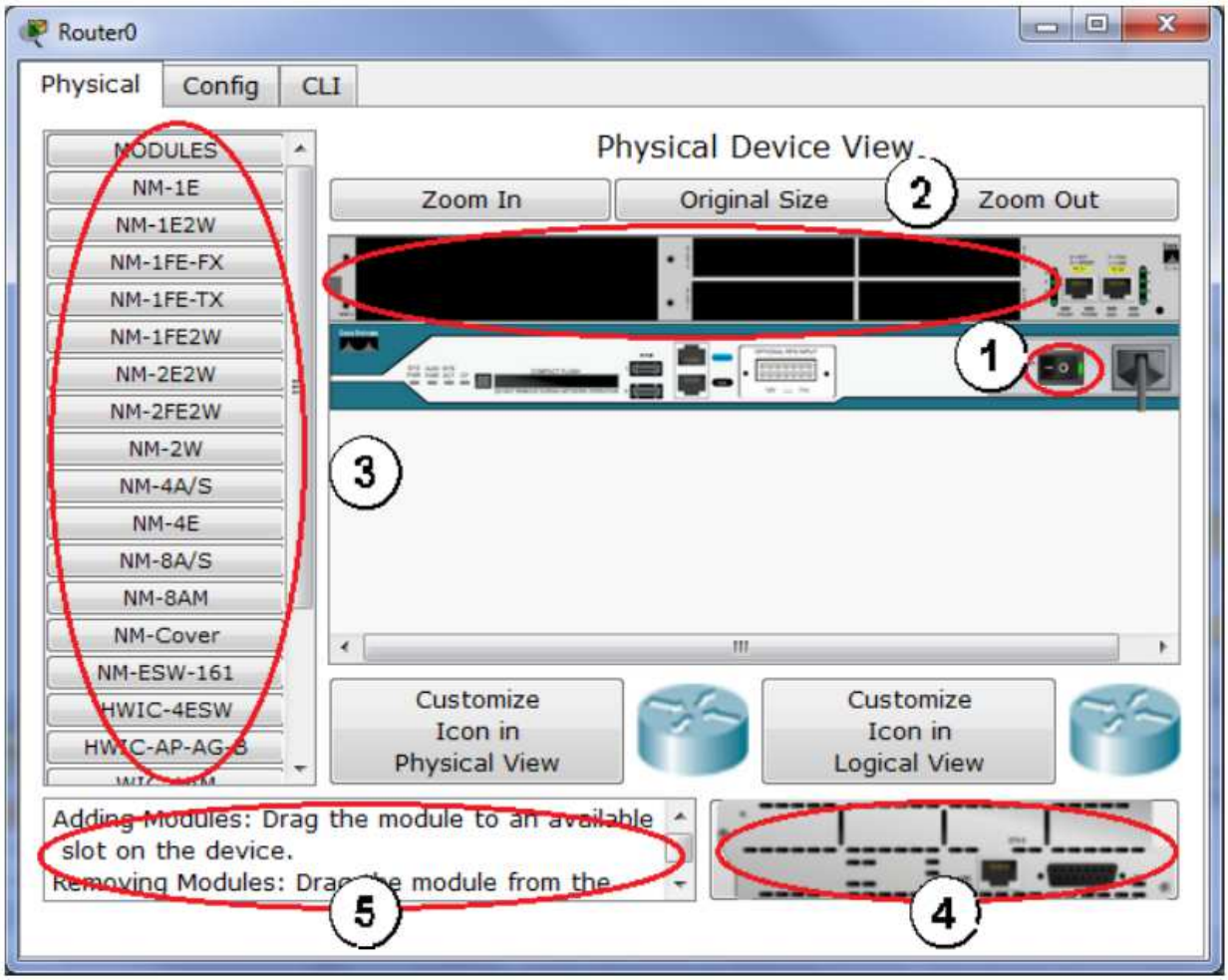

Рисунок 1.3 – Окно конфигурирования устройства, вкладка Physical

В зависимости от типа устройства могут присутствовать следующие вкладки: Physical, Config, CLI, Desktop. На вкладке Physical (см. рисунок 1.3) изображено устройство сослотами расширения, если таковые присутствуют в нем (2).Выключатель питания (1) позволяет включить или выключитьустройство. Если устройство включено, то нельзя изменить его аппаратную часть (добавить/удалить модули), если устройство выключено – нельзя получить доступ к вкладкам Config, CLI, Desktop. На вкладке может присутствовать список дополнительных модулей (3), поддерживаемых устройством. Если выбрать какой-либо модуль, то в нижней части вкладки будет отображено его краткое описание (5) и внешний вид (4). Для того чтобы добавить модуль в устройство, его необходимо переместить мышкой в соответствующий слот расширения из списка (3), либо из области внешнего вида модуля (4).

Вкладка Config позволяет настроить параметры функционирования устройства в целом, сетевых служб (DNS, DHCP, TFTP ит. п.) и его интерфейсов, не прибегая непосредственно к его штатным средствам настройки (например, для маршрутизатора). Пример вкладки Config для устройства Server0 приведен на рисунке 1.4:

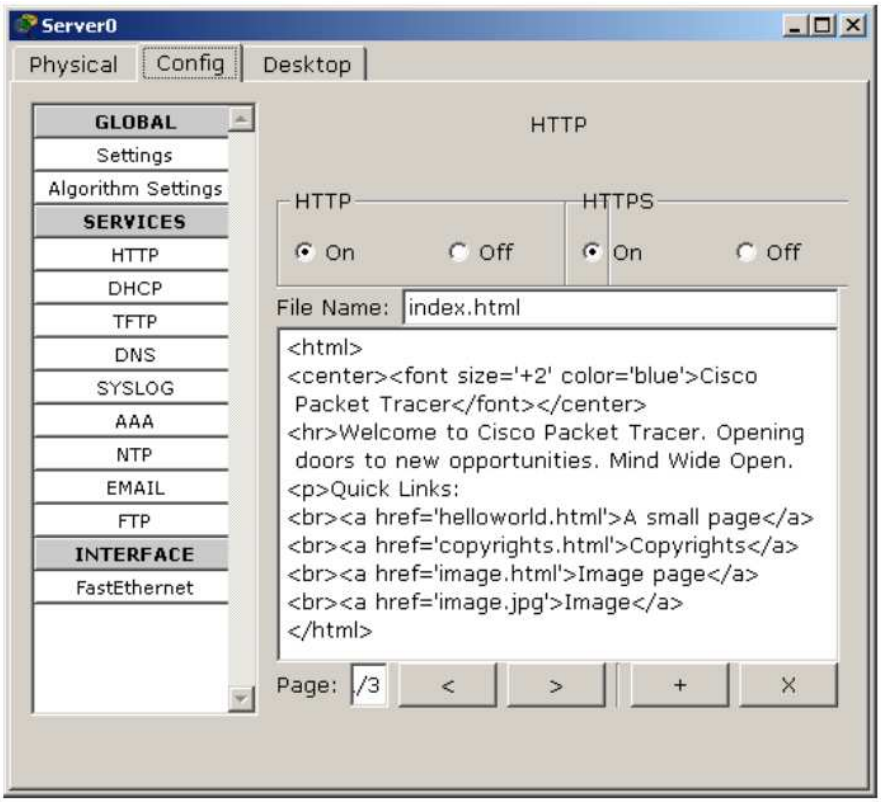

Рисунок 1.4 – Окно конфигурирования устройства, вкладка Config

Вкладка Desktop предоставляет доступ к программному обеспечению, доступному пользователю на конечном устройстве (PC, Server). На рисунке 1.5 приведен пример вкладки Desktop для компьютера PC.

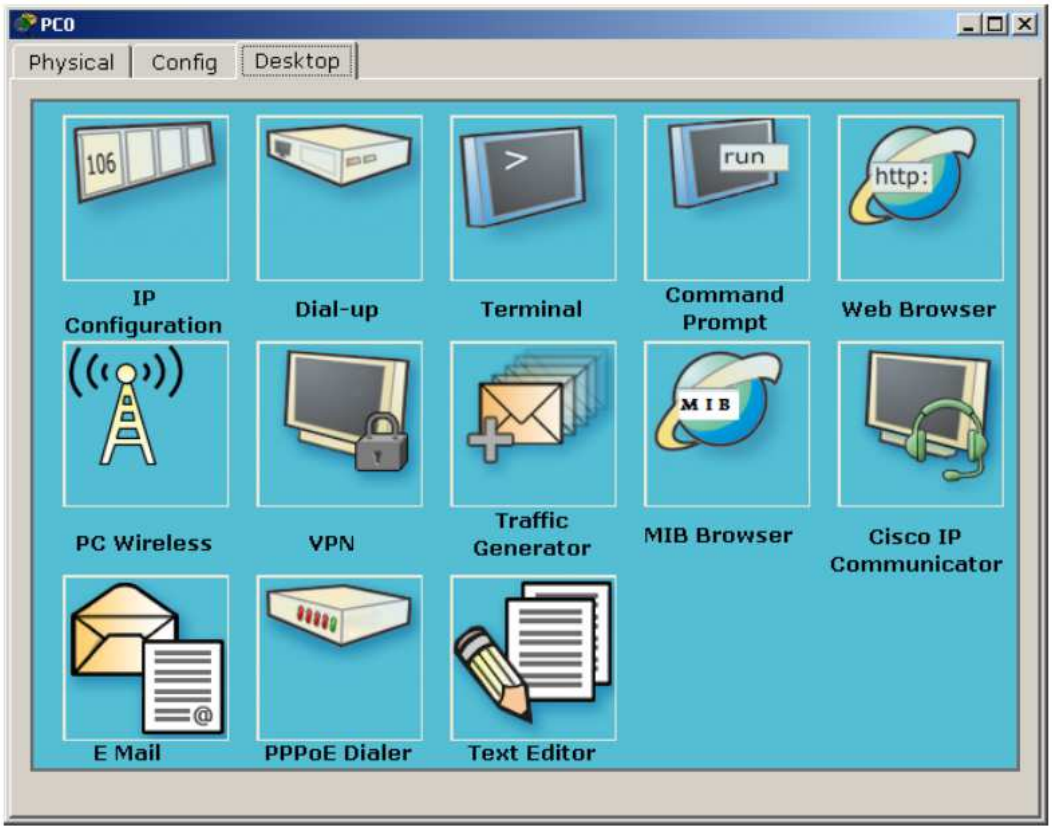

Рисунок 1.5 – ПО устройства, вкладка Desktop

Так как **данное ПО является имитацией реальных утилит ОС, оно имеет упрощенный интерфейс и ограниченный набор функций, в основном ориентированный на работу с сетью**, например, из17 команд доступных в командной строке (Command Prompt) только 4 не имеют отношения к работе с сетью. Для таких сетевых устройств как «Маршрутизатор» или«Коммутатор» вкладка Desktop заменена на CLI, предоставляющую доступ пользователя к командной строке Cisco IOS. Набор доступных команд и параметров уступает их количеству на реальном устройстве: присутствуют основные, часто используемые команды, либо позволяющие освоить основные моменты тех или иных концепций и принципов, заложенных в работу сетей, сетевых протоколов и устройств.

Сводную информацию (состояние портов, IP- и MAC- адреса и т. п.) об устройстве, находящемся в рабочей области, можно получить, наведя на него указатель мышки. Кнопка Inspect (увеличительное стекло) на панели инструментов рабочей области также выводит определенную информацию об устройстве: в зависимости от типа устройства контекстное меню содержит различное количество пунктов.

Для удаления лишних устройств из рабочей области программы используется клавиша Delete (Del) или кнопка Delete на панели инструментов рабочей области.

Более подробную информацию по работе с программой и описание ее пользовательского интерфейса можно найти в справочной системе, поставляемой в виде набора html-страниц [1].

1.3 Задание на лабораторную работу

1) Собрать сеть в соответствии с рисунком 1.6.

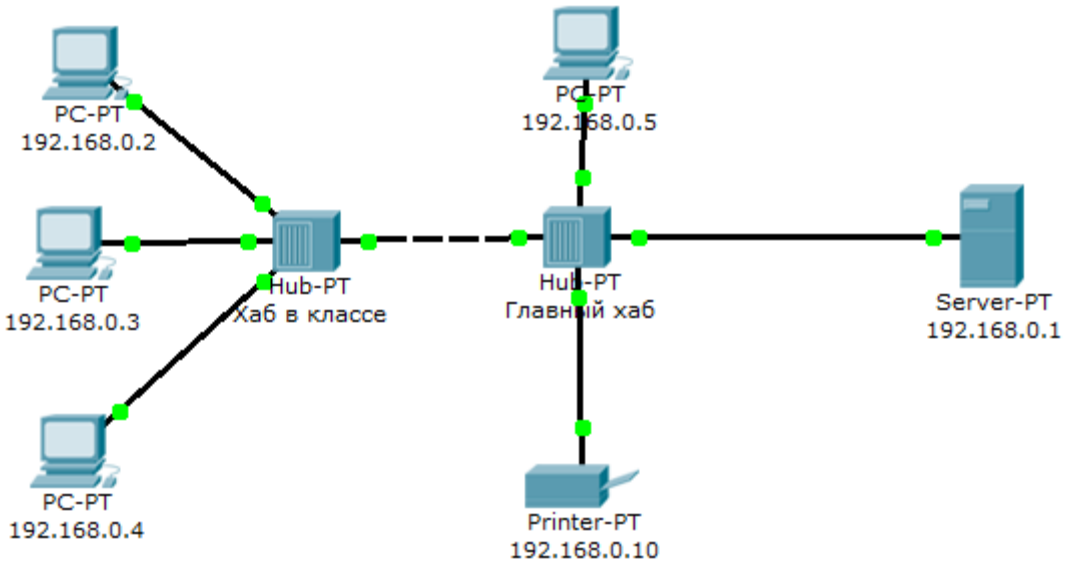

Рисунок 1.6 – Сеть для выполнения работы

2) Перейти в режим симуляции (Shift+S).

3) Отфильтровать пакеты с протоколом ICMP для исключения случайного трафика между узлами.

4) С одного из узлов пропинговать другой узел (выбрать далеко расположенные узлы, чтобы наглядней увидеть как будут проходить пакеты по сети в режиме симуляции).

5) Кликом по пакету сохранить диалоговое окно сподробной информацией о нем. Проследить инкапсуляцию данных по модели OSI.

6) Проследить прохождения пакета на каждом из этапов передачи данных с последующем сохранением результатов работы.

7) Заменить концентраторы (Hub) на коммутаторы 2-го уровня (Switch) и повторно выполнить п.2-6.

1.4 Примерный перечень вопросов для защиты лабораторной работы

1) Для чего используется режим симуляции?
2) Как просмотреть прохождение пакета по уровням модели OSI?
3) Можно ли определить причину того, что посланный в режиме симуляции пакет не дошел до адресата и на каком этапе произошел сбой работы сети?
4) Укажите в составе пакета IP адреса отправителя и получателя.
5) Как изменить фильтры списка событий?
6) Как в режиме симуляции определить, какие протоколы были задействованы в работе сети?
7) Как в режиме симуляции проследить изменение содержимого пакета при прохождении его по сети?
8) Перечислите основные возможности режима симуляции.

2 Лабораторная работа №2 «Первоначальная настройка сетевых устройств»

2.1 Цель работы

Изучение первоначальных настроек сетевых устройств в эмуляторе Cisco Packet Tracer.

2.2 Краткие теоретические сведения

2.2.1 Способы подключения к сетевым устройствам

Сетевые устройства, как правило, **настраиваются в командной строке ОС Cisco IOS. Подсоединение к ним осуществляется по протоколу Telnet на IP-адрес любого из его сетевых интерфейсов или с помощью любой терминальной программы через последовательный порт компьютера, связанный с консольным портом устройства** (рисунок 2.1).

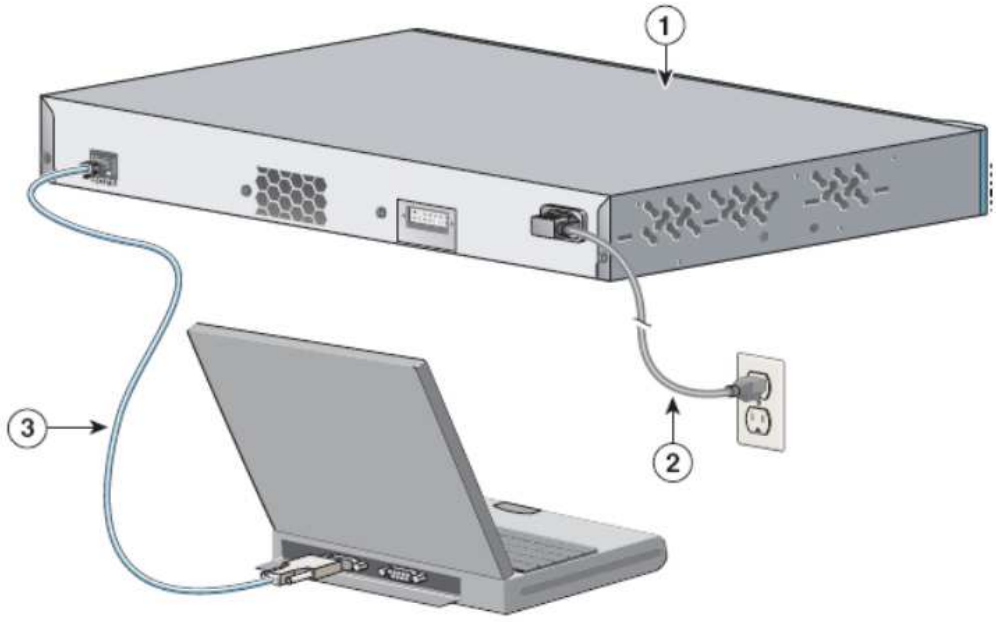

Рисунок 2.1 – Подключение по консольному кабелю

На рисунке 2.1 изображена схема подключения по консольному порту: на тыльной стороне коммутатора (1) расположены силовой разъем для подключения шнура питания (2) и консольный порт (3), обеспечивающий подключение к COM-порту компьютера администратора посредством кабеля RJ-45-to-DB-9.

Последний способ предпочтительнее, потому что в процессе настройки оборудования могут измениться параметры физического порта или административного IP-интерфейса, что приведет к потере соединения, установленного по протоколу Telnet.

Следует иметь в виду, что аварийное отключение консоли не регистрируется оборудованием, и сеанс остается в том состоянии, в котором находился на момент отключения. При повторном подключении пользователь окажется в том же контексте (если только не сработал автоматический выход в контекст пользователя по таймеру неактивности). Напротив, при разрыве Telnet-соединения коммутатор закрывает сеанс работы [1].

Для конфигурирования сетевых устройств в консольном режиме может использоваться программа HyperTerminal, входящая в состав стандартных программ ОС Windows XP, **или сторонние программы, например, Putty**, если используется ОС Windows более поздних версий или другая операционная система. Синтаксис команд, вводимых для конфигурирования, несколько различается у различных производителей, однако общий смысл их остается неизменным [2].

2.2.2 Контексты командной строки

В операционной системе Cisco IOS имеются два основных пользовательских режима для администрирования коммутатора и несколько других режимов, позволяющих контролировать конфигурацию устройства. В дополнение к различным режимам программное обеспечение Cisco IOS обеспечивает такие функции, как интерактивная справка и редактирование командной строки, которые позволяют взаимодействовать с коммутатором в административных целях.

1) Пользовательский EXEC-режим.

Switch>

Пользователям предоставляется возможность подключаться к коммутатору посредством консольного порта или Telnet-сеанса.

Стандартно при первоначальном доступе к коммутатору пользователь входит в пользовательский EXEC-режим (user EXEC), в котором предоставляется ограниченный набор команд. При подключении к коммутатору может потребоваться пароль пользовательского уровня.

2) Привилегированный EXEC-режим.

Switch>enable

Switch#

После того как пользователь получает доступ к пользовательскому EXEC-режиму, можно применить команду enable для входа в привилегированный EXEC-режим (privilegedEXEC), который предоставляет полный доступ ко всем командам ОС. Для того чтобы покинуть привилегированный EXEC-режим, используется команда disable (возврат в пользовательский режим) или exit.

3) Конфигурационный режим.

Switch#configure terminal

Switch(config)#

Войти в конфигурационный режим можно из привилегированного EXEC-режима. В режиме конфигурации можно вводить любые команды для настройки функций коммутатора, которые доступны в программном образе операционной системы IOS. Любая команда конфигурации вступает в действие немедленно после ввода (а не после возврата в контекст администратора).

Конфигурационный режим организован иерархически. Режим глобальной конфигурации (globalconfigurationmode) содержит команды, которые влияют на коммутатор в целом. В режиме конфигурирования интерфейса (interfaceconfigurationmode) администратору предоставляются команды, позволяющие настраивать интерфейсы коммутатора в зависимости от настраиваемого ресурса.

Для перехода со специфического уровня конфигурирования наболее общий вводится команда exit. Для того чтобы покинуть режим глобальной конфигурации и вернуться в привилегированный EXEC-режим необходимо ввести команду exit. Для того чтобы покинуть любой конфигурационный режим и вернуться в привилегированный EXEC-режим, применяется команда end или комбинация клавиш [Ctrl]+[z].

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

Switch(config)# – глобальный;

Switch(config-if)# – интерфейса;

Switch(config-line)# – терминальной линии.

4) Режим конфигурирования базы данных VLAN-сетей (устаревший, использовать не рекомендуется).

Switch# vlan data base

Switch(vlan)#

Перейти в указанный режим можно из привилегированного EXEC-режима. После ввода команды появится приглашение режима конфигурирования базы данных VLAN-сетей (vlan data base mode). В данном режиме с помощью команд vlan (и/или vtp) конфигурируются и модифицируются VLAN- и VTP-параметры.

После внесения изменений в базу данных VLAN они не вступят в действие до тех пор, пока не будет введена команда apply для активизации изменений в базе данных или команда exit, которая позволяет активизировать изменения и покинуть режим. Команда abort отменяет какие-либо сделанные изменения в базе данных и позволяет покинуть рассматриваемый режим конфигурирования.

Кроме того, существует возможность просмотреть текущее состояние базы данных и предполагаемые изменения, используя команды группы show.

Необходимо запомнить вид приглашений командной строки (изображены в прямоугольнках) во всех вышеуказанных контекстах и команды перехода из контекста в контекст (изображены над стрелками), это поможет при настройке коммутатора (рисунок 2.2) [1].

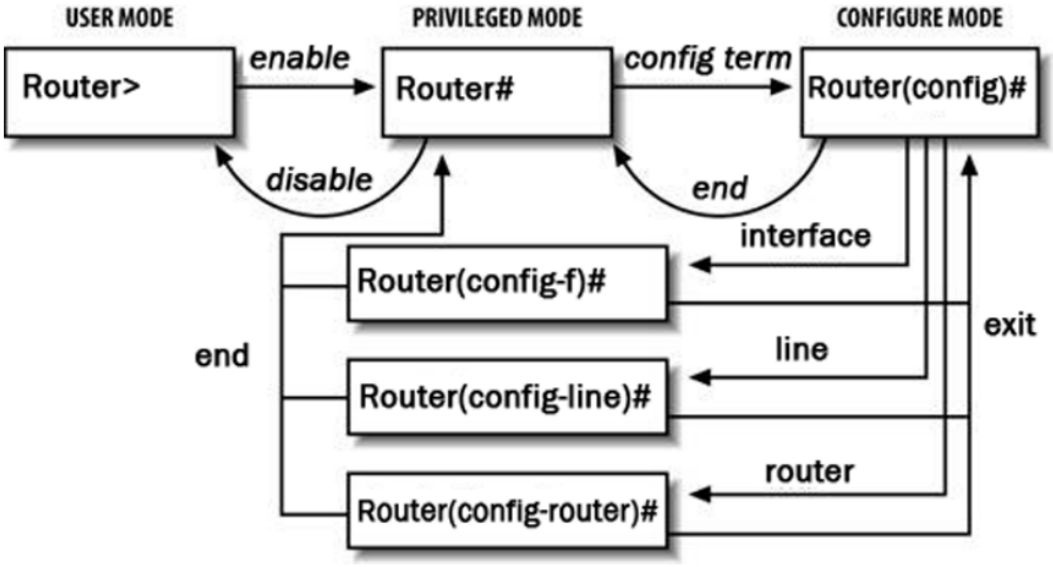

Рисунок 2.2 – Схема контекстов Cisco IOS (пример для маршрутизаторов)

2.2.3 Конфигурирование паролей на подключение к устройству

Пароли обеспечивают некоторый уровень защиты коммутатора, предотвращающий неавторизованное подключение к нему**. Коммутаторы Catalyst стандартно имеют два уровня парольной защиты: пользовательский и привилегированный**. Для обеспечения защиты устройства следует применять аутентификацию пользователя с использованием локальной базы коммутатора и шифрование паролей.

Пароль уровня пользователя предотвращает доступ неавторзованных лиц к интерфейсу командной строки (CLI) из Telnet- или консольного сеанса. Он настраивается для каждой линии подключения отдельно с помощью команд password, параметром которой является устанавливаемый пароль, и login без параметров.

Команда login обеспечивает процесс аутентификации пользователя и является обязательной для линий подключенияIOS-коммутаторов. До тех пор, пока пароль не будет установлен или в конфигурации линии будет отсутствовать команда login,подключение по Telnet невозможно. Выбор той или иной линии для ее конфигурирования осуществляется с помощью команды режима глобального конфигурирования:

Switch(config)# linecon 0 – для консольной линии,

Switch(config)# linevty 0 4 – для линий виртуального терминала в диапазоне номеров с 0 по 4.

Пароль привилегированного режима предотвращает доступнее авторизованных лиц к соответствующему режиму, в котором могут вноситься изменения в конфигурацию коммутатора и осуществляться другие функции администрирования. Он **задается помощью команды enable secret, обеспечивающей его шифрование, устаревшая команда enable password не шифрует пароль** и оставлена для совместимости с программным обеспечением ранних версий, причем во второй команде пароль должен отличаться от устанавливаемого в первой.

Для того чтобы пароли не хранились в файле конфигурации в открытом виде, можно использовать встроенную службу

шифрования, но учтите, что она не обеспечивает их шифрование, а призвана лишь усложнить чтение паролей с экрана. Указанная служба запускается командой:

Service password-encryption.

Как упоминалось ранее, предпочтительнее применять аутентификацию пользователя с использованием локальной базы данных коммутатора, для чего сначала создаются записи локальной базы пользователей с помощью команды:

Switch(config)#username<имя>privilege<уровень>secret<пароль>.

Затем для каждой линии подключения к коммутатору указывается команда login с параметром локальной аутентификации [1]:

Switch(config-line)#login local.

2.2.4 Настройка интерфейсов

Для перехода в режим настройки необходимого интерфейса следует, находясь в глобальном режиме, выполнить команду:

lab1(config)#interface <имя_интерфейса>.

По умолчанию все интерфейсы маршрутизатора выключены. **Интерфейс включается** командой:

lab1(config-if)#no shutdown.

Работоспособность настроек физического и канального уровней можно проверить командой в контексте администратора:

lab1#show interface <имя_интерфейса>.

Сообщения об изменении состояния физического и канального уровней любого интерфейса выводятся маршрутизатором на консоль. **Команда show interface также выводит сведения об используемом протоколе канального уровня, IP-адресе и статистику отправленных и полученных данных и ошибок**.

Настройка IP-адреса интерфейса производится командой:

lab1(config-if)#ip address <адрес><маска>.

Подробная информация о параметрах протокола IP доступна в контексте администратора по команде:

lab1#show ip interface <имя_интерфейса>.

Краткая сводная таблица состояний IP-интерфейсов[1]:

lab1#show ip interface brief.

2.3 Задание на лабораторную работу

1) Запустить Cisco Packet Tracer.
2) Собрать схему в соответствии с рисунком 2.3.

Рисунок 2.3 – Подключение по консольному кабелю

3) На компьютере Laptop 0 в закладке Desktop запустить приложение Terminal с параметрами по умолчанию. Нажмите [Enter] для входа в пользовательский режим.
4) Перейти в привилегированный режим.
5) Перейти в режим глобального конфигурирования и обратно в привилегированный.
6) Осуществить переход в представленные контексты Cisco IOS.
7) Просмотреть список команд каждого контекста с помощью команды ?.
8) Выполнить в привилегированном EXEC-режиме несколько команд группы show, используя сокращенную запись команд.
9) Выполнить в режиме глобального конфигурирования несколько команд группы show, используя команду do.
10) В текущей конфигурации найти команды, устанавливающие пароли на линии con и vty.
11) Установить пароль console для линии con0.
12) Выйти из сеанса консоли с помощью команды logout и войти в новый сеанс, используя введенные данные аутентификации.

13) В текущей конфигурации найти команды, устанавливающие пароль для входа в привилегированный режим.

14) Запустить службу шифрования паролей и в текущей конфигурации найти команды, устанавливающие пароли.

15) Создать запись в локальной базе данных аутентификации о пользователе admin с уровнем привилегий 0 и секретным паролем cisco.

16) Настроить линии con0 и vty0 – vty4 на использование локальной аутентификации. Для отмены старых паролей можно использовать команду: Switch(config-line)#nopassword.

17) Выйти из сеанса консоли и войти в новый сеанс, используя введенные данные аутентификации.

18) В текущей конфигурации найти команды, устанавливающие действующие на коммутаторе пароли.

19) Сохранить текущую конфигурацию.

Примечание: каждая итерация должна сопровождаться скриншотом (-ами).

2.4 Примерный перечень вопросов для защиты лабораторной работы

1) Какие существуют способы подключения к сетевому оборудованию для управления им?

2) Какие существуют контексты командной строки IOS и каковы возможности администрирования каждого из них?

3) Какой командой выводится сводная таблица состояний IP- интерфейсов?

4) Какова последовательность ввода команд в сетевых устройствах Cisco Systems для настройки IP-адреса на интерфейсе?

5) Какую команду предпочтительней использовать при создании пароля на коммутаторах?

6) Какие программные средства используется на ОС Windowsдля доступа к сетевому устройству по протоколу Telnet?

7) Какой процесс запускает команда login на сетевых устройствах?

3 Лабораторная работа №3 «Блокировка резервных портов (STP)»

3.1 Цель работы

Исследование протокола обнаружения и предотвращения формирования мостовых петель второго уровня STP.

3.2 Краткие теоретические сведения

Протокол STP, основанный на стандарте мостового протокола IEEE 802.1D, **обнаруживает и предотвращает формирование мостовых петель второго уровня**. Параллельные маршруты в конфигурации сети могут существовать, но передача кадров допускается только по одному из них.

Коммутаторы сети запускают по одному экземпляру STP на каждую VLAN-сеть с помощью алгоритма PVST (Per-VLAN Spanning Tree – отдельные экземпляры распределенного связующего дерева для разных сетей VLAN). PVST-алгоритм требует использования между коммутаторами магистральных ISL-каналов.

Функционирование алгоритма STP и его конфигурирование на коммутаторах рассмотрим на примере упрощенной схемы сети и только для стандартной VLAN-сети с номером 1.

Так как поддержка протокола связующего дерева включена по умолчанию, то по истечении некоторого времени, необходимого для отработки алгоритма STP, на графе Вашей сети будет построено связующее дерево и, несмотря на присутствующие физические петли, между любыми узлами в сети будет существовать единственный маршрут. Например, в сети, изображенной на рисунке 3.1, между узлами PC0 и PC1 существует только один активный маршрут – через коммутаторы с номерами 0, 1 и 2 (в Packet Tracer заблокированные порты коммутаторов изображаются светло-коричневыми точками).

Для вывода информации о состоянии STP используются следующие команды привилегированного режима:

Switch#show spanning-tree active – наактивных интерфейсах;

Switch#show spanning-tree detail – на всех интерфейсах;

Switch#show spanning-tree interface int-id –на указанном интерфейсе;

Switch#show spanning-tree vlan vlan-id – в указанной VLAN-сети;

Switch#showspanning-treesummary – вывод общей информации о состоянии STP

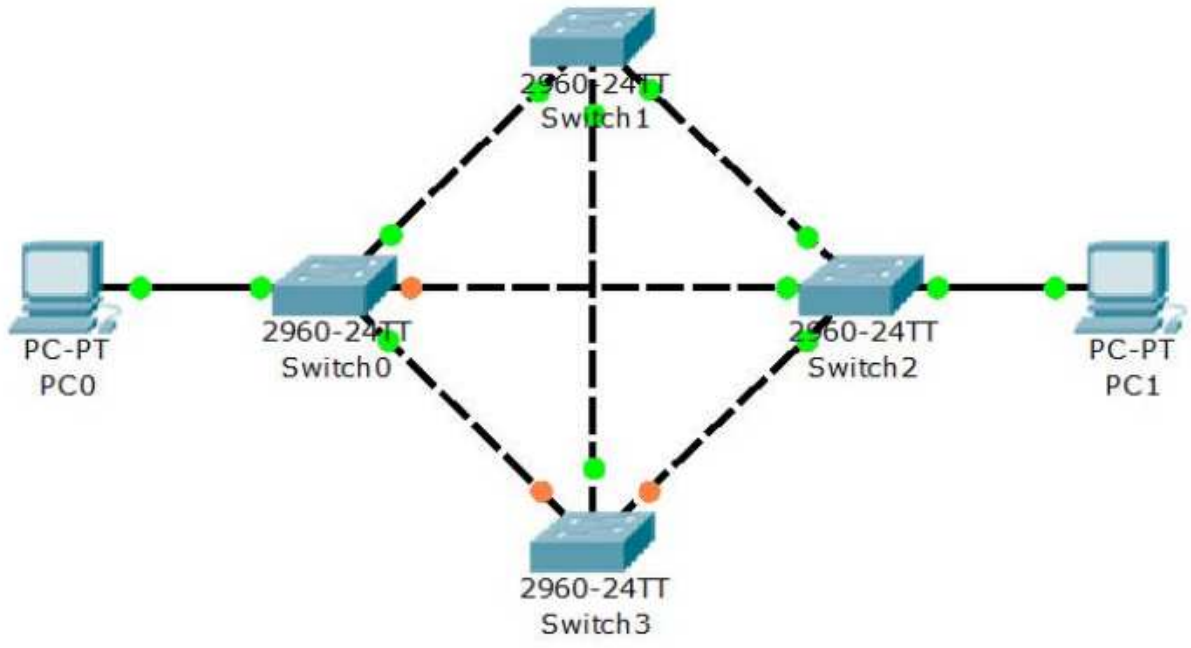

Рисунок 3.1 – Схема сети с избыточными линиями связи

Для конфигурирования протокола STP используются следующие команды режима глобального конфигурирования:

Switch(config)#spanning-treevlanvlan-id –включение функции поддержки протокола STP (с префиксом no –отключение);

Switch(config)#spanning-treemode {pvst |rapid-pvst} – выбор режима функционирования протокола;

Switch(config)#spanning-treevlanvlan-idroot {primary | secondary} – выбор основного (primary) идополнительного (secondary) корневого коммутатора;

Switch(config)#spanning-treevlanvlan-idprioritypriority – установка приоритета коммутатора, допустимые значения параметра **priority** – 4096; 8192; 12288; 16384;20480; 24576; 28672; 32768; 36864; 40960; 45056; 49152; 53248;57344 и 61440 (по умолчанию – 32768).

Кроме приведенных есть и другие команды режимов глобального конфигурирования и конфигурирования интерфейсов, позволяющие более тонко настраивать функционирование

протоколаSTP в сети, но их изучение выходит за рамки данного пособия[1].

3.3 Задание на лабораторную работу

1) Создать схему сети, изображенную на рисунке 3.1 (использовать интерфейсы Fast Ethernet).

2) Определить активное связующее дерево STP в Вашей сети.

3) Выбрать Switch3 дополнительным корневым коммутатором для расчета связующего дерева. Определить активное связующее дерево STP в сети.

4) Выбрать Switch1 основным корневым коммутатором для расчета связующего дерева. Определить активное связующее дерево STP в сети.

5) Установить приоритет для расчета связующего дерева на коммутаторе Switch2 – 20480. Определить активное связующее дерево STP в сети.

6) Удалить линию связи между коммутаторами Switch0и Switch2. Определить приблизительное время расчет адерева по алгоритму PVST. Определить активное связующее дерево STP в сети.

7) Восстановить линию связи между коммутаторами Switch0и Switch2. Установить на всех коммутаторах режим Rapid-PVST.

8) Удалить линию между коммутаторами Switch0 и Switch2.Определить приблизительное время расчета дерева по алгоритму Rapid-PVST.

Примечание: каждая итерация должна сопровождаться скриншотом (-ами).

3.4 Примерный перечень вопросов для защиты лабораторной работы

1) Для чего необходим протокол STP?

2) Может ли администратор каким-либо образом повлиять на расчет покрывающего дерева в сети?

3) Какой командой осуществляется выбор режима функционирования протокола?

4) Какие команды используются для вывода информации о состоянии STP?

5) Какой командой осуществляется отключение функции поддержки протокола STP?

4 Лабораторная работа №4 «Организация виртуальных сетей (VLAN)»

4.1 Цель работы

Исследование способов построения виртуальных локальных сетей (VLAN).

4.2 Краткие теоретические сведения

4.2.1 Конфигурирование статических VLAN

Сети VLAN – это определенные внутри коммутаторов широковещательные домены, позволяющие внутри устройства второго уровня управлять широковещательными, групповыми, одноадресными рассылками, а также одноадресными рассылками с неизвестным получателем. Каждая сеть VLAN создается в локальной базе данных используемого коммутатора. Если в коммутаторе отсутствуют сведения о какой-либо VLAN-сети, то он не может передавать трафик для этой сети VLAN через свои порты. **VLAN-сети создаются по номерам, при этом существует два диапазона, пригодных для использования VLAN-номеров (обычный диапазон 1 ÷ 1000 и расширенный – 1025 ÷ 4096).** При создании VLAN-сети можно также назначить ей определенные атрибуты, такие как имя, тип и операционное состояние. По умолчанию на коммутаторе существуют предопределенные VLAN – их нельзя удалить или переименовать. **Все физические порты устройства по умолчанию находятся в VLAN1**, называемой стандартной сетью VLAN (defaultVLAN), поэтому ее в целях безопасности и не рекомендуют использовать. **Для вывода краткой информации о VLAN служит команда:**

Switch#showvlanbrief.

Процесс создания статических VLAN-сетей включает в себя несколько этапов. Во-первых, необходимо в режиме глобального конфигурирования (рекомендуется вместо режима конфигурирования базы данных VLAN) **установить протокол VTP в прозрачный режим функционирования:**

Switch#configure terminal

Switch(config)#vtp mode transparent.

Во-вторых, **создать собственно сеть VLAN** и по желанию **указать ее имя с помощью последовательности команд:**

Switch(config)#vlan <номер>

Switch(config-vlan)#name <имя>

Switch(config-vlan)#end.

В-третьих, необходимо **назначить в созданные VLAN-сети физические порты коммутатора**, для чего перейти в режим конфигурирования выбранного интерфейса, а затем перевести его в режим доступа и назначить его в соответствующую VLAN-сеть. Например, с помощью следующих команд порт FastEthernet 0/5 назначается в VLAN с номером 50:

Switch#configure terminal

Switch(config)#interface FastEthernet 0/5

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 50.

Для выполнения некоторой последовательности команд одновременно для нескольких портов коммутатора можно использовать **выбор диапазона портов, осуществляемый с помощью команды:**

Switch(config)#interface range FastEthernet 0/5 - 8

Состояние интерфейсов коммутатора на канальном и сетевом уровнях можно отобразить с помощью следующих команд соответственно (после параметра interface можно указать имя интерфейса для вывода информации только о его состоянии) [1]:

Switch#show interface

Switch#show interface switchport.

4.2.2 Конфигурирование IP –адреса административного управления

IP-адреса используются в коммутаторах второго уровня только в целях администрирования. Данный этап не является обязательным для функционирования коммутатора. В случае, если IP-адрес не был задан, единственным способом управления коммутатором является консольное соединение. **Для конфигурирования IP-адреса используется последовательность команд:**

Switch(config)#interfacevlan<номер>

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

Switch(config-if)#exit.

Для просмотра информации об административном интерфейсеможно использовать следующие команды:

Switch#show interface vlan <номер>

Switch#show ip interface vlan <номер>.

Для просмотра краткой информации обо всех интерфейсахможно использовать команду [1]:

Switch#show ip interface brief.

4.2.3 Конфигурирование магистральных (транковых) линий

Дело в том, что VLAN-сети являются локальными в базе данных каждого коммутатора, и информация о принадлежности узловк ним не передается между коммутаторами. **Магистральные каналы (trunk links – транковые линии) обеспечивают VLAN-идентификацию для кадров, перемещающихся между коммутаторами сети.** В коммутаторах фирмы Cisco имеются два механизма Ethernet-транкинга: протокол ISL и стандарт IEEE 802.1Q. Некоторые типы коммутаторов способны согласовывать параметры магистральных каналов.

Магистральные каналы стандартно транспортируют трафик от всех VLAN-сетей к коммутатору и от него, но могут быть настроены наподдержку трафика только определенной VLAN-сети.

Для создания транка между коммутаторами необходимо выполнить для каждого интерфейса создаваемого канала описанную ниже последовательность действий (один из вариантов):

-**перевести интерфейс в режим trunk с помощью команды:**

Switch(config-if)#switchport mode trunk;

- указать метод инкапсуляции, используемый в канале, с помощью команды:

Switch(config-if)#switchport trunk encapsulation <negotiate|isl|dotlQ>.

Для некоторых коммутаторов стандартным методом инкапсуляции является ISL, используемый нами Catalyst-2960 поддерживает только лишь IEEE 802.1Q, поэтому данная команда в

его ОС отсутствует, а при конфигурировании, например, Catalyst-3560 она необходима;

-**удалить неиспользуемые VLAN-сети** из магистрального канала вручную (необязательно, но рекомендуется) с помощью команды:

Switch(config-if)#switchporttrunkallowedvlanremove<список>;

- в случае необходимости, **добавить новые VLAN-сети** в магистральный канал с помощью команды:

Switch(config-if)#switchport trunk allowed vlan add <список>.

Для отображения информации о магистральных каналах используется команда привилегированного режима[1]:

Switch#show interfaces trunk.

4.3 Задание на лабораторную работу

1) Вывести на экран информацию о VLAN, существующих в коммутаторе по умолчанию.
2) Установить протокол VTP в прозрачный режим функционирования.
3) Создать две виртуальных локальных сети: с номерами 10 и 20 без имени и одну с номером 99 и именем – Administration.
4) Вывести на экран информацию о VLAN, существующих в коммутаторе.
5) Назначить порт fa0/24 в VLAN с именем Administration.
6) Назначить порты fa0/1 – fa0/10 в VLAN 10.
7) Назначить порты fa0/11 – fa0/20 в VLAN 20.
8) Сохранить текущую конфигурацию.
9) Вывести на экран информацию о VLAN, существующих в коммутаторе.
10) Добавить в схему сети компьютеры PC0–PC4, подсоединить их к соответствующим портам коммутатора, назначить им IP-адреса согласно схеме, приведенной на рисунке 4.1.

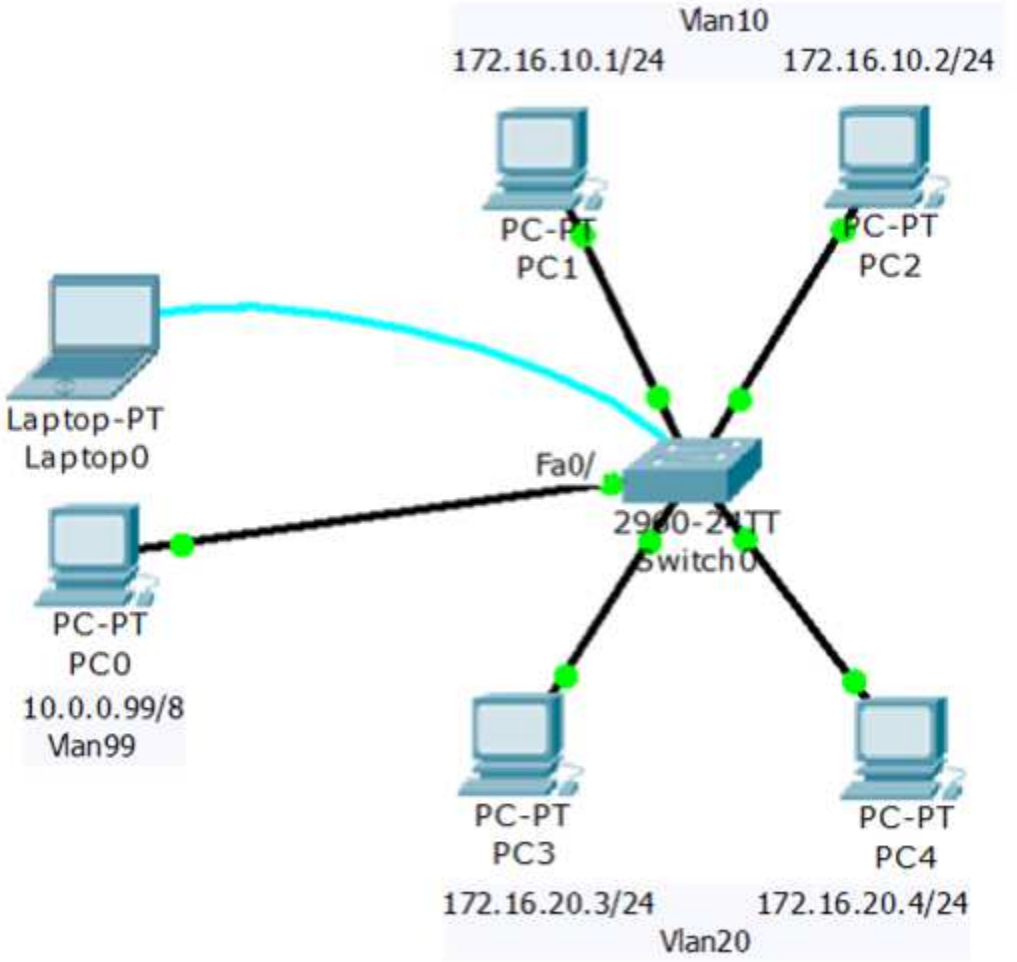

Рисунок 4.1 -- Схема сети с VLAN99, VLAN10 и VLAN20

11) Используя приведенные команды, изучите параметры функционирования портов коммутатора, выясните различия в режимах работы портов, к которым подключены и не подключены компьютеры, а также портов, которые не настраивались Вами.

12) С помощью команды ping убедитесь, что в рамках VLAN-сетей взаимодействие между компьютерами возможно, а между сетями нет.

13) Назначить административный IP-адрес 10.0.0.10/8 интерфейсу vlan99.

14) Сохранить текущую конфигурацию.

15) Используя команду ping, убедитесь, что PC0 может взаимодействовать с коммутатором.

16) Используя команду telnet, подключитесь с PC0 к коммутатору.

17) Вывести информацию о настройках административного интерфейса vlan99.

18) Вывести информацию об IP-интерфейсах коммутатора.

19) Справа от имеющейся схемы создать сеть, изображенную на рисунке 4.2. Интерфейсы коммутатора FastEthernet с номерами с 1 по 5 назначить в VLAN10, с 6 по 10 –в VLAN20 и подключить Hub0 к Fa0/1, Server0 – к Fa0/2, Server1 – к Fa0/6.

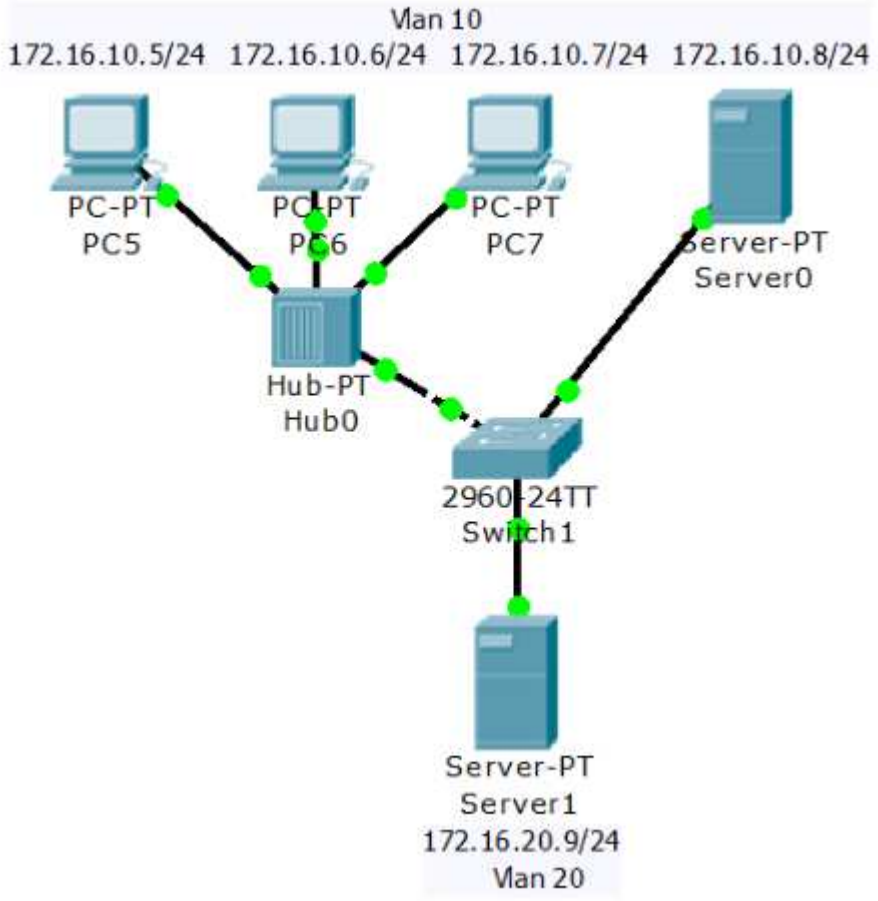

Рисунок 4.2 – Расширение имеющейся сети

20) Соединить Switch0 и Switch1 друг с другом, используя для этого их интерфейсы GigabitEthernet1/1. У Вас должна получиться схема сети, представленная на рисунке 4.3.

21) Убедиться в том, что взаимодействие узлов, принадлежащих одной и той же VLAN-сети, невозможно, если они подключены к разным коммутаторам.

22) Перевести интерфейсы GigabitEthernet1/1 обоих коммутаторов в режим trunk.

23) Удалить неиспользуемые VLAN-сети из магистрального канала.

24) Вывести информацию о магистральных каналах коммутаторов.

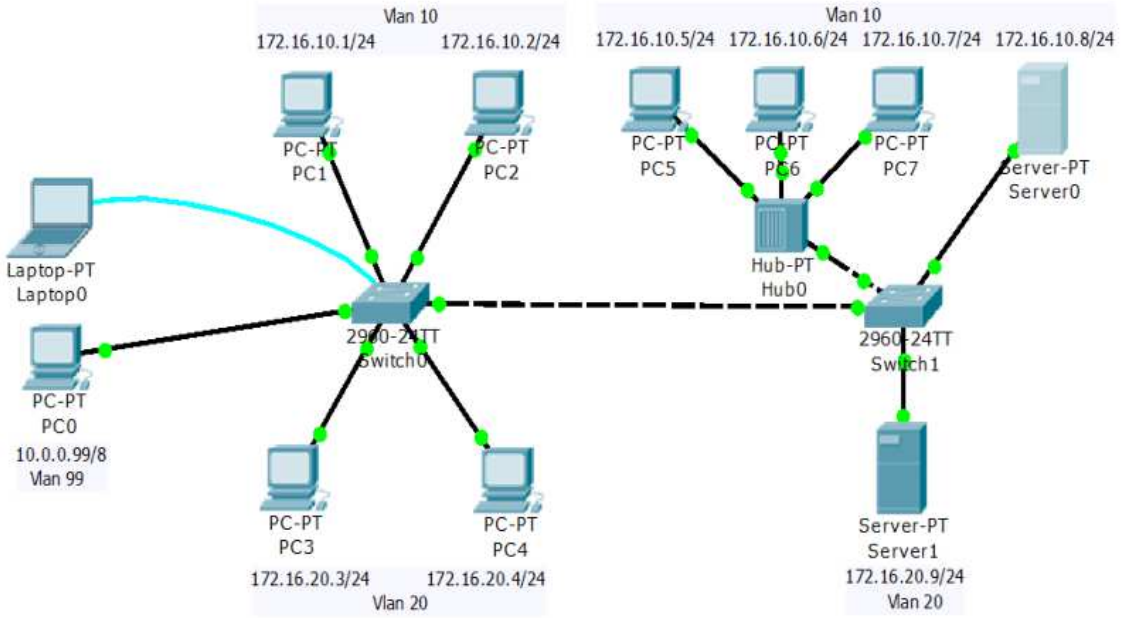

Рисунок 4.3 – Схема сети с магистральным кабелем

4.4 Примерный перечень вопросов для защиты лабораторной работы

1) Для чего используются виртуальные локальные сети (VLAN)?

2)Какой командой устанавливается протокол VTP в прозрачный режим функционирования?

3) В каком стандарте описана технология VLAN?

4) Каковы причины разделения единой сети на виртуальные?

5) Какой порт называется тэгированным?

6) Какой командой можно перевести интерфейс в режим trunk?

7) Какие команды можно использовать для просмотра информации об административном интерфейсе?

5 Лабораторная работа №5 «Статическая маршрутизация»

5.1 Цель работы

Изучение принципов построения вычислительных сетей с использованием маршрутизаторов со статической маршрутизацией.

5.2 Краткие теоретические сведения

При небольшом количестве подсетей, как правило, **используется статическая маршрутизация**. Статические маршруты не меняются самим маршрутизатором. Данный тип маршрутизации потребляет мало вычислительных ресурсов и полезна в сетях, которые не имеют нескольких путей к адресату назначения. Если от маршрутизатора к маршрутизатору есть только один путь, то часто используют статическую маршрутизацию.

Рассмотрим типичные примеры конфигурирования сети с использованием статической маршрутизации. Предположим, что структура сети имеет вид, показанный на рисунке 5.1.

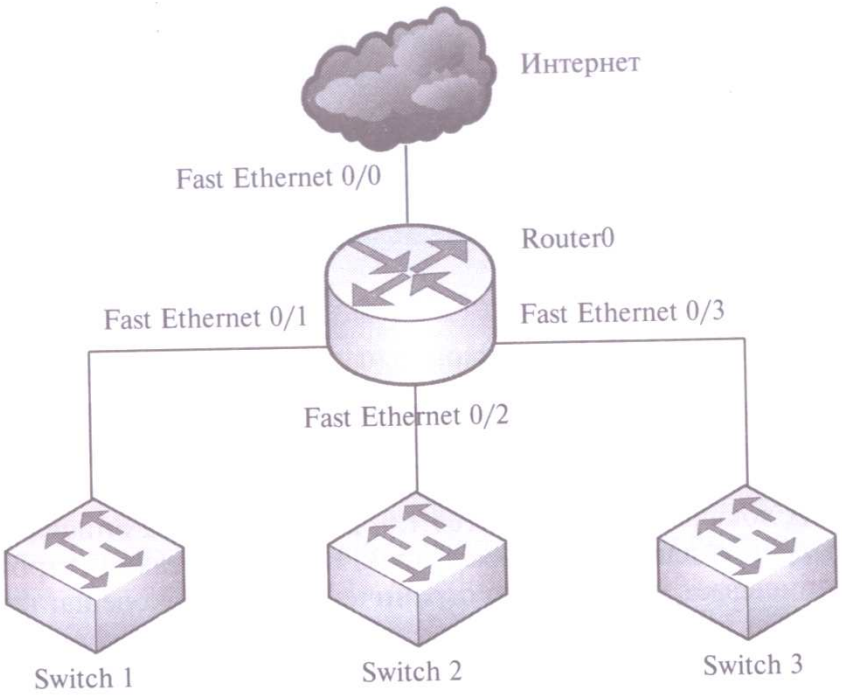

Рисунок 5.1 – Структура сети

Из рисунка 5.1 следует, что сеть состоит их трех подсетей (это могут быть, например, три отдела предприятия). Разделения на подсети осуществляется с использованием маршрутизатора

Router0, через него же осуществляется доступ к сети Интернет. Каждая подсеть содержит коммутатор второго уровня емкостью 24 порта.

Предположим, что для адресации сети будет использоваться частный адрес 192.168.1.0/24, преобразование частных адресов в общедоступные будет осуществляться маршрутизатором в соответствии с протоколом NAT.

Каждая подсеть может содержать до 24 **конечных узлов**, **плюс адрес интерфейса маршрутизатора, плюс два специальных адреса (для номера сети и широковещания)**, следовательно под адресацию узлов в каждой подсети необходимо отвести 5 разрядов (2^5=32). Оставшиеся 3 разряда четвертого байта можно использовать для адресации подсетей. Тогда маска подсети будет иметь вид: 11111111.11111111.11111111.11100000, или в десятичном формате: 255.255.255.224.

Тогда в нашей сети можно выделить 2^3=8 подсетей, из которых используем только три, а остальные можно оставить в резерве для будущее развития сети.

Подсетям назначим следующие адреса:

- 192.168.1.32/27;
- 192.168.1.64/27;
- 192.168.1.96/27.

Для конфигурирования статической маршрутизации в нашем примере портам маршрутизатора необходимо назначить сетевые адреса из диапазона адресного пространства перечисленных выше подсетей. Соответственно, порт FastEthernet, входящий в первую подсеть, получает адрес 192.168.1.33/27, во вторую - адрес 192.168.1.65/27, в третью – 192.168.1.97/27.

Компьютерам подсетей также **необходимо задать соответствующие сетевые настройки**. Этот процесс можно автоматизировать с применением протокола DHCP, или сконфигурировать конечные узлы вручную. **В состав минимальных настроек узла входят: IP-адрес, маска подсети**, а также **адрес шлюза по умолчанию**. В качестве шлюза по умолчанию в нашем примере для каждой из подсетей будет выступать маршрутизатор Router0, точнее, его интерфейс, включенный в подсеть.

Например, если конечные узлы работают под управлением ОС Windows, для конфигурирования необходимо зайти во вкладку

«Подключение по локальной сети - Свойства» и выбрать пункт «Протокол Интернета (TCP/IP)» (рисунок 5.2).

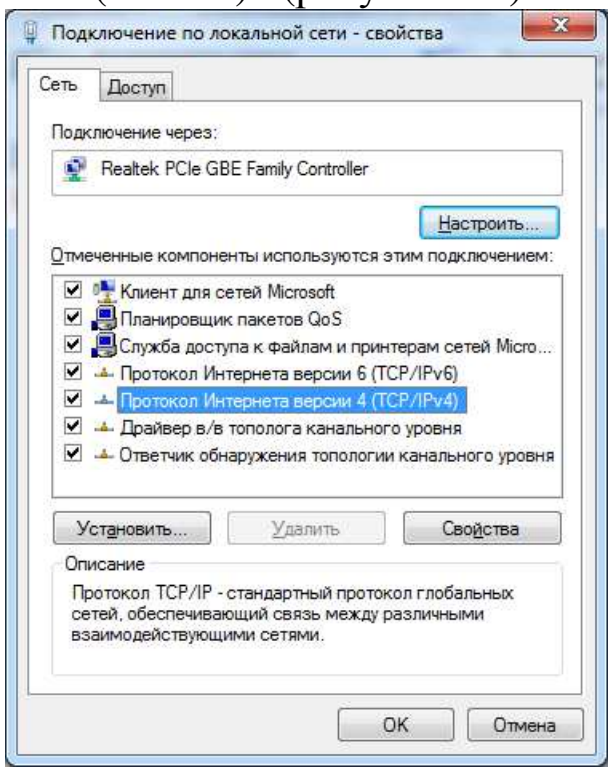

Рисунок 5.2 – Конфигурирование конечного узла

В появившемся окне необходимо выделить пункт «Использовать следующий IP-адрес»и в соответствующие поля внести минимальную конфигурацию (рисунок 5.3).

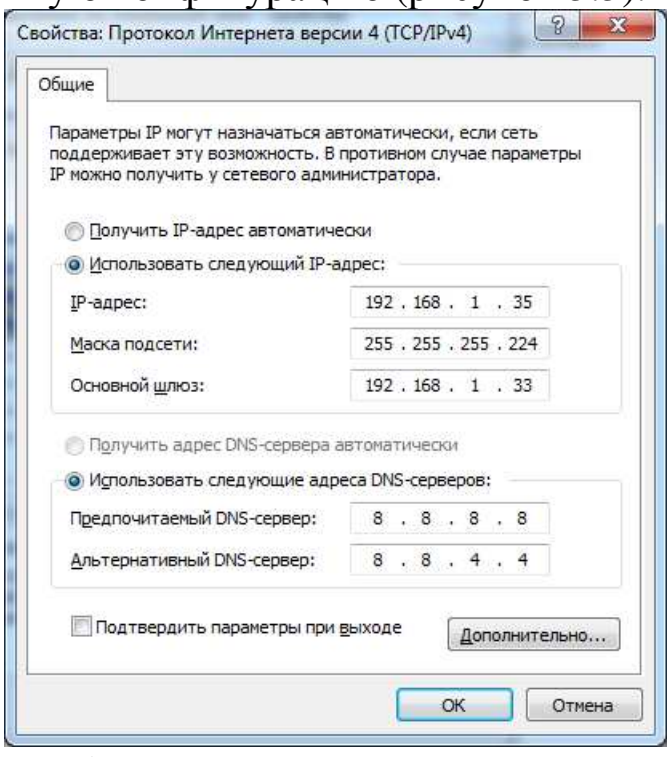

Рисунок 5.3 – Ручная настройка сетевых параметров

На рисунке 5.3 представлен пример конфигурирования конечного узла, входящего в первую подсеть.

Конфигурирование интерфейсов маршрутизатора зависит от его модели. Например, для маршрутизатора Cisco набор команд конфигурирования будет иметь следующий вид:

- Router0>**enable** – переход в привилегированный режим;

- Router0# **configureterminal** – вход в режим глобального конфигурирования;

- Router0 (conf)#**interfacefastEthernet 0/1** – переход к конфигурированию конкретного интерфейса (в данном случае, интерфейса fastEthernet 0/1);

- Router0 (conf -if)# **ipaddress 192.168.1.33 255.255.255.224** – назначение интерфейсуIP- адреса (с указанием маски).

Для того чтобы пакеты отправлялись во внешнюю сеть, пересылались на порт FastEthernet 0/0, необходимо прописать **маршрут по умолчанию**:

- Router0 (conf)# **interface fast ethernet 0/0**;

- Router0 (conf -if)# **ip route 0.0.0.0 0.0.0.0**<адрес порта fast ethernet 0/0 или выходной интерфей с маршрутизатора>[1].

В обобщенном виде запись маршрутного правила (далее маршрута) можно представить так:

ip route network netmask gateway

Например, конкретная запись может быть представлена как:

iproute 12.5.7.0 255.255.255.0 78.3.65.1,

где 12.5.7.0 – это адрес подсети (network), 255.255.255.0 – маска данной подсети (netmask), а 78.3.65.1 – адрес шлюза (gateway). **Шлюз представляет собой маршрутизатор, на который посылается весь трафик, удовлетворяющий данному маршруту**, т.е. имеющий адрес получателя пакетов входящий в указанную подсеть. **В качестве шлюза может использоваться next-hop маршрутизатор** [2].

Конфигурирование статической маршрутизации в нашем простейшем примере можно считать законченным [1].

После настройки всех маршрутизаторов сети необходимо проверить связь между компьютерами командой **ping, traceroute**. Если связь есть – все настройки сделаны верно, в противном случае, чтобы убедиться в том, что маршрутизатор действительно правильно сконфигурирован и работает корректно, просмотрите

таблицу маршрутизации роутера, используя команду show следующим образом:

- Router0#**showiproute**

Пример успешного прохождения трафика показан на рисунке 5.4.

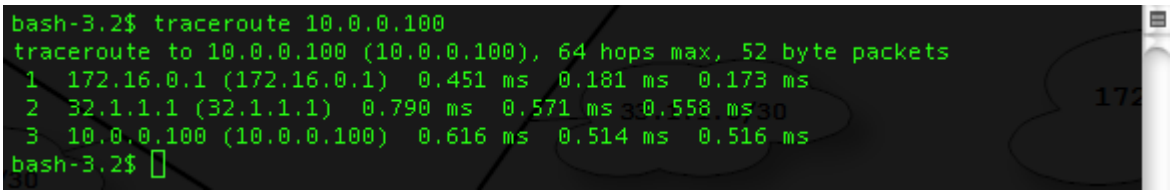

Рисунок 5.4 – Проверка связи между компьютерами командой traceroute

5.3 Исходные данные для выполнения лабораторной работы

Корпоративная сеть 15.0.0.0/8 разбита на десять подсетей, из них в данный момент задействовано шесть подсетей в шести разных подразделениях организации.

Состав сети:

- три маршрутизатора;
- шесть коммутаторов (по одному в каждом отделе на подсеть);
- один компьютер в каждой сети.

5.4 Задание для выполнения работы

1) Рассчитать параметры подсетей и задайте на компьютерах IP адрес, маску и шлюз в каждой отдельной подсети.

2) Создать произвольную топологию сети, соединив маршрутизаторы с подсетями в любом порядке. При этом соедините роутеры между собой произвольно – напрямую, через штатные коммутаторы подразделения или дополнительные коммутаторы.

3) Проверить работоспособность корпоративной сети командой PING – все компьютеры должны быть доступны.

5.5 Примерный перечень вопросов для защиты лабораторной работы

1) В чем преимущества статической маршрутизации?

2) Дайте характеристику параметрам статической таблицы маршрутизации?

3) Какие этапы при установке устройства присущи маршрутизаторам компании Cisco, но отсутствуют у коммутаторов?

4)Какую из указанных ниже команд можно встретить в интерфейсе командной строки маршрутизатора, но не коммутатора?

- команда clocrate;
- команда ipaddress маска адрес;
- команда ip address dhcp;
- команда interface vlan 1

5) Чем отличаются интерфейсы командной строки маршрутизатора и коммутатора компании Cisco?

6) Какая из указанных ниже команд не покажет настройки IP-адресов и масок в устройстве?

- show running-config;
- show protocol тип, номер;
- show ip interface brief;

Show version

7) Перечислите основные функции маршрутизатора в соответствии с уровнями модели OSI.

8) Приведите классификацию маршрутизаторов по областям применения.

9) Перечислите основные технические характеристики маршрутизаторов.

10) Дайте характеристику основным сериям маршрутизаторов компании Cisco.

11) Приведите перечень протоколов маршрутизации и дайте им краткие характеристики.

12) Приведите перечень поддерживаемых маршрутизаторами интерфейсов для локальных и глобальных сетей и определите их назначение.

13) Приведите перечень поддерживаемых маршрутизаторами сетевых протоколов и определите их назначение.

6 Лабораторная работа №6 «Дистанционно-векторная маршрутизация с использованием протокола RIP»

6.1 Цель работы

Изучение принципов построения вычислительных сетей с использованием маршрутизаторов, работающих по протоколу RIP.

6.2 Краткая теоретическая справка

6.2.1 Протокол RIP

Протокол RIP (Routing Information Protocol) является одним из первых протоколов маршрутизации и относится к дистанционно-векторным протоколам. Существует две версии RIP – первая версия (**RIPv.1**) использует маршрутизацию на основе классов и **описана в RFC 1058**, вторая версия (**RIPv.2**) использует бесклассовую маршрутизацию и **описана в RFC 1388** [1].

Применение дистанционно-векторной маршрутизации накладывает ограничения на размер составной сети. При этом вводится понятие максимального диаметра сети [2] – максимальное расстояние, на которое может быть передан пакет, после превышения которого пункт назначения считается недостижимым. **Для протоколов RIP** обеих версий **максимальный диаметр сети составляет 15 маршрутизаторов**, соответственно, маршрут с метрикой 16 считается недостижимым.

Для рассмотрения процедур, предусмотренных протоколом RIP, изучим пример составной сети, представленный на рисунке 6.1.

На рисунке 1 представлены три маршрутизатора – R1 – R3, у каждого из которых обозначены порты FastEthernet (Fa) с назначенными IP–адресами. Адреса портов, как и ранее, соответствуют адресам подсетей, в которые они входят.

На первом этапе протокола RIP**создаются минимальные таблицы маршрутизации**, которые содержат только адреса непосредственно подключенных подсетей.

Минимальную таблицу маршрутизатора R1 представим в виде таблицы 6.1.

Таблица 6.1- Минимальная таблица маршрутизатора R1

Адрес сети назначения	Адрес порта следующего маршрутизатора	Адрес выходного порта	Метрика
192.168.1.0	-	192.168.1.1	1
192.168.2.0	-	192.168.2.1	1

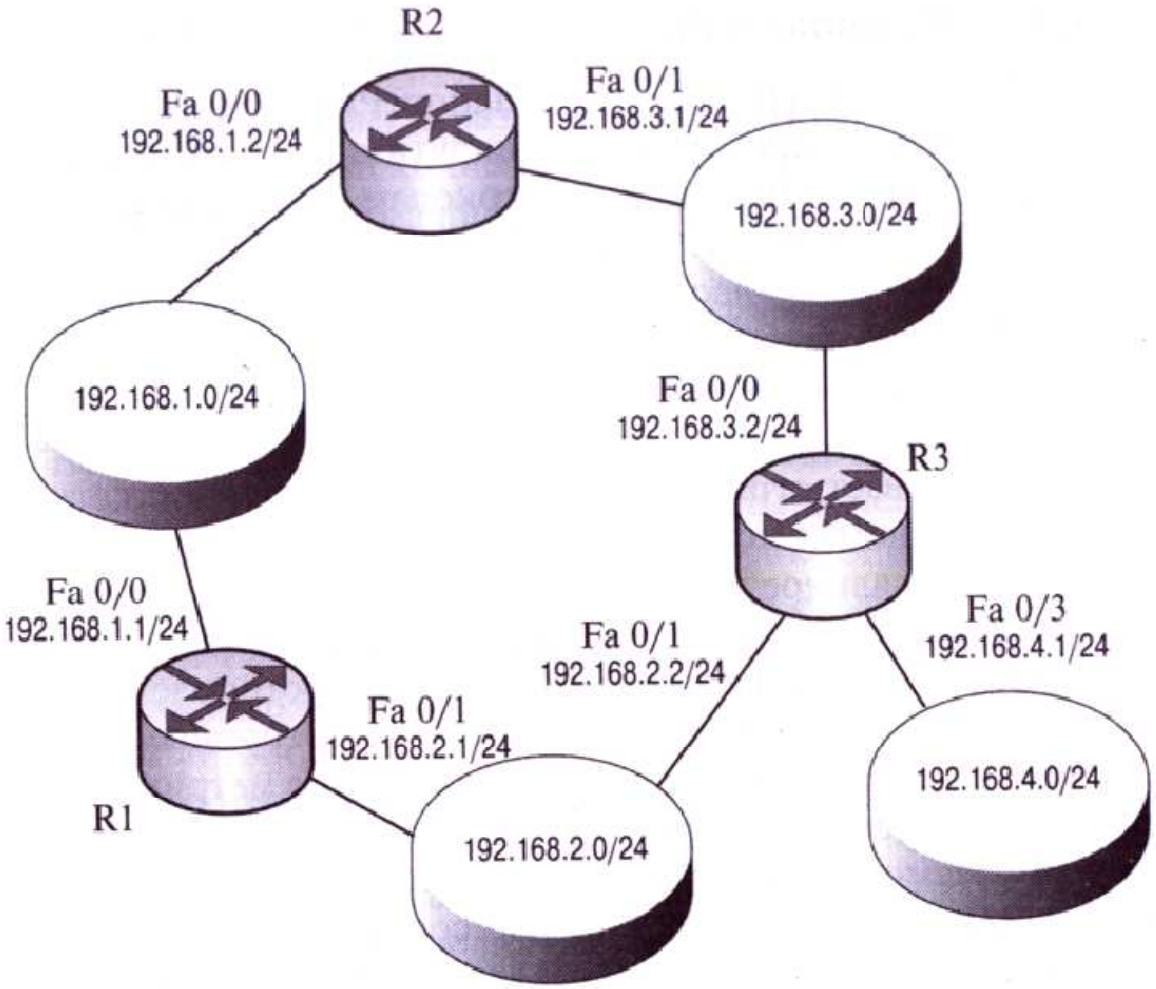

Рисунок 6.1 – Пример сети

Минимальные таблицы маршрутизаторов R2 и R3 имеют аналогичный вид и представлены в таблицах 6.2 и 6.3 соответственно.

Таблица 6.2 – Минимальная таблица маршрутизатора R2

Адрес сети назначения	**Адрес порта следующего маршрутизатора**	**Адрес выходного порта**	**Метрика**
192.168.1.0	-	192.168.1.1	1
192.168.3.0	-	192.168.3.1	1

Таблица 6.3 – Минимальная таблица маршрутизатора R3

Адрес сети назначения	**Адрес порта следующего маршрутизатора**	**Адрес выходного порта**	**Метрика**
192.168.3.0	-	192.168.3.2	1
192.168.2.0	-	192.168.2.2	1
192.168.4.0	-	192.168.4.1	1

На следующем этапе каждый из маршрутизаторов рассылает минимальную таблицу своим «соседям». Для этого используется UDP – дейтаграмма с номером порта 520. В этой дейтаграмме содержатся сведения о сети, имеющейся в минимальной таблице, и расстоянии до нее.

Например, «соседями» для маршрутизатора R1 являются маршрутизаторы R2 и R3. Поэтому им передаются сообщения примерно следующего вида:

- сеть 192.168.1.0, метрика 1;
- сеть 192.168.2.0, метрика 1.

Аналогичным образом свою минимальную таблицу маршрутизатор R2 передает маршрутизаторам R1 и R3, а маршрутизатор R3 –маршрутизаторам R1 и R2.

После получения информации от своих «соседей» маршрутизатор обрабатывает ее – у**величивает значение принятой метрики на единицу и запоминает порт, на который пришло данное сообщение, а также адрес маршрутизатора (точнее, его порта)**, передавшего сообщение. Эта информация

заносится в таблицу маршрутизации (в которой уже имеются минимальные записи).

Например, после приёма RIP – сообщения от маршрутизаторов R2 и R3 таблица маршрутизатора R1 примет вид, представленный в таблице 6.4.

Таблица 6.4 – Таблица маршрутизатора R1

Адрес сети назначения	**Адрес порта следующего маршрутизатора**	**Адрес выходного порта**	**Метрика**
192.168.1.0	-	192.168.1.1	1
192.168.2.0	-	192.168.2.1	1
192.168.1.0	192.168.1.2	192.168.1.1	2
192.168.3.0	192.168.1.2	192.168.1.1	2
192.168.3.0	192.168.2.2	192.168.2.1	2
192.168.2.0	192.168.2.2	192.168.2.1	2
192.168.4.0	192.168.2.2	192.168.2.1	2

Нетрудно заметить, что строки 3 и 4 были заполнены в результате получения информации от маршрутизатора R2, а строки 5-7 – в результате получения информации от маршрутизатора R3.

Затем маршрутизатор сравнивает принятую информацию с той, которая содержалась в его минимальной таблице. В нашем примере информация о сети 192.168.1.0 содержится как в 1, так и в 3 строках, однако в строке 3 метрика больше, следовательно, эта строка удаляется. Аналогичным образом удаляется строка 6. В строках 4 и 5 содержатся данные о разных маршрутах к одной и той же сети – 192.168.3.0 – и с одним и тем же значением метрики. Поэтому в таблице сохраняется та запись, которая появилась раньше (например, строка 4).

После этого рассмотренные выше **процедуры повторяются, только «соседям» рассылаются** уже не минимальные таблицы, а **таблицы с данными, полученными от других маршрутизаторов**. Правило обработки полученной информации и внесения новых данных в таблицу остается прежним – запись о новом маршруте к уже известной сети производится в том случае, если метрика нового маршрута меньше метрики имеющегося маршрута.

В нашем простейшем примере новых записей в таблицу внесено не будет. Тем не менее, **маршрутизаторы будут продолжать рассылку своих таблиц каждые 30 секунд**, чем обеспечивается корректировка таблиц в случае изменения состояния сети.

Одним из важнейших понятий алгоритмов маршрутизации является время сходимости. Считается, что **алгоритм «сошелся», когда все маршрутизаторы имеют согласованную информацию о доступных маршрутах**. Время сходимости протокола RIPдостаточно велико, поэтому **в данном протоколе возможны возникновения петель маршрутизации**, что приводит к «зацикливанию» пакетов. В настоящее время эта проблем решается путем введения дополнительных мер (например, использование метода «расщепления горизонта») и ограничением максимального значения метрики.

С другой стороны, данное ограничение не позволяет использовать RIPв крупных сетях. Кроме того, сама **логика работы RIP приводит к существенному «засорению» сети служебным трафиком**, так как таблицы передаются маршрутизаторами в полном объеме независимо от состояния сети [3].

6.2.2 Настройка протокола RIP на маршрутизаторах

Пример настройки протокола RIP на маршрутизаторе Router1 для сети, представленной на рисунке 6.2, показан ниже.

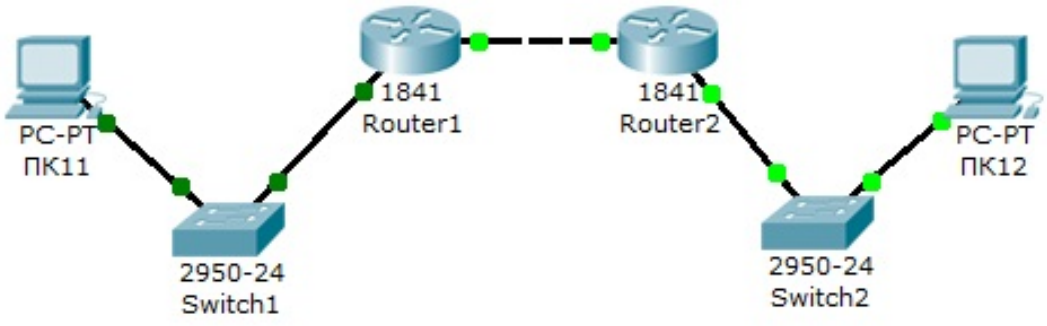

Рисунок 6.2 – Схема сети, где Switch1 – сеть 10.11.0.0/16, Switch2 – сеть 10.12.0.0/16, сеть для маршрутизаторов - 10.10.0.0/16

Для произведения настройки войдите в конфигурации в консоль роутера и выполните следующие настройки (при вводе

команд маску подсети можно не указывать, т.к. она будет браться автоматически из настроек интерфейса маршрутизатора):

Войдите в привилегированный режим:

Router1>**en**

Войдите в режим конфигурации:

Router1>#**conft**

Войдите в режим конфигурирования протокола RIP:

Router1(config)#**routerrip**

Подключите клиентскую сеть к маршрутизатору:

Router1(config-router)#**network 10.11.0.0**

Подключите вторую сеть к маршрутизатору:

Router1(config-router)#**network 10.10.0.0**

Задайте использование второй версии протокол RIP:

Router1(config-router)#**version 2**

Выйдите из режима конфигурирования протокола RIP:

Router1(config-router)#**exit**

Выйдите из консоли настроек:

Router1(config)#**exit**

Сохраните настройки в память маршрутизатора:

Router1>#**writememory**

После настройки всех маршрутизаторов сети необходимо проверить связь между компьютерами командой **ping, traceroute**. Если связь есть – все настройки сделаны верно, в противном случае, чтобы убедиться в том, что маршрутизатор действительно правильно сконфигурирован и работает корректно, просмотрите таблицу RIP роутера, используя команду show следующим образом:

Router#**show ip route rip**

Пример результата работы команды показан на рисунке 6.3.

```
Router6>en
Router6#show ip route rip
R    11.0.0.0/8 [120/2] via 81.0.0.4, 00:00:08, FastEthernet0/1
R    12.0.0.0/8 [120/1] via 61.0.0.3, 00:00:08, Ethernet0/0/0
R    13.0.0.0/8 [120/1] via 81.0.0.4, 00:00:08, FastEthernet0/1
R    21.0.0.0/8 [120/2] via 61.0.0.3, 00:00:08, Ethernet0/0/0
                [120/2] via 81.0.0.4, 00:00:08, FastEthernet0/1
R    31.0.0.0/8 [120/1] via 81.0.0.4, 00:00:08, FastEthernet0/1
R    51.0.0.0/8 [120/1] via 61.0.0.3, 00:00:08, Ethernet0/0/0
Router6#
```

Рисунок 6.3 – Таблица маршрутизации RIP

6.3 Задание на лабораторную работу

1) Создайте схему в сетевом эмуляторе в соответствии с рисунком 6.4.

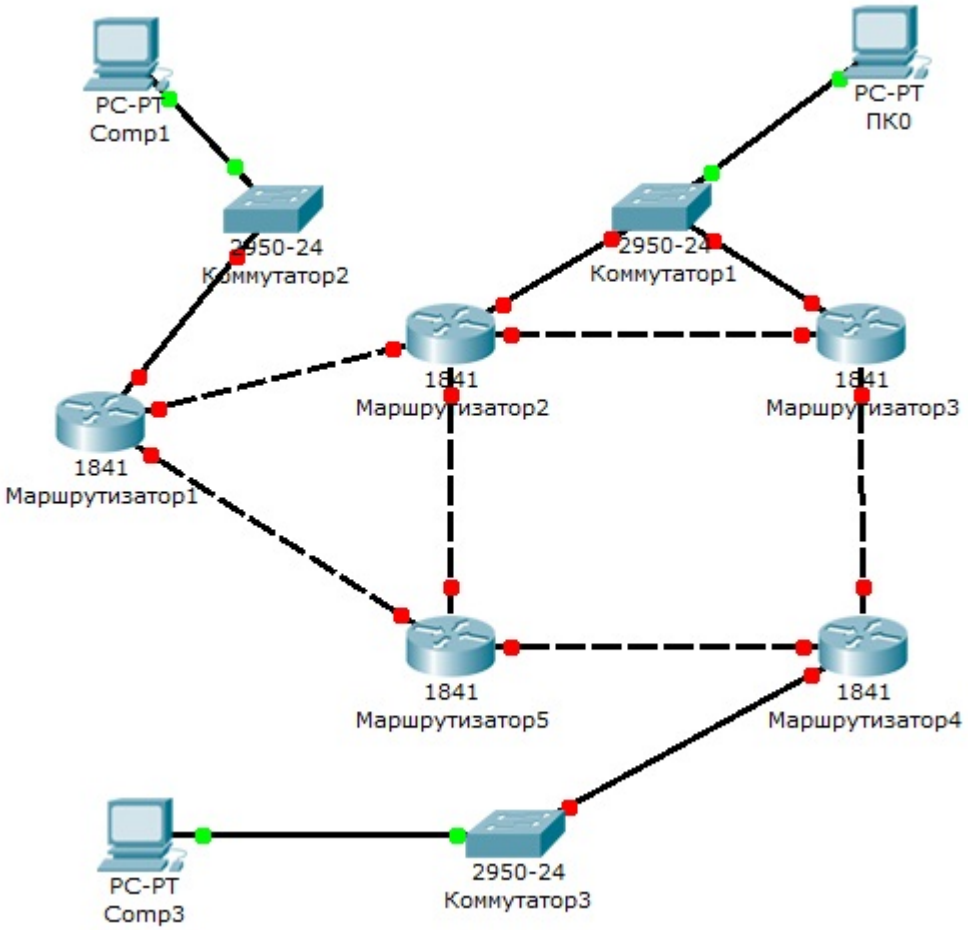

Рисунок 6.4 – Схема сети в программной среде Cisco Packet Tracer

2) Настройте сеть с использованием протокола RIP.

3) Проверьте связь между компьютерами Comp1 и Comp3 с помощью команд **ping** и **traceroute**при включенном и выключенном пятом маршрутизаторе.

4) Проверьте связь между компьютерами ПК0 и Comp1 с помощью команд **ping** и **traceroute** при включенном и выключенном втором маршрутизаторе.

6.4 Примерный перечень вопросов для защиты лабораторной работы

1)Какова схема работы протокола RIP?

2)Каковы этапы настройки протокола маршрутизации RIPv.2?

3) Какое обстоятельство не позволяет использовать RIPв крупных сетях?

4) Когда считается, что алгоритм протокола RIP«сошелся»?

5) Какими дополнительными мерами решается возникновение петель машрутизации при использовании протокола RIP?

6) С каким интервалом маршрутизаторы продолжают рассылку своих таблиц?

7) Что такое максимальный диаметр сети?

8) Какого значения достигает максимальный диаметр сети при использовании протокола RIP?

9) В каких документах описана первая и вторая версия протокола маршрутизации RIP?

10) Чем отличается вторая версия протокола RIPот перовой?

11) Какой номер порта используется для рассылки UDP-дейтаграмм с информацией о сети, имеющейся в минимальной таблице, и расстоянии до нее?

12) Какой командой можно просмотреть RIP-таблицу Cisco-маршрутизатора?

7 Лабораторная работа №7 «Трансляция сетевых адресов (NAT)»

7.1 Цель работы

Изучение принципов работы протокола NAT (Network Address Translation).

7.2 Краткие теоретические сведения

NAT (NetworkAddressTranslation) – трансляция адресов, позволяющая скрывать адреса сети от узлов, находящихся за маршрутизатором. При прохождении пакетов через маршрутизатор внутренние адресасети перед выходом с внешнего интерфейса транслируются в другие адреса. NAT конфигурируется с помощью команд nat и global.

Когда исходящий пакет от узла, находящегося во внутренней зоне, попадает на маршрутизатор, на котором сконфигурирована система NAT, адрес источника пакета сравнивается с таблицей существующих трансляций. Если этого адреса источника нет в таблице, он транслируется в один из адресов пула и в таблице трансляций появляется новая запись для этого адреса источника. Пул выдаваемых адресов конфигурируется командой global. В результате этого происходит обновление таблицы трансляций, а пакет перенаправляется дальше. По истечении определенного времени (значение по умолчанию равно трем часам) запись в таблице трансляций для адреса источника, не пославшего ни одного пакета, очищается и адрес, выданный из пула, освобождается для использования другими узлами внутренней зоны.

Задание правил трансляции адресов исходящих пакетов для одного либо нескольких узлов осуществляется с помощью команды nat.

Синтаксис команды можно представить следующим образом:

nat [(if_name)] nat_id address [netmask] [[tcp] tcp_max_conns [emb_limit] [norandomseq]]] [udp udp_max_conns], где:

- if_name – имя интерфейса, подключенного к сети, адреса которой необходимо транслировать;

- nat_id – число от 1 до 65535, соответствующее номеру пулаглобальных адресов, в которые будут транслироваться внутренниеадреса;

- address [netmask] – адрес, в который будет происходитьтрансляция;

- tcp_max_conns – максимальное число одновременных соединений, разрешенных узлам внутренней зоны. Соединения в состоянии бездействия закрываются автоматически по истечении таймаута, задаваемого командой timeout conn;

- emb_limit – максимальное число незавершенных (embryonic) соединений. К незавершенным соединениям относятся те, которые еще не были до конца установлены между источником и назначением, например, при установке TCP-соединения между узлами;

- norandomseq – устанавливает необходимость при каждом новом соединении генерировать случайный initial sequence number (ISN). Связано это с тем, что TCP/IP стек некоторых ОС использует предсказуемые ISN, а это дает возможность злоумышленнику вклиниться в чужую сессию;

- udp_max_conns – максимальное число одновременных UDP-соединений, разрешенных каждому из узлов внутренней сети.

UDP-соединения, находящиеся в состоянии бездействия, закрываются автоматически по истечении таймаута, задаваемого командой timeout conn.

Пример настройки службы NAT:

PIX(config)#nat (inside) 1 10.0.0.0255.255.255.0.

В команде nat параметром nat_id указывается номер пула **глобальных адресов, которые можно сконфигурировать командой global. Синтаксис:**

global [(if_name)] nat_id {mapped_ip [-mapped_ip] [netmask mapped_mask]} | interface, где:

- if_name – имя интерфейса, на котором необходимо использовать задаваемый пул глобальных адресов;

- mapped_ip [-mapped_ip] – один адрес либо диапазон адресов;

- netmask mapped_mask – задание маски для пула адресов вслучае, если используются подсети. Если диапазон адресов с заданной маской покрывает несколько подсетей, то адрес подсети и широковещательный адрес подсети не выдаются для трансляции.

Например, если задан диапазон адресов 192.168.0.20-192.168.0.140и маска 255.255.255.128, то адрес второй подсети 192.168.0.128 и широковещательный адрес первой подсети 192.168.0.127 выдаваться не будут;

- interface – определяет использование PAT (Port AddressTranslation) на интерфейсе. Пример:

PIX(config)#nat (inside) 1 10.0.0.0255.255.255.0

PIX(config)#global (outside) 1 192.168.0.3-192.168.0.100

В этом примере сконфигурирован пул из 98 адресов(192.168.0.3-192.168.0.100) под номером 1, в которые будут транслироваться внутренние адреса узлов из сети 10.0.0.0 при прохождении сетевых пакетов через маршрутизатор.

Выдача адресов осуществляется динамически, начиная сначала диапазона и до его конца. В примере первым выданным адресом будет 192.168.0.3.

Командой nat control включается одноименный режим.

При работе в этом режиме пакеты, идущие из внутреннего (inside) интерфейса на внешний (outside), должны иметь сконфигурированное для них правило трансляции. То есть, каждый узел сети внутренней зоны может обмениваться данными с узлами сети внешней зоны, если заданы правила трансляции для этих внутренних узлов.

Если на маршрутизатор приходит пакет от внутреннего узла, для которого не сконфигурировано правило трансляции, то этот пакет им необрабатывается.

Режим nat control является выключенным по умолчанию. Поэтому маршрутизатор транслирует адрес источника пакета в любом случае.

Кроме команды nat существует команда static, с помощьюкоторой осуществляется конфигурирование статической трансляции. Синтаксискоманды:

PIX(config)# static (real_ifc, global_ifc){global_ip | interface} {real_ip [netmaskmask]}, где:

- real_ifc – интерфейс, на который приходят пакеты, подлежащие трансляции;

- global_ifc – интерфейс, с которого уходит для дальнейшеймаршрутизации транслированный пакет;

- global_ip – адрес, в который будет осуществляться трансляция;

- real_ip – адрес, который будет транслироваться. Пример:

PIX(config)#static (inside,outside)192.168.100.10 10.10.10.10 netmask255.255.255.255

Все пакеты, приходящие на адрес 192.168.100.10 будут передаваться на узел с адресом 10.10.10.10.

Команда fixup на маршрутизаторе предоставляет некоторые возможности глубокого анализа пакетов.

Например, команда fixup protocol http приводит к тому,что маршрутизатор выполняет ряд действий, к которым относятся:

- ведение журналов, фиксирующих URL-запросы, содержащие команды GET;
- мониторинг URL-запросов при помощи средств N2H2 или Websense;
- фильтрация опасных сценариев Java и ActiveX [1].

Для последних двух функций маршрутизатор должен быть сконфигурирован с командой filter. Пример команд для углубленного анализа трафика по основным протоколам [1]:

PIX(config)#fixupprotocolftp 21
PIX(config)#fixup protocol http 80
PIX(config)#fixup protocol h323 1720
PIX(config)#fixup protocol rsh 514
PIX(config)#fixup protocol smtp 25
PIX(config)# fixup protocol sqlnet 1521..

7.3 Задание на лабораторную работу

1) Настроить службу NAT на внутреннем интерфейсе маршрутизатора.
2) Выполнить конфигурацию пула глобальных адресов для внутреннего интерфейса межсетевого экрана.
3) Включить nat control режим и проверить возможность прохождения сетевых пакетов между интерфейсами устройства.
4) Выключить nat control режим.
5) Сконфигурировать статическую трансляцию на внешнем интерфейсе межсетевого экрана.
6) С помощью программного сниффера проверить работу статической трансляции.

Примечание: каждая итерация должна сопровождаться скриншотом (-ами).

7.4 Примерный перечень вопросов для защиты лабораторной работы

1) Зачем необходима технология NAT?
2) Какой командой осуществляется конфигурирование статической трансляции?
3) Какая команда включает одноименный режим?
4) Каков синтаксис команды настройки NAT?
5) Какой командой включается NAT?
6) Какими преимуществами обладает динамический NATпо сравнению со статическим?

8 Лабораторная работа №8 «Списки управления доступом (ACL)»

8.1 Цель работы

Изучение работы со стандартными и расширенными списками доступа.

8.2 Краткие теоретические сведения

8.2.1 Стандартные списки доступа

Списки доступа (access lists) представляют собой общие критерии отбора, которые можно впоследствии применять при фильтрации дейтаграмм, для отбора маршрутов, определения приоритетного трафика и в других задачах.

Списки доступа, производящие отбор по IP-адресам, **создаются командами access-list в режиме глобальной конфигурации**, каждый список определяется номером – числом в диапазоне 0 ÷ 99.

Каждая такая **команда добавляет новый критерий отбора в список:**

router(config)#access-list<номер_списка><{deny|permit}><IP-адрес>[маска_шаблона].

IP-адрес и маска шаблона записываются в десятично-точечной нотации, при этом в маске шаблона устанавливаются биты, значение которых в адресе следует игнорировать, остальные биты сбрасываются. При этом сетевая маска (netmask) и маска шаблона(wildcard) – это разные вещи. Например, чтобы строка списка сработала для всех узлов с адресами 1.16.124.xxx, адрес должен быть1.16.124.0, а маска – 0.0.0.255, поскольку значения первых 24 бит жестко заданы, а значения последних 8 бит могут быть любыми.

Как видно в этом случае маска шаблона является инверсией соответствующей сетевой маски. Однако маска шаблона в общем случае не связана с сетевой маской и даже может быть разрывной (содержать чередования нулей и единиц). Например, строка списка должна сработать для всех нечетных адресов в сети 1.2.3.0/24. Соответствующая комбинация адреса и маски шаблона: 1.2.3.10.0.0.254.

Комбинация «адрес – маска шаблона» вида 0.0.0.0 255.255.255.255(то есть соответствующая всем возможным адресам) может быть записана в виде одного ключевого слова any. Если маска отсутствует, то речь идет об IP-адресе одного узла.

Операторы permit и deny определяют, соответственно, положительное (принять, пропустить, отправить, отобрать) **или отрицательное** (отбросить, отказать, игнорировать) **будет принято решение при срабатывании данного критерия отбора.** Например, если список используется при фильтрации дейтаграмм по адресу источника, то эти операторы определяют, пропустить или отбросить дейтаграмму, адрес источника которой удовлетворяет комбинации«адрес – маска шаблона». Если же список применяется для идентификации какой-либо категории трафика, то оператор allow отбирает трафик в эту категорию, а deny – нет.

Список доступа представляет собой последовательность из одного и более критериев отбора, имеющих одинаковый номер списка. Последовательность критериев имеет значение: маршрутизатор просматривает их по порядку; срабатывает первый критерий, в котором обнаружено соответствие образцу; оставшаяся часть списка игнорируется. Любые новые критерии добавляются только в конец списка. Удалить критерий нельзя, можно удалить только весь список. В конце списка неявно подразумевается критерий «отказать в любом случае» (deny any) – он срабатывает, если ни одного соответствия обнаружено не было[1].

Для аннулирования списка доступа следует ввести команду:

router(config)#no access-list <номер_списка>.

Чтобы применить список доступа для фильтрации пакетов, проходящих через определенный интерфейс, нужно в режиме конфигурации этого интерфейса ввести команду:

router(config-if)#ip access-group <номер_списка><{in|out}>.

Ключевое слово in или out определяет, будет ли список применяться к входящим или исходящим пакетам соответственно.

Входящими считаются пакеты, поступающие к интерфейсу из сети.

Исходящие пакеты движутся в обратном направлении.

Только один список доступа может быть применен на конкретном интерфейсе для фильтрации входящих пакетов, и один –для исходящих. Соответственно, все необходимые критерии

фильтрации должны быть сформулированы администратором внутриодного списка.

В стандартных списках доступа отбор пакетов производитсяпо IP-адресу источника пакета [2].

8.2.2 Расширенные списки доступа

Кроме стандартных (standard) списков доступа существуют также расширенные (extended), имеющие большее количество параметров и предлагающие более богатые возможности для формирования критериев отбора.

Расширенные списки доступа создаются также с помощью команды access-list в режиме глобальной конфигурации, но номера этих списков лежат в диапазоне 100–199. Пример синтаксиса **команды создания строки расширенного списка для контроля TCP-соединений [2]:**

router(config)#access-list<номер_списка><{deny| permit}>tcp<IP-адрес_источника><маска_шаблона> [оператор порт[порт]]<IP-адрес_получателя><маска_шаблона> [оператор порт[порт]] [established]

Маски шаблона для адреса источника и узла назначения определяются так же, как и в стандартных списках.

Оператор при значении порта должен иметь одно из следующих значений: lt (меньше), gt (больше), eq (равно), neq (не равно), range (диапазон включительно). После оператора следует номер порта (или два номера порта в случае оператора range), к которому этот оператор применяется.

Комбинация оператор-порт, следующая сразу же за адресом источника, относится к портам источника. Соответственно, комбинация оператор-порт, которая следует сразу же за адресом получателя, относится к портам узла-получателя. Применение этих комбинаций позволяет отбирать пакеты не только по адресам мест отправки и назначения, но и по номерам TCP- или UDP-портов.

Кроме того, ключевое слово established определяет сегменты TCP, передаваемые в состоянии установленного соединения. Это значит, что строке, в которую включен параметр established, будут соответствовать только сегменты с установленным флагом ACK (или RST).

Пример: «запретить установление соединений с помощью протокола Telnet со всеми узлами сети 22.22.22.0 netmask 255.255.255.0 со стороны всех узлов Интернета, причем в обратном направлении все соединения должны устанавливаться; остальные TCP-соединения разрешены». Фильтр устанавливается для входящих сегментов со стороны Интернета (предположим, к Интернету маршрутизатор подключен через интерфейс FastEthernet 1/0).

router(config)#access-list 101 permit tcp any22.22.22.0 0.0.0.255 eq 23 established

router(config)#access-list 101 deny tcp any22.22.22.0 0.0.0.255 eq 23

router(config)#access-list 101 permit ip any any

router(config)#interface FastEthernet 1/0

router(config-if)#ip access-group 101 in.

Указание ip вместо tcp в команде access-list означает «все протоколы». Отметим, что в конце каждого списка доступа подразумевается deny ip any any, поэтому в предыдущем примере мы указали permit ip any any для разрешения произвольных пакетов, не попавших под предшествующие критерии.

Расширенный список с протоколом ip позволяет также производить отбор произвольных пакетов по адресу отправителя и по адресу получателя (в стандартных списках отбор производится только по адресу отравителя).

Критерии для отбора UDP-сообщений составляются аналогично TCP, при этом вместо tcp следует указать udp, а параметр established, конечно, не применим.

Контроль за ICMP-сообщениями может осуществляться с помощью критериев отбора типа:

router(config)#access-list<номер_списка><{deny|permit}>icmp<IP-адрес_источника><маска_шаблона><IP-адрес_назначения><маска_шаблона>[icmp-тип [icmp-код]].

Здесь icmp-тип и, если требуется уточнение, icmp-код определяют ICMP-сообщение.

Вообще, в расширенных списках можно работать с пакетами любого IP-протокола. Для этого после оператора deny/permit надо указать название протокола (ahp, esp, eigrp, gre, icmp, igmp, igrp, ipinip, ospf, tcp, udp) или его номер, которым он кодируется в поле

Protocol заголовка пакета. Далее указываются адреса источника и узла назначения с масками и, возможно, дополнительные параметры, специфичные для данного протокола.

В конце команды access-list (расширенный) можно указать параметр log, тогда все случаи срабатывания данного критерия (то есть обнаружения пакета, соответствующего критерию), **будут протоколироваться на консоль или как указано командой logging.** После того, как протоколируется первый случай срабатывания, дальше сообщения посылаются каждые 5 минут с указанием числа срабатываний за отчетный период.

Просмотр имеющихся списков доступа (с указыванием числа срабатываний каждого критерия):

router#showaccess-lists.

Более подробную статистику работы списков доступа можнополучить, включив режим ipaccounting. Режим включается в контексте конфигурирования интерфейса. **Следующая команда включает режим учета случаев нарушения** (то есть, пакетов, которые небыли пропущены списком доступа на данном интерфейсе):

router(config-if)#ip accounting access-violations.

Просмотр накопленной статистики (с указанием адресов отправителей и получателей пакетов):

router#show ip accounting access-violations.

При конфигурировании запрещающих фильтров (в конце которых подразумевается deny all) администратор должен не забыть оставить «дверь» для сообщений протоколов маршрутизации, если они используются на конфигурируемом интерфейсе [1].

8.3 Задание на лабораторную работу

1) Создать стандартный список доступа, разрешающий прохождения сетевых пакетов только для сетей 192.168.20.1/24 и 10.0.0.1/24. Для этого в глобальном контексте конфигурирования необходимо выполнить следующие команды:

router(config)#access-list 1 permit 192.168.20.1 0.0.0.255

router(config)#access-list 1 permit10.0.0.1 0.0.0.255

router(config)#access-list 1 deny any any.

2) Применить созданный стандартный список доступа на вход одного из интерфейсов межсетевого экрана.

3) С помощью команды ping проверить доступность компьютеров из сетей 192.168.20.1/24 и 10.0.0.1/24.

4) Аннулировать созданный стандартный список доступа.

5) Создать расширенный список доступа, запрещающий установление соединений с помощью протокола HTTP со всеми узлами сети 192.168.20.0 netmask 255.255.255.0 со стороны всех узлов сети «Интернет», но разрешающий установление всех соединений в обратном направлении.

6) Применить созданный расширенный список доступа на вход одного из интерфейсов межсетевого экрана.

7) Проверить работоспособность созданного расширенного списка, подключив к межсетевому экрану две сети с Web-серверами и осуществив к ним поочередно запросы.

8) Просмотреть число срабатываний каждого критерия из созданного списка доступа.

9) Включить учет случаев нарушения списка доступа.

10) Выполнить несколько запросов к Web-серверам.

11) Просмотреть результаты работы команды ping.

12) Вывести на консоль накопленную статистику по учету случаев нарушений.

13) Аннулировать созданный расширенный список доступа.

Примечание: каждая итерация должна сопровождаться скриншотом (-ами).

8.4 Примерный перечень вопросов для защиты лабораторной работы

1) Что представляют собой списки доступа (accesslists)?

2) Какие существуют списки доступа и чем они отличаются друг от друга?

3) Какая команда добавляет новый критерий отбора в стандартный список доступа?

4) Какие операторы определяют положительное или отрицательное решение при срабатывании заданного критерия?

5) Какой командой производится аннулирование списка доступа?

6) Какие пакеты считаются входящими?

7) Какие действие будет производить команда log в конце access lists (расширенный)?

8) Какой командой осуществляется просмотр всех имеющихся списков доступа?

9) Какой командой осуществляется просмотр накопленной статистики?

9 Лабораторная работа №9 «Демилитаризованные зоны (DMZ)»

9.1 Цель работы

Изучение способом построения демилитаризованных зон (DMZ) с использованием оборудования CiscoSystems.

9.2 Краткие теоретические сведения

Начиная с версии IOS 12.4, в маршрутизаторах появилась **функция Zone-BasedPolicyFirewall, позволяющая производить настройку правил межсетевого экрана.** Эта функция позволяет назначить интерфейсам маршрутизатора зоны безопасности и установить правила взаимодействия между ними.

Конфигурирование Zone-BasedPolicyFirewall заключается в выполнение следующих шагов:

1) назначить зоны межсетевого экрана;

2) определить возможность прохождения сетевого трафика между зонами;

3) включить существующие сетевые интерфейсы в созданные зоны;

4) определить классы, к которым будут применяться политики для пересечения пары зон;

5) определить политики для пар зон, регламентирующие производимые действия над проходящим сетевым трафиком;

6) применить политики для выбранных пар зон [1].

9.3 Задание на лабораторную работу

1) Создать в Cisco Packet Tracer топологию сети, представленную на рисунке 9.1.

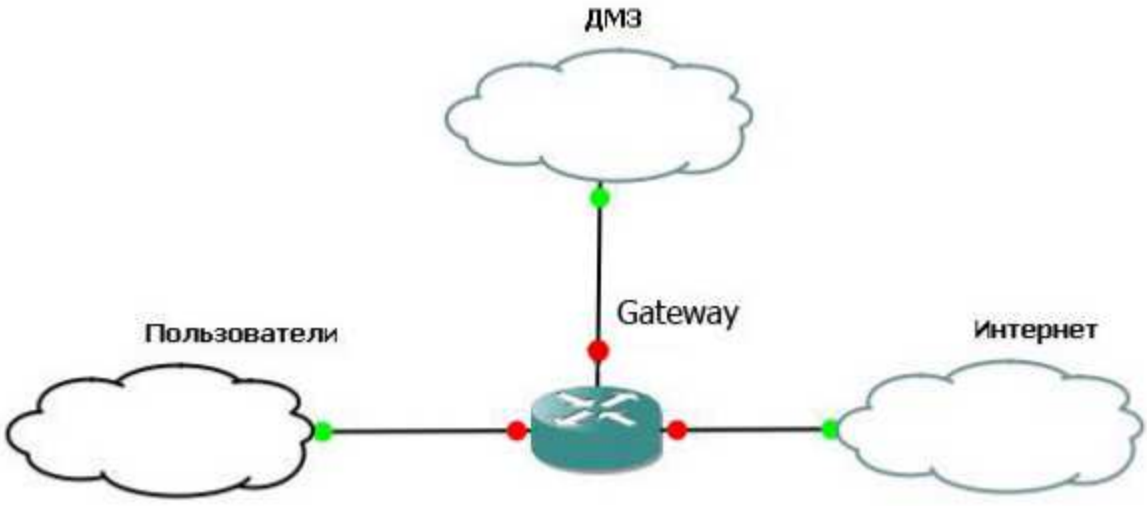

Рисунок 9.1 – Топология сети

2) В режиме глобального конфигурирования определить зоны безопасности. Для пользователей задать зону с именеminside, для Интернета – outside, для ДМЗ – DMZ.

Gateway(config)#zone security outside
Gateway(config-sec-zone)#description internet
Gateway(config-sec-zone)#exit
Gateway(config)#zone security inside
Gateway(config-sec-zone)# description intranet
Gateway(config-sec-zone)#exit
Gateway(config)#zone security dmz
Gateway(config-sec-zone)#description DMZ
Gateway(config-sec-zone)#exit.

3) Назначить интерфейсы в зоны. По умолчанию прохождения трафика между зонами запрещено.

Для зоны outside:
Gateway(config)#interface FastEthernet0/0
Gateway(config-if)#ip address 10.0.0.2 255.0.0.0
Gateway(config-if)#no shutdown
Gateway(config-if)#zone-member security outside
Gateway(config-if)#description outside
Gateway(config-if)#exit.
Для зоны inside:
Gateway(config)#interface FastEthernet0/1
Gateway(config-if)#ip address 192.168.20.2 255.255.255.0
Gateway(config-if)#no shutdown
Gateway(config-if)#zone-member security inside

Gateway(config-if)#description inside
Gateway(config-if)#exit.
Для зоны DMZ:
Gateway(config)#interface FastEthernet1/0
Gateway(config-if)#ip address 172.16.0.2 255.255.255.0
Gateway(config-if)#no shutdown
Gateway(config-if)#zone-member security dmz
Gateway(config-if)#description DMZ
Gateway(config-if)#exit.

4) Определить протоколы, по которым пользователямразрешено выходить в Интернет (http, ftp, smtp, pop3, dns,icmp).

Gateway(config)#class-map type inspect match-any cm_http-ftp-dns-smtp-pop3-icmp
Gateway(config-cmap)#match protocol http
Gateway(config-cmap)#match protocol ftp
Gateway(config-cmap)#match protocol pop3
Gateway(config-cmap)#match protocol smtp
Gateway(config-cmap)#match protocol dns
Gateway(config-cmap)#match protocol icmp
Gateway(config-cmap)#exit.

5) Определить политики:

Gateway(config)#policy-map type inspect in-out
Gateway(config-pmap)#class type inspect cm_http-ftp-dns-smtp-pop3-icmp
Gateway(config-pmap-c)#inspect
Gateway(config-pmap-c)#exit
Gateway(config-pmap)#exit.

6) Создатьцепочкуизпарызоninside → outside:

Gateway(config)#zone-pair security inside-outside source inside destination outside
Gateway(config-sec-zone-pair)#service-policy type inspect in-out
Gateway(config-sec-zone-pair)#exit.

7) Создать списки доступа для публичных серверов:

Gateway(config)#access-list 101 remark web-server
Gateway(config)#access-list 101 permit ip any host 172.16.0.4
Gateway(config)#access-list 102 remark mail-server
Gateway(config)#access-list 102 permit ip anyhost 172.16.0.5
Gateway(config)#access-list 103 remark ftp-server

Gateway(config)#access-list 103 permit ip anyhost 172.16.0.6.

8) Определить протоколы для доступа к серверам из внешнейсети:

Gateway(config)#class-map type inspect match-allweb
Gateway(config-cmap)#match access-group 101
Gateway(config-cmap)#match protocol http
Gateway(config-cmap)#exit
Gateway(config)#class-map type inspect match-allmail
Gateway(config-cmap)#match access-group 102
Gateway(config-cmap)#match protocol smtp
Gateway(config-cmap)#match protocol pop3
Gateway(config-cmap)#exit
Gateway(config)#class-map type inspect match-allftp
Gateway(config-cmap)#match access-group 103
Gateway(config-cmap)#match protocol ftp
Gateway(config-cmap)#exit.

9)ЗадатьполитикидляДМЗ:

Gateway(config)#policy-map type inspect web-mail-ftp-dmz
Gateway(config-pmap)#class type inspect web
Gateway(config-pmap-c)#inspect
Gateway(config-pmap-c)#exit
Gateway(config-pmap)#class type inspect mail
Gateway(config-pmap-c)#inspect
Gateway(config-pmap-c)#exit
Gateway(config-pmap)#class type inspect ftp
Gateway(config-pmap-c)#inspect
Gateway(config-pmap-c)#exit
Gateway(config-pmap)#exit.

10)Создать цепочку из пары зон outside → dmz:

Gateway(config)#zone-pair security out-dmzsource outside destination dmz

Gateway(config-sec-zone-pair)#service-policytype inspect web-mail-ftp-dmz

Gateway(config-sec-zone-pair)#exit.

11) Проверить работоспособность созданной конфигурации.

Примечание: каждая итерация должна сопровождаться скриншотом (-ами).

9.4 Примерный перечень вопросов для защиты лабораторной работы

1) Зачем необходимо построение демилитаризованных зон (DMZ)?
2) В выполнении каких шагов заключается конфигурирование Zone-Based Policy Firewall?
3) Какие существуют схемы построения сетей с использованием демилитаризованных зон?
4) Скакой версии IOS появилась технология Zone-Based Policy Firewall?

Список использованных источников

1) Андрончик А.Н., Коллеров А.С., Синадский А.С., Щербаков М.Ю. Сетевая защита на базе технологий фирмы CiscoSystems. Практический курс: учеб. пособие; под общ. ред. Синадского Н.И.- Екатеринбург: изд-во Урал. ун-та, 2014. – 180 с.
2) Соболь Б.В., Манин А.А., Герасименко М.С. Сети и телекоммуникации : учеб. пособие. – Ростов н/Д : Феникс, 2015. – 191 с.
3) Дорт-Гольц А.А., Симонина О.А. Принципы построения инфокоммуникационных сетей: методические указания к лабораторным работам. – УМЦ СПбГУТ, СПб, 2012. – 86 с.