ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ ИВАНОВСКОЙ ОБЛАСТИ
ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«КИНЕШЕМСКИЙ ТЕХНОЛОГИЧЕСКИЙ КОЛЛЕДЖ»

УТВЕРЖДАЮ
Директор ОГБПОУ КТК
_____ /И.А. Смирнов/
«31» августа 2022г.

Фонд оценочных средств
по ПМ.01 Выполнение работ по проектированию сетевой инфраструктуры
по специальности среднего профессионального образования
программа подготовки специалистов среднего звена
технологического профиля
09.02.06 Сетевое и системное администрирование

Срок обучения 3 года 10 месяцев

Кинешма, 2022

Фонд оценочных средств по ПМ.01 Выполнение работ по проектированию сетевой инфраструктуры разработан в соответствии с Федеральным государственным образовательным стандартом среднего профессионального образования по специальности 09.02.06 Сетевое и системное администрирование.

Разработчик: Шаронов Максим Олегович – преподаватель ОГБПОУ «Кинешемский технологический колледж»

Фонд оценочных средств по ПМ.01 Выполнение работ по проектированию сетевой инфраструктуры рассмотрен и одобрен на заседании методической комиссии учебно-методического объединения по укрупненным группам специальностей 09.00.00 Информатика и вычислительная техника, 13.00.00 Электро - и теплоэнергетика, 15.00.00 Машиностроение, 18.00.00 Химические технологии

Протокол № 1 от «31» августа 2022г.

Председатель _____ Киселева Е.В.

Паспорт
фонда оценочных средств по профессиональному модулю **ПМ 01 Выполнение работ по проектированию сетевой инфраструктуры**

1.2. Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля студент должен освоить основной вид деятельности Выполнение работ по проектированию сетевой инфраструктуры и соответствующие ему профессиональные компетенции, общие компетенции.

1.2.1 Перечень общих компетенций

Код	Наименование общих компетенций
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 2	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 3	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 4	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 5	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 6	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.
ОК 7	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 8	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.
ОК 9	Использовать информационные технологии в профессиональной деятельности.
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языке.
ОК 11	Планировать предпринимательскую деятельность в профессиональной сфере

1.2.2 Перечень профессиональных компетенций

Код	***Наименование видов деятельности и профессиональных компетенций***
ВД 1.	Выполнение работ по проектированию сетевой инфраструктуры
ПК 1.1.	Выполнять проектирование кабельной структуры компьютерной сети.
ПК 1.2.	Осуществлять выбор технологии, инструментальных средств и средств вычислительной техники при организации процесса разработки и исследования объектов профессиональной деятельности
ПК 1.3.	Обеспечивать защиту информации в сети с использованием программно-аппаратных средств.
ПК 1.4.	Принимать участие в приемо-сдаточных испытаниях компьютерных сетей и сетевого оборудования различного уровня и в оценке качества и экономической эффективности сетевой топологии.
ПК 1.5.	Выполнять требования нормативно-технической документации, иметь опыт оформления проектной документации.

Контроли-	Код форми-	Результат освоения (умения и знания)	Оценочные

руемые разделы (темы) дисциплины*	руемой компетенции	уметь	знать	средства
Раздел 1. Компьютерные сети	ПК 1.1-ПК 1.5 ОК 01-11	общие принципы построения сетей, сетевых топологий, многослойной модели OSI, требований к компьютерным сетям; стандарты кабелей, основные виды коммуникационных устройств, терминов, понятий, стандартов и типовых элементов структурированной кабельной системы.	проектировать локальную сеть, выбирать сетевые топологии; использовать многофункциональные приборы мониторинга, программно-аппаратные средства технического контроля локальной сети.	Вопросы для подготовки к дифференцированному зачёту, Самостоятельная работа, Тестирование, Комплексный экзамен
Раздел 2. Организация, принципы построения и функционирования компьютерных сетей	ПК 1.1-ПК 1.5 ОК 01-11	архитектуру протоколов, стандартизации сетей, этапов проектирования сетевой инфраструктуры; базовые протоколы и технологии локальных сетей; принципы построения высокоскоростных локальных сетей;	проектировать локальную сеть, выбирать сетевые топологии; использовать многофункциональные приборы мониторинга, программно-аппаратные средства технического контроля локальной сети.	Вопросы для подготовки к дифференцированному зачёту, Самостоятельная работа, Тестирование, Комплексный экзамен

Приложение 1

ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ ИВАНОВСКОЙ ОБЛАСТИ

ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

«КИНЕШЕМСКИЙ ТЕХНОЛОГИЧЕСКИЙ КОЛЛЕДЖ»

Вопросы для подготовки
к *дифференцированному зачету*

Раздел 1. Компьютерные сети

Тема 1.1. Введение в сетевые технологии

1. Интернет и современные сетевые технологии – область применения и назначение.
2. Виды компьютерных сетей.
3. Глобальные и локальные сети
4. Одноранговые и клиент-серверные архитектуры
5. Основные компоненты сетей, сетевая среда и сетевые устройства.
6. Технологии подключения к Интернет.
7. Конвергентные сети. Качество и надежность сетей.
8. Основные понятия сетевой безопасности.
9. Тенденции развития сетей.
10. Сетевые протоколы. Взаимодействие протоколов.
11. Набор протоколов TCP/IP и процесс обмена данными.
12. Организации по стандартизации: ISOC, IAB, IETF, IEEE, ISO.
13. Многоуровневые модели OSI и TCP/IP.
14. Инкапсуляция данных.
15. Протокольные блоки данных (PDU).
16. Доступ к локальным ресурсам.
17. Сетевая адресация. MAC- и IP- адреса.
18. Доступ к удалённым ресурсам.
19. Шлюз по умолчанию.
20. Сетевые протоколы и коммуникации
21. Протоколы и стандарты физического уровня.
22. Способы подключения к сети.
23. Сетевые интерфейсные платы (NIC).
24. Среды передачи данных и их характеристики: пропускная способность, производительность.
25. Виды медных сетевых кабелей: UTP, STP, коаксиальный.
26. Разновидности, особенности прокладки и тестирования кабелей.
27. Канальный уровень и его подуровни: Управление логическим каналом (LLC) и Управление доступом к среде передачи данных MAC.
28. Структура кадра канального уровня и принципы его формирования. Стандарты канального уровня. Физическая и логическая топология сети.
29. Топологии «точка-точка», «звезда», «полносвязанная», «кольцевая».
30. Сетевые технологии Ethernet
31. Семейство сетевых технологий Ethernet.
32. Принцип работы Ethernet.
33. Взаимодействие на подуровнях LLC и MAC.
34. Управление доступом к среде передачи данных (CSMA). MAC-адрес: идентификация Ethernet.
35. Атрибуты кадра Ethernet.
36. Представления MAC-адресов. Одно- и многоадресной, широковещательной рассылок.

37. Сквозное подключение, MAC- и IP-адреса.
38. Основная информация о портах коммутатора.
39. Таблица MAC-адресов коммутатора. Функция Auto-MDIX.
40. Способы пересылки кадра на коммутаторах Cisco.
41. Буферизация памяти на коммутаторах.
42. Фиксированная и модульная конфигурации коммутаторов.
43. Сравнение коммутации уровня 2 и уровня 3. Технология Cisco Express Forwarding.
44. Виртуальный интерфейс коммутатора (SVI), Маршрутизируемый порт, EtherChannel уровня 3. Конфигурация маршрутизируемого порта.
45. Сетевой уровень в процессе передачи данных.
46. Протоколы сетевого уровня. Основные характеристики IP-протокола.
47. Структура пакетов IPv4 и IPv6. Особенности и преимущества протокола Pv6. Методы маршрутизации узлов. Таблица маршрутизации узлов и маршрутизатора для протоколов IPv4 и IPv6.
48. Устройство маршрутизатора – процессор, память, операционная система. Подключение к маршрутизатору через различные порты.
49. Настройка исходных параметров, интерфейсов, шлюза по умолчанию и других характеристик маршрутизатора
50. Назначение и задачи транспортного уровня.
51. Мультиплексирование сеансов связи.
52. Описание и сравнение протоколов TCP и UDP – надежность и производительность, область применения. Адресация портов и сегментация TCP и UDP.
53. Обмен данными по TCP. Процессы TCP сервера.
54. Установление TCP-соединения и его завершение.
55. Принципы «трёхстороннего рукопожатия» TCP. Надёжность и управление потоком TCP –
56. Структура IPv4-адресов.
57. Сетевая и узловая часть IP-адреса.
58. Преобразование адресов между двоичным и десятеричным представлением.
59. Маска подсети IPv4. Сетевой адрес, адрес узла и широковещательный адрес сети IPv4. Присвоение узлу статического и динамического IPv4-адреса.
60. Многоадресная передача. Публичные и частные IPv4-адреса. IPv4-адреса специального назначения. Присвоение IP-адресов.
61. Структуры локального и глобального индивидуальных IPv6-адресов.
62. Статическая и динамическая конфигурации глобального индивидуального адреса.
63. ICMP-сервисы.
64. Отличия для протоколов IPv4 и IPv6.
65. Сегментация IP-сетей. Обмен данными между подсетями.
66. Планирование адресации в подсетях. Расчетные формулы для сегментации сети.
67. Разбиение на подсети на основе требований узлов и сетей, в соответствии с требованиями сетей.
68. Определение маски подсети. Разбиение на подсети с использованием маски переменной длины (VLSM).
69. Базовая модель и назначение блоков адресов VLSM.
70. Планирование адресации сети.
71. Особенности проектирования IPv6-сети.
72. Разбиение на подсети с использованием идентификатора интерфейса.
73. Служба доменных имён (DNS).
74. Формат сообщений и иерархия DNS.
75. Утилита «nslookup».
76. Служба DHCP.
77. Протокол передачи файлов (FTP).
78. Протокол обмена блоками серверных сообщений (SMB).

79. Концепции «Всеобъемлющий Интернет» BYOD.
80. Доставка данных по конвергентным сетям.
81. Планирование и создание небольшой компьютерной сети: определение ключевых факторов, выбор топологии и сетевых устройств, выбор и настройка протоколов, системы адресации.
82. Меры по обеспечению безопасности сети.
83. Уязвимости и сетевые атаки.
84. Разведывательные атаки, Атаки доступа, Отказ в обслуживании (DoS-атаки).
85. Резервное копирование, обновление и установка исправлений.
86. Межсетевые экраны.
87. Аутентификация, авторизация и учёт.
88. Включение протокола SSH.
89. Файловые системы маршрутизаторов и коммутаторов.
90. Резервное копирование и восстановление с помощью текстовых файлов, протокола TFTP, USB-накопителя.
91. Встроенные службы маршрутизации.
92. Поддержка беспроводных подключений.
93. Настройка встроенного маршрутизатора.

Тема 1.2. Принципы маршрутизации и коммутации

1. Объединённые сети.
2. Иерархия в коммутируемой сети.
3. Роль коммутируемых сетей. Коммутируемая среда. Динамическое заполнение таблицы MAC-адресов коммутатора.
4. Методы пересылки на коммутаторе.
5. Коммутация с промежуточным хранением. Сквозная коммутация.
6. Коммутационные домены. Снижение перегрузок сети
7. Основные концепции и настройка коммутации.
8. Первоначальная настройка коммутатора и восстановление после системного сбоя. Настройка доступа для базового управления коммутатором с IPv4. Дуплексная связь.
9. Настройка портов коммутатора на физическом уровне.
10. Поиск и устранение проблем на уровне доступа к сети.
11. Безопасность коммутатора. Защищённый удалённый доступ. Настройка SSH.
12. Распространённые угрозы безопасности: переполнение таблицы MAC-адресов, DHCP-спуфинг, использование уязвимостей протокола CDP, Атаки Telnet и др.
13. Аудит и практические рекомендации по обеспечению безопасности сети.
14. Безопасность порта коммутатора.
15. Отслеживание DHCP сообщений. Функция безопасности порта.
16. Виды защиты MAC-адресов.
17. Режимы реагирования на нарушение безопасности. Проверка и настройка портов. Протокол сетевого времени (NTP).
18. Виртуальные локальные сети (VLAN) – классификация и основные характеристики.
19. Транки виртуальных сетей.
20. Контроль широковещательных доменов в сетях VLAN.
21. Реализации виртуальной локальной сети. Назначение портов сетям VLAN.
22. Настройка транковых каналов.
23. Протокол динамического создания транкового канала (DTP).
24. Поиск и устранение неполадок в виртуальных локальных сетях и транковых каналах.
25. Проблемы с IP-адресацией сети VLAN. Несовпадения режимов транковой связи.
26. Проектирование и обеспечение безопасности VLAN: hopping, спуфинг коммутатора, атака с двойным тегированием, Сеть PVLAN периметра.
27. Практические рекомендации по проектированию виртуальной локальной сети.
28. Настройка маршрутизатора. Механизмы пересылки пакетов.

29. Подключение и настройка устройств. Светодиодные индикаторы на маршрутизаторе.
30. Активация и настройка IP-адресации.
31. Проверка связности сетей с прямым подключением.
32. Проверка настроек интерфейса.
33. Фильтрация выходных данных команд «show». Коммутация пакетов между сетями. Функция коммутации маршрутизатора. Маршрутизация пакетов.
34. Определение пути. Процесс принятия решения о пересылке пакетов. Выбор оптимального пути.
35. Анализ таблиц маршрутизации – источник данных, принципы формирование возможности настройки.
36. Записи таблицы маршрутизации для сетей с прямым подключением.
37. Задание статических маршрутов. Протоколы динамической маршрутизации сетей IPv4 и IPv6.
38. Принципы работы маршрутизации между VLAN.
39. Настройка маршрутизации на базе маршрутизаторов с несколькими физическими интерфейсами, с использованием конфигурации router-on-a-stick, через многоуровневый коммутатор.
40. Проблемы маршрутизации между VLAN. Проверка конфигурации коммутатора и настроек маршрутизатора. Неполадки в работе интерфейса.
41. Ошибки в IP-адресах и масках подсети. Настройка и работа коммутации на 3-м уровне. Маршрутизация между VLAN через виртуальные интерфейсы коммутатора, маршрутизируемые порты.
42. Преимущества и задачи статической маршрутизации.
43. Типы статических маршрутов: стандартный, по умолчанию, суммарный, плавающий. Настройка статических маршрутов IPv4 и IPv6.
44. Классовые маски подсети.
45. Объединение маршрутов. Организация суперсетей.
46. Использование масок подсети фиксированной длины (FLSM).
47. Объединение сетевых адресов IPv4 и IPv6.
48. Поиск и устранение неполадок в настройках статического маршрута и маршрута по умолчанию.
49. Протоколы динамической маршрутизации – назначение, принципы работы и история развития. Сравнение динамической и статической маршрутизации.
50. Принципы работы протоколов маршрутизации: пуск после включения питания, Сетевое обнаружение, Обмен данными маршрутизации, Обеспечение сходимости.
51. Классификация протоколов маршрутизации.
52. Протоколы IGP и EGP.
53. Классовые и бесклассовые протоколы маршрутизации.
54. Характеристики и метрики протоколов.
55. Динамическая дистанционно-векторная маршрутизация.
56. Дистанционно-векторный алгоритм.
57. Механизмы отправки и получения данных маршрутизации, расчёта оптимальных путей и добавления маршрутов в таблицу маршрутизации, обнаружения и реагирования на изменения в топологии.
58. Лавинная рассылка пакетов состояния канала. Лавинная рассылка пакетов состояния канала. Недостатки протоколов маршрутизации по состоянию канала.
59. Процесс поиска маршрута.
60. Семейство протоколов OSPF. Характеристики, принципы работы и компоненты OSPF. Особенности OSPF для одной и нескольких областей.
61. Режим конфигурации идентификаторы маршрутизатора.
62. Настройка пассивных интерфейсов.
63. Настройка значений пропускной способности интерфейса.

64. Проверка соседних устройств, настроек протокола, данных процесса и других характеристик OSPF.
65. Сравнение OSPFv2 и OSPFv3.
66. Списки контроля доступа (ACL).
67. Принцип работы ACLсписков. Типы ACL-списков Cisco для IPv4.
68. Присваивание номеров и имён ACL-спискам. Расчёт шаблонной маски в ACL-списках. Рекомендации по созданию и размещению ACL-списков.
69. Размещение стандартных и расширенных ACL-списков. Настройка стандартного ACL-списка. Применение стандартных ACL-списков на интерфейсах. Комментарии к ACL-спискам.
70. Проверка и редактирование стандартных нумерованных ACLсписков. ACL-статистика. Защита портов VTY с помощью стандартного ACL-списка IPv4.
71. Структура и настройка расширенных ACL-списков для IPv4. Фильтрация трафика с использованием расширенных ACL-списков.
72. Поиск и устранение неполадок ACL-списков.
73. Распространённые ошибки ACL-списков. Сравнение ACL-списков для IPv4 и IPv6. Настройка и проверка ACL-списков для IPv6.
74. Протокол DHCP. DHCPv4: базовая операция, формат сообщений, сообщения обнаружения и предложения. Настройка, проверка и ретрансляция простого DHCPv4-сервера.
75. Настройка маршрутизатора в качестве DHCPv4-клиента. Настройка маршрутизатора класса SOHO. Поиск и устранение неполадок в работе маршрутизатора DHCPv4. Протокол DHCPv6. Автоматическая настройка адреса без отслеживания состояния (SLAAC). Принцип работы SLAAC с DHCPv6. DHCPv6 с и без отслеживания состояния. Процессы DHCPv6.
76. Настройка маршрутизатора в качестве DHCPv6-сервера и DHCPv6-клиента. Поиск и устранение неполадок в работе DHCPv6.
77. Преобразование сетевых адресов IPv4.
78. Концептуальное преобразование сетевых адресов (NAT).
79. Терминология и принципы работы NAT. Пространство частных IPv4-адресов. Статическое и динамическое преобразование сетевых адресов (NAT).
80. Преобразование адресов портов (PAT). Сравнение NAT и PAT. Преимущества и недостатки NAT. Анализ статического преобразования NAT.
81. Принцип работы динамического NAT Настройка и проверка NAT, PAT. Переадресация портов. Настройка NAT и протокола IPv6.
82. Поиск и устранение неполадок в работе NAT

Раздел 2. Организация, принципы построения и функционирования компьютерных сетей

1. Реализация проекта сети.
2. Проект иерархической сети.
3. Расширение сети.
4. Выбор сетевых устройств.
5. Коммутационное оборудование.
6. Маршрутизаторы. Управляющие устройства.
7. Понятия протокола spanning-tree.
8. Предназначение протокола spanning-tree.
9. Принцип работы STP. Типы протоколов STP. Настройка протокола STP.
10. Настройка PVST+. Настройка Rapid PVST+. Проблемы настройки STP.
11. Основные понятия агрегирования каналов.
12. Агрегирование каналов. Принцип работы EtherChannel. Настройка агрегирования каналов. Настройка EtherChannel. Проверка, поиск и устранение неполадок в работе EtherChannel
13. Расширенные параметры протокола OSPF для одной области.
14. Маршрутизация на уровнях распределения и ядра. OSPF в сетях с множественным доступом.
15. Распространение маршрута по умолчанию.

16. Точная настройка интерфейсов OSPF. Защита OSPF.
17. Устранение неполадок реализации протокола OSPF для одной области.
18. Составляющие процедуры поиска и устранения неполадок в работе OSPF для одной области.
19. Поиск и устранение неполадок в маршрутизации OSPFv2 для одной области.
20. Поиск и устранение неполадок в OSPFv3 для одной области
21. Принцип работы OSPF для нескольких областей.
22. Назначение OSPF для нескольких областей.
23. Принцип работы пакетов LSA в OSPF для нескольких областей.
24. Таблица маршрутизации и типы маршрутов OSPF.
25. Настройка OSPF для нескольких областей.
26. Настройка OSPF для нескольких областей. Объединение маршрутов OSPF.
27. Проверка OSPF для нескольких областей.
28. Обзор технологий глобальной сети.
29. Цель создания глобальных сетей.
30. Принцип работы глобальной сети. Выбор технологии глобальной сети.
31. Сервисы глобальной сети. Инфраструктуры частных глобальных сетей.
32. Инфраструктура общедоступной глобальной сети. Выбор сервисов глобальной сети.
33. Обзор последовательного соединения «точка-точка». Связь по последовательному каналу.
34. Инкапсуляция HDLC.
35. Принцип работы протокола PPP. Преимущества протокола PPP. LCP и NCP. Сеансы PPP.
36. Настройка протокола PPP. Настройка протокола PPP. Аутентификация PPP. Отладка соединений WAN. Отладка PPP.
37. Удалённая работа. Преимущества удалённой работы. Бизнес-требования для удалённых работников.
38. Сравнение решений широкополосного доступа.
39. Кабель. DSL. Беспроводные широкополосные сети.
40. Выбор решений широкополосного доступа. Настройка подключений xDSL. Обзор PPPoE. Настройка PPPoE
41. Сети VPN. Основы сетей VPN. Типы сетей VPN.
42. Туннели GRE между объектами. Основы GRE. Настройка туннелей GRE.
43. Общие сведения об IPsec. Защита протокола IP. Структура протокола IPsec. Удалённый доступ. Решения VPN для удалённого доступа.
44. Сети VPN удалённого доступа с использованием IPsec.
45. Syslog. Принцип работы Syslog. Настройка Syslog. SNMP. Принцип работы SNMP.
46. Настройка SNMP. NetFlow. Принцип работы NetFlow. Настройка NetFlow. Проверка моделей трафика.
47. Поиск и устранение неполадок с использованием системного подхода.
48. Документация по сети. Процедура поиска и устранения неполадок. Изоляция проблемы с помощью многоуровневых моделей.
49. Отладка сети. Средства поиска и устранения неполадок.
50. Симптомы и причины отладки сети. Поиск и устранение неполадок связи в сетях IP.

Критерии оценки:

Оценку «отлично» заслуживает студент, обнаруживший всесторонние, систематические и глубокие знания по вопросам программного материала; показавший умение свободно логически анализировать литературу, рекомендованную программой, правильно оценивать и четко, сжато, ясно излагать свою точку зрения по проблемам; проявивший творческие способности в процессе изложения учебного материала; продемонстрировавший в процессе изложения учебного материала на экзамене твердые навыки и умение приложить теоретические знания к практическому их применению при дальнейшем обучении и в последующей профессиональной деятельности.

Оценку «хорошо» заслуживает студент, обнаруживший полное знание программного

материала; показавший систематический характер знаний, успешно, без существенных недочетов, ответивший на все вопросы экзаменационного билета, но некоторые ответы являются не совсем полными; при ответах на дополнительные вопросы студент обнаруживает знания логических связей вопросов билета с другими разделами курса, но ответы недостаточно четкие. Студент потенциально способен к овладению знаниями и обновлению их в ходе дальнейшей учебы и предстоящей профессиональной деятельности.

Оценку «удовлетворительно» заслуживает студент, обнаруживший знание основных вопросов дисциплины в объеме необходимом для дальнейшей учебы и предстоящей работы по профессии; умеющий выполнить задания, предусмотренной программой, знакомый с основной учебной литературой, рекомендованной программой; допустивший непринципиальные погрешности в ответе на экзамене и обладающий знаниями для их устранения как самостоятельно, так и под руководством экзаменатора.

Оценка «неудовлетворительно» выставляется студенту обнаружившему пробелы в знаниях основного программного материала; допустившему принципиальные ошибки в выполнении предусмотренных программой заданий экзаменационного билета и не способному к их исправлению без дополнительных занятий по дисциплине.

Приложение 2

ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ ИВАНОВСКОЙ ОБЛАСТИ

ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

«КИНЕШЕМСКИЙ ТЕХНОЛОГИЧЕСКИЙ КОЛЛЕДЖ»

Темы рефератов

1. Интернет и современные сетевые технологии – область применения и назначение.
2. Виды компьютерных сетей.
3. Технологии подключения к Интернет.
4. Основные понятия сетевой безопасности.
5. Тенденции развития сетей.
6. Сетевые протоколы и коммуникации
7. Разновидности, особенности прокладки и тестирования кабелей.
8. Сетевые технологии Ethernet
9. Принцип работы Ethernet.
10. Основная информация о портах коммутатора.
11. Сетевой уровень в процессе передачи данных.
12. Устройство маршрутизатора – процессор, память, операционная система. Подключение к маршрутизатору через различные порты.
13. Мультиплексирование сеансов связи.
14. Определение маски подсети. Разбиение на подсети с использованием маски переменной длины (VLSM).
15. Планирование и создание небольшой компьютерной сети: определение ключевых факторов, выбор топологии и сетевых устройств, выбор и настройка протоколов, системы адресации.
16. Меры по обеспечению безопасности сети.
17. Уязвимости и сетевые атаки.
18. Настройка встроенного маршрутизатора.
19. Иерархия в коммутируемой сети.
20. Безопасность порта коммутатора.
21. Проектирование и обеспечение безопасности VLAN: hopping, спуфинг коммутатора, атака с двойным тегированием, Сеть PVLAN периметра.
22. Практические рекомендации по проектированию виртуальной локальной сети.
23. Настройка маршрутизатора. Механизмы пересылки пакетов.
24. Маршрутизация пакетов.
25. Преимущества и задачи статической маршрутизации.
26. Поиск и устранение неполадок в настройках статического маршрута и маршрута по умолчанию.
27. Классовые и бесклассовые протоколы маршрутизации.
28. Характеристики и метрики протоколов.
29. Динамическая дистанционно-векторная маршрутизация.
30. Дистанционно-векторный алгоритм.
31. Процесс поиска маршрута.
32. Поиск и устранение неполадок в работе NAT
33. Коммутационное оборудование.
34. Основные понятия агрегирования каналов.
35. Обзор технологий глобальной сети.
36. Поиск и устранение неполадок с использованием системного подхода.
37. Документация по сети. Процедура поиска и устранения неполадок. Изоляция проблемы с помощью многоуровневых моделей.

Примерная структура реферата

- Титульный лист.
- Оглавление – излагается название составляющих (глав, вопросов) реферата, указываются страницы.
- Введение – формулируется суть исследуемой проблемы ее актуальность, обосновывается выбор темы. Указывается цель и задачи. Показывается научный интерес и практическое значение. Объем введения составляет 2-3 страницы.
- Основная часть – доказательно раскрывается проблема или одна из ее сторон; могут быть представлены таблицы, графики, схемы. Основная часть должна включать в себя также собственное мнение студента.
- Заключение – подводятся итоги или дается обобщенный вывод по теме реферата, указывается, что интересно, что спорно, предлагаются рекомендации.
- Объем заключения 2-3 страницы.
- Список литературы – источники должны быть перечислены в алфавитной последовательности (по фамилии автора или по названию сборников), необходимо указать место издания, название издательства, год, источники (библиография, не менее 20 наименований, в том числе 2-3 иностранных). Оформление списка литературы по ГОСТ 71-2003 «Библиографическая запись, Библиографическое описание. Общие требования и правила составления».
- Выступление по реферату.
- На основе написанного реферата студент может сделать устное выступление перед группой, либо другой аудиторией. Рефераты могут быть представлены на семинарах, научно-практических конференциях, а также использоваться как зачетные работы (в отдельных случаях) или сообщение на практическом занятии (семинаре). При этом преподавателем оценивается предметная сущность выполненного самостоятельного исследования, способность к письменному изложению изучаемого вопроса, правильность выводов, способность публичного выступления и ответов на вопросы, умение вести дискуссию по теме исследования, правильность и грамотность оформления документа.

Рекомендации к оформлению реферата

- Абзац включает в себя не менее 3-х предложений.
- Название каждой главы начинается с новой страницы, объем главы не может быть меньше 2 страниц.
- В тексте должны отсутствовать сокращения, кроме общепринятых, общепринятые или необходимые сокращения при первоначальном употреблении должны быть расшифрованы.
- Каждая цитата, каждый рисунок или график, каждая формула, каждый расчет должны иметь сноску. Если рисунок или расчет являются авторскими, тогда это необходимо отразить в тексте сноски.
- Работа предоставляется как в рукописном виде (почерк читаемый, т.е. разборчивый), так и в напечатанном виде через 1-1.5 интервала. Шрифт – TimesNewRoman, размер шрифта – 12-14. Вся работа должна быть напечатана в одном виде шрифта, если это не смысловое выделение по тексту.

Список использованной литературы и других источников составляется в следующей последовательности:

- Законы, постановления правительства.
- Нормативные акты, инструктивные материалы, официальные справочники.
- Специальная литература.
- Периодические издания.

Приложение 3

ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ ИВАНОВСКОЙ ОБЛАСТИ

ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

«КИНЕШЕМСКИЙ ТЕХНОЛОГИЧЕСКИЙ КОЛЛЕДЖ»

Билеты к экзамену

Экзаменационный билет №1

1. Компьютерные сети. Типы сетей передачи данных.
2. Трансляция сетевых адресов NAT. Назначение и основные виды NAT. Перегруженный NAT.
3. Построить сеть на основе коммутатора и четырёх ПК. Используя различные маски переменной длины, изолировать трафик ПК1 и ПК2 от ПК3 и ПК4.

Преподаватель_____ М.О. Шаронов

Экзаменационный билет №2

1. Понятие сетевого протокола. Основные типы сетевых протоколов.
2. Настройка протокола динамической маршрутизации OSPFv2.
3. Имеется сеть на основе двух L2-коммутаторов. К каждому коммутатору подключены по три ПК. Создать три сетевых сегмента на основе VLAN, по одному сегменту на каждом коммутаторе и третий сегмент сделать
распределённый по двум коммутаторам.

Преподаватель_____ М.О. Шаронов

Экзаменационный билет №3

1. Модель OSI. Уровни передачи данных. Основные функции уровня.
2. Протокол динамической маршрутизации EIGRP. Особенности, преимущества и недостатки.
3. Построить сеть на основе двух L2-коммутаторов с конфигурационной петлёй, т.е. коммутаторы соединены двумя линками. К каждом коммутатору подключены по два ПК. Настроить работу EtherChannel между коммутаторами.

еподаватель_____ М.О. Шаронов

Экзаменационный билет №4

1. Адресация в сетях передачи данных. Сетевые IP-адреса
2. Диагностика неисправностей в работе протокола динамической маршрутизации EIGRP.
3. Построить сеть на основе двух L2-коммутаторов и четырёх подключенных к ним ПК, по два к каждому. Задать на каждом коммутационном сегменте разные маски и адреса. Подключить L2-коммутаторы к маршрутизатору и настроить получить на нём связь двух сегментов коммутации.

Преподаватель_____ М.О. Шаронов

Экзаменационный билет №5

1. Основы коммутации. Коллизии, домен коллизий. Широковещательный домен. Симметричное и асимметричное коммутирование.
2 Соединение «точка-точка». Протокол PPPoE.
3. Построить сеть на основе двух L3 -коммутаторов и двух подключенных к ним ПК, по одному к каждому. Выставить на каждом ПК IP-адреса из разных классов. Прописать на каждом маршрутизаторе дефолтные маршруты так, чтобы ПК могли пинговать друг друга

Экзаменационный билет №6

1. Виртуальные локальные сети VLAN. Порты доступа и транковые порты.
2. Мониторинг сети. Мониторинг web-сервера. Утилита tcpdump.
3. Построить сеть на основе двух маршрутизаторов и двух подключенных к ним ПК, по одному к каждому. Выставить на каждом ПК IP-адреса из разных классов. Прописать на каждом маршрутизаторе дефолтные маршруты так, чтобы ПК могли пинговать друг друга.

Преподаватель_____ М.О. Шаронов

Экзаменационный билет №7

1. Основы маршрутизации. Метрика, домен маршрутизации, конвергенции в сетях.
2. Поиск и устранение неполадок в сети. Отладка сети.
3. Построить сеть на основе L2-коммутатора, двух подключенных к нему ПК и одного сервера. Настроить на сервере протокол динамической адресации DHCP. Получить на каждом ПК IP- адреса от DHCP-сервера.

Преподаватель_____ М.О. Шаронов

Экзаменационный билет №8

1. Статическая маршрутизации. Её достоинства и недостатки. Особенности настройки и диагностики.
2 Основы сетевой безопасности. Назначение и основные функции протокола AAA.
3. Построить сеть на основе двух маршрутизаторов. К первому маршрутизатору подключен ПК, имитирующий ЛВС, ко второму маршрутизатору подключен сервер, имитирующий сервер провайдера. Между маршрутизаторами имеет кроссовый линк. Настроить на маршрутизаторе ЛВС NAT типа PAT

Преподаватель_____ М.О. Шаронов

Экзаменационный билет №9

1. Протоколы динамической маршрутизации RIP и RIPv2. Особенности, преимущества и недостатки.

2. Виртуальные частные сети VPN. Основные понятия и виды.
3. Построит сеть на основе трёх последовательно соединённых маршрутизаторов. К двум крайним маршрутизаторам цепочки подключены по одному ПК. Настроить на маршрутизаторах работу протокола OSPF так, чтобы ПК могли пинговать друг друга.

Преподаватель_____ М.О. Шаронов

Экзаменационный билет №10

1. Динамическая конфигурация и адресация сетевых узлов, протокол DHCP.
2. Виртуальные сети. Функция Anti-Replay, туннелирование. Динамические многоточечные виртуальные частные сети DMVPN.
3. Построить сеть на основе двух L2-коммутаторов, подключенных маршрутизатору. К каждому коммутатору подключены по два ПК, имеющие IP-адреса разных классов. Настроить маршрутизатор так, чтобы все ПК могли пинговать друг друга.

Преподаватель_____ М.О. Шаронов

Экзаменационный билет №11

1. Основные понятия протокола STP. Корневой и назначенный коммутатор. Расчёт стоимости маршрута. Состояния портов в STP.
2. Технология IPSec. Транспортный и туннельный режимы. Протокол управления ключами ISARMP.
3. Построить сеть на основе L2-коммутатора и четырёх подключенных к нему ПК. Настроить на ПК1 и ПК2 маски из класса B, а на ПК3 и ПК4 маски из класса C. Подключить L2- коммутатор к маршрутизатору и создать на нём стандартные списки доступа, позволяющие ПК1 «видеть» ПК3, но запрещающие связи: ПК1-ПК4 и ПК2-ПК3.

Преподаватель_____ М.О. Шаронов

Экзаменационный билет №12

1. Беспроводные локальные сети WLAN. Зона покрытия, пропускная способность, помехи, потребляемая мощность, стоимость. WAP, микросота.
2. Сетевые системы обнаружения вторжений.
3. Построить сеть на основе L2-коммутатора и четырёх подключенных к нему ПК. Выделить ПК1 и ПК2 в VLAN2, а ПК3 и ПК4 в VLAN3. Подключить L2-коммутатора к маршрутизатору. Настроить на маршрутизаторе расширенный список доступа разрешающий http-протокол между VLAN.

Преподаватель_____ М.О. Шаронов

Экзаменационный билет №13

1. Поиск и устранение неисправностей в беспроводных локальных сетях.
2. Сетевые эмуляторы. Назначение и основные функции Cisco Packet Tracer.
3. Построить сеть на основе L2-коммутатора, двух подключенных к нему ПК и одного публичного DMZ-сервера. Подключить Ь2-коммутатор к межсетевому экрану Sisco ASA. Межсетевой экран подключить к маршрутизатору провайдера, к которому также подключить сервер. Настроить на Cisco ASA инспектирование трафика таким образом, чтобы сервер, находящийся в локальной сети, был доступен из сети провайдера, но с данного сервера ЛВС была недоступна.

Преподаватель_____ М.О. Шаронов

Экзаменационный билет №14

1. Протоколы WLAN. Их классификация, различия, преимущества и недостатки. Wi-Fi.
2. Сетевые системы предотвращения вторжений
3. Построить сеть на основе L2-коммутатора и шести подключенных к нему ПК. Разделить все ПК на три VLAN (2, 3 и 4) по два ПК в каждой. Подключить L2-коммутатор к маршрутизатору. Настроить на маршрутизаторе списки доступа, разрешающие связь между VLAN2 и VLAN4.

Преподаватель_____ М.О. Шаронов

Экзаменационный билет №15

1. Агрегирование каналов на основе EtherChannel.
2. Протокол сетевого времени NTP. Назначение и алгоритм работы.
3. Построить сеть на основе L2-коммутатора и четырёх подключенных к нему ПК. Выделить ПК1 и ПК2 в VLAN2, а ПК3 и ПК4 в VLAN3. Подключить L2-коммутатора к маршрутизатору. Настроить на маршрутизаторе расширенный список доступа позволяющий выполнять пинг между VLAN.

Преподаватель_____ М.О. Шаронов

Экзаменационный билет №16

1 Масштабирование сетей. Принцип работы протокола STP, протокол RSTP.
2. Технология IPSec, её место в модели OSI. Протоколы AH и ESP.
3. Построить сеть на основе двух маршрутизаторов, к каждому из которых подключен ПК. Настроить на маршрутизаторах работу протокола динамической маршрутизации EIGRP.

Преподаватель_____ М.О. Шаронов

Экзаменационный билет №17

1. Протокол динамической маршрутизации OSPF и OSPFv2. Особенности, преимущества и недостатки.
2. Виртуальные частные сети VPN. Удалённый доступ (Remote Access) и создание распределённых виртуальных локальных сетей (Site-to-Site).
3. Построить сеть на основе L2-коммутатора, к которому подключены три ПК. Выделить каждый ПК в отдельную VLAN. Подключить L2-коммутатора транковым линком к L3-коммутатору. Настроить на Ь3-коммутаторе маршрутизацию между VLAN-сегментами на основе VLAN-интерфейсов.

Преподаватель_____ М.О. Шаронов

Экзаменационный билет №18

1 Динамическая маршрутизации. Её достоинства и недостатки. Особенности настройки и диагностики..
2. Технология IPSec, основные понятия. Протоколы PAP и CHAP. OTP и цифровые сертификаты. Биометрия, контекстуальные проверки.

3. Построить сеть на основе двух маршрутизаторов, к каждому из которых подключен ПК. Настроить на маршрутизаторах работу протокола динамической маршрутизации OSPF.

Преподаватель_____ М.О. Шаронов

Экзаменационный билет №19

1. Основы маршрутизации. Типы протоколов маршрутизации. Автономная система..
2. Протокол сетевого управления SNMP. Назначение, алгоритм работы.
3. Построить сеть на основе L2-коммутатора. Подключить L2-коммутатор к маршрутизатору. Настроить на маршрутизаторе работу DHCP-протокола. Получить на каждом ПК IP-адреса от DHCP-сервера..

Преподаватель_____ Ветюгов А.

Экзаменационный билет №20

1 Принцип маршрутизации. Типы маршрутов. Административное расстояние.
2. Широкополосный доступ, DSL. Типы широкополосного доступа, преимущества и недостатки.
3. Построить сеть на основе двух маршрутизаторов и двух подключенных к ним ПК, по одному к каждому. Выставить на каждом ПК IP-адреса из разных классов. Прописать на каждом маршрутизаторе статические, но не дефолтные, маршруты так, чтобы ПК могли пинговать друг друга.

Преподаватель_____ Ветюгов А.

Экзаменационный билет №21

1. Виртуальные локальные сети VLAN. Назначение, основные функции. VLAN по умолчанию.
2. Соединение «точка-точка». Протокол PPP. Протоколы LCP и NCP.
3. Построить сеть на основе двух L3 -коммутаторов и двух подключенных к ним ПК, по одному к каждому. Выставить на каждом ПК IP-адреса из разных классов. Прописать на каждом маршрутизаторе статические, но не дефолтные, маршруты так, чтобы ПК могли пинговать друг друга

Преподаватель_____ Ветюгов А.

Экзаменационный билет №22

1. Принцип коммутации. Симплексный, полудуплексный и дуплексный режимы. Одноадресная, многоадресная и широковещательная связь.
2. Диагностика неисправностей в работе протокола динамической маршрутизации OSPF.
3. Построить сеть на основе одного Ь2-коммутатора, к которому подключены четыре ПК. Выделить ПК1 и ПК2 в VLAN2, а ПК3 и ПК4 в VLAN3. Подключить коммутатор к маршрутизатору и настроить на нём связь между сегментами коммутации на основе sub-интерфейсов.

Преподаватель_____ Ветюгов А.

Приложение 3

ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ ИВАНОВСКОЙ ОБЛАСТИ

ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

«КИНЕШЕМСКИЙ ТЕХНОЛОГИЧЕСКИЙ КОЛЛЕДЖ»

Практические работы по ПМ.01 Выполнение работ по проектированию сетевой инфраструктуры

Содержание

Практическое занятие № 1 - Оконцовка кабеля витая пара

Тема: Оконцовка кабеля витая пара

Количество часов (лекцтя+практика) 2+4.

Цель работы:

1. Изучение обжима коннекторов 8P8C методом прямого соединения;
2. Изучение обжим коннекторов 8P8C методом кроссового соединения;
3. Развитие и закрепление интереса обучаемых к преподаваемому предмету.

Оборудование:

коннекторы 8P8C;

кабель витая пара;

кримпер;

кабель-тестер.

Ход работы:

Изучить методические указания к работе;

Осуществить обжим коннектора прямым методом;

Осуществить обжим коннектора кроссовым методом;

Проверить правильность соединения с помощью кабель-тестера.

Методические указания к выполнению:

Для 10Base-TX и 100Base-TX задействованы лишь оранжевые и зеленые проводки (контакты 1+2 и 3+6). Синюю пару часто используют для телефонных линий (контакты 4+5). Для технологий 1000Base-TX и ряда других менее популярных задействованы все 8 контактов, также для Gigabit технологий рекомендую использовать экранированную витую пару.

Рисунок 1 – Схема распределения проводников при прямом обжиме

Кросс-линковый (перекрестный) порядок обжима витой пары применяется в случае, когда требуется соединить между собой 2 концентратора, не имеющих переключения uplink/normal, а также для прямого соединения 2-х компьютеров. Меняются местами 2 пары: 1-2 на 3-6. Где-то с 2004 года устройства научились автоматически переставлять пары местами и кроссовый обжим утратил смысл.

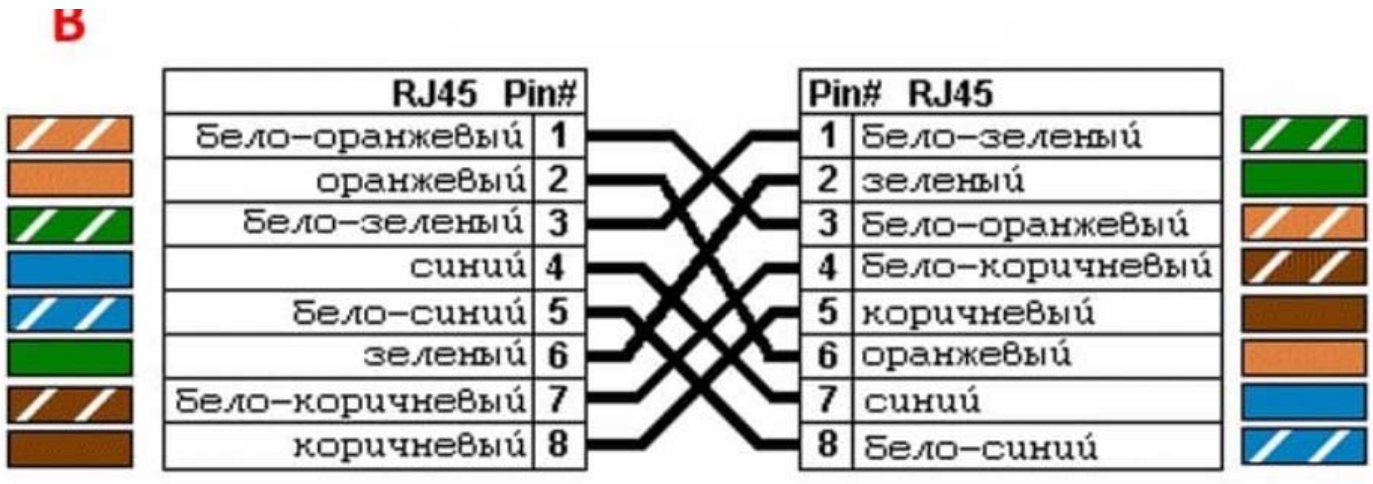


Рисунок 2 – Схема распределения проводников при кроссовом обжиме

Для стандарта Ethernet 100Base-T используются четыре жилы (оранжевая и зеленая пара), а оставшиеся четыре зарезервированы для стандарта Gigabit Ethernet (1000Base-T). Есть два варианта разводки 568A или 568B, выбор за Вами. Чаще используется второй вариант (568B). Самое главное чтобы во всей сети использовался один из вариантов.

Обжимаем витую пару

Многие считают, что это самый сложный этап прокладки сети, поскольку проводков так много, в них так легко запутаться, нужно покупать специальный обжимной инструмент и т.д. На самом деле все довольно просто. Для обжима витой пары вам потребуются специальные клещи и пара коннекторов RJ-45

Рисунок 3 – Обжимной инструмент RJ-45

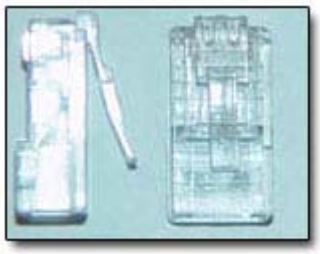


Рисунок 4 – Коннекторы RJ-45

Последовательность действий при обжиме:

1. Аккуратно обрежьте конец кабеля, при этом лучше всего пользоваться резаком, встроенным в обжимной инструмент.

2. Снимите с кабеля изоляцию. Можно использовать специальный нож для зачистки изоляции витой пары, его лезвие выступает ровно на толщину изоляции, так вы не повредите проводники. Впрочем, если нет специального ножа, можно воспользоваться обычным или взять ножницы.

3. Разведите и расплетите проводки, выровняйте их в один ряд, при этом соблюдая цветовую последовательность.

4. Обкусите проводки так, чтобы их осталось чуть больше сантиметра.

5. Вставляйте проводники в разъем RJ-45

6. Проверьте, правильно ли вы расположили проводки

7. Убедитесь все ли провода полностью вошли в разъем и уперлись в его переднюю стенку.

8. Поместите коннектор с установленной парой в клещи, затем плавно, но сильно произведите обжим.

.

Содержание отчета

1. Название работы.
2. Цель работы.
3. Выполнение заданий.
4. Проверка. Ответ.

4. Вопросы для самопроверки

1. Активное сетевое оборудование
2. Пассивное сетевое оборудование.
3. Перечислите виды сред передачи данных.
4. Как с помощью стандартных сетевых утилит проверить работоспособность сетевого адаптера
5. Почему концентратор и повторитель относят к пассивному сетевому оборудованию?

Критерии оценки:

1. Работа оценивается на «пять баллов», если все части задания выполнены верно и выводы сделаны правильно.

2. Работа оценивается на «четыре балла» если не выполнена одна часть задания, выводы сделаны правильно

3. Работа оценивается на «три балла» если не выполнены 2 части задания, выводы сделаны правильно

Список литературы

1. Олифер В. Г. Компьютерные сети : принципы, технологии, протоколы : учеб. пособие : гриф Минобрнауки РФ : пер. с англ. / В. Г. Олифер, Н. А. Олифер. – 4-е изд. – СПб. и др. : Питер, 2012. – 943 с. : ил. – (Учебник для вузов : стандарт третьего поколения) . – На рус. яз. – ISBN 978-5-459-00920-0 : 403.70.

2. Таненбаум Э., Уэзеролл Д. Т18 Компьютерные сети. 5-е изд. — СПб.: Питер, 2012. — 960 с.: ил.

3. Шевченко В.П. Вычислительные системы, сети и телекоммуникации : учебник / В.П. Шевченко. – М.:КНОРУС, 2012. – 288 с.

4. Первухин Д.А. Информационные сети и телекоммуникации: Учеб. пособие/Д.А. Первухин, О.В. Афанасьева, Ю.В. Ильюшин. - СПб.: «СатисЪ», 2015. - 267 с.

5. Головин Ю.А. Информационные сети : учебник для студ. учреждений высш. проф. образования / Головин Ю.А., Суконщиков А.А,., Яковлев С.А. – М. : Издательский центр «Академия», 2011. – 384 с. ISBN 978-5-7695-6459-8

6. Величко В.В. Основы инфокоммуникационных технологий. Учебное пособие для вузов / В.В. Величко, Г.П. Катунин, В.П. Шувалов; под редакцией профессора В.П. Шувалова. – М. : Горячая линия–Телеком, 2009. – 712 с.: ил. ISBN 978-5-9912-0055-4

Практическое занятие № 2 - Организация простейшей компьютерной сети с помощью коммутатора и концентратора

Тема: Разработка и создание простейшей одноранговой сети

Задание: Отчет по теме (пример в презентации урока)

Цель работы

Построить простейшую компьютерную сеть с использованием комму-таторов и концентраторов.

Задание

1. Запустить Cisco Packet Tracer.

2. Построить простейшую компьютерную сеть с использованием концентратора.

3. Построить простейшую компьютерную сеть с использованием коммутатора.

4. Сравнить работу этих сетей.

Краткая теория

Если в сети появляется более двух компьютеров, то для организации сети необходимо использовать специализированные устройства. Для этого используются концентраторы (Hub), которые функционируют на первом уровне модели OSI, либо как коммутаторы (Switch), которые работают на втором уровне модели OSI. Концентратор (Hub) повторяет сигналы, посту-пившие с одного из его портов на все остальные активные порты. Коммута-тор выполняет функции коммутации по заранее известным MAC-адресам.

Основное преимущество концентратора это его низкая стоимость. Он имеет следующие недостатки: невысокая скорость и отсутствие безопасно-сти. В настоящее время концентратор применяется довольно редко на ком-пьютерных сетях. Концентратор в отличие от коммутатора отправляет паке-ты на все порты, кроме порта источника. Так, например, если компьютер PC0 отправляет пакеты PC1, то концентратор отправляет этот пакет на все ком-пьютеры, которые к нему подключены, кроме порта источника.

Коммутатор в отличие от этого отправляет пакеты только на тот порт, который необходим. Происходит это за счет использования таблицы MAC-адресов, в которой за каждым портом коммутатора закреплен определенный MAC-адрес устройства.

Порядок выполнения работы

1. Запустить Cisco Packet Tracer;
2. Необходимо создать сеть, в которой имеется 4 компьютера. Для этого во вкладке END Devices выбираем персональные компьютеры PC, присваиваем им IP –адреса, как было показано в лабораторной работе №1. IP- адреса можно взять следующие: 192.168.1.1, 192.168.1.2, 192.168.1.3, 192.168.1.4. Маску класса С 255.255.255.0 оставляем. Присвоение IP-адреса PC0 показано на рисунке 1.

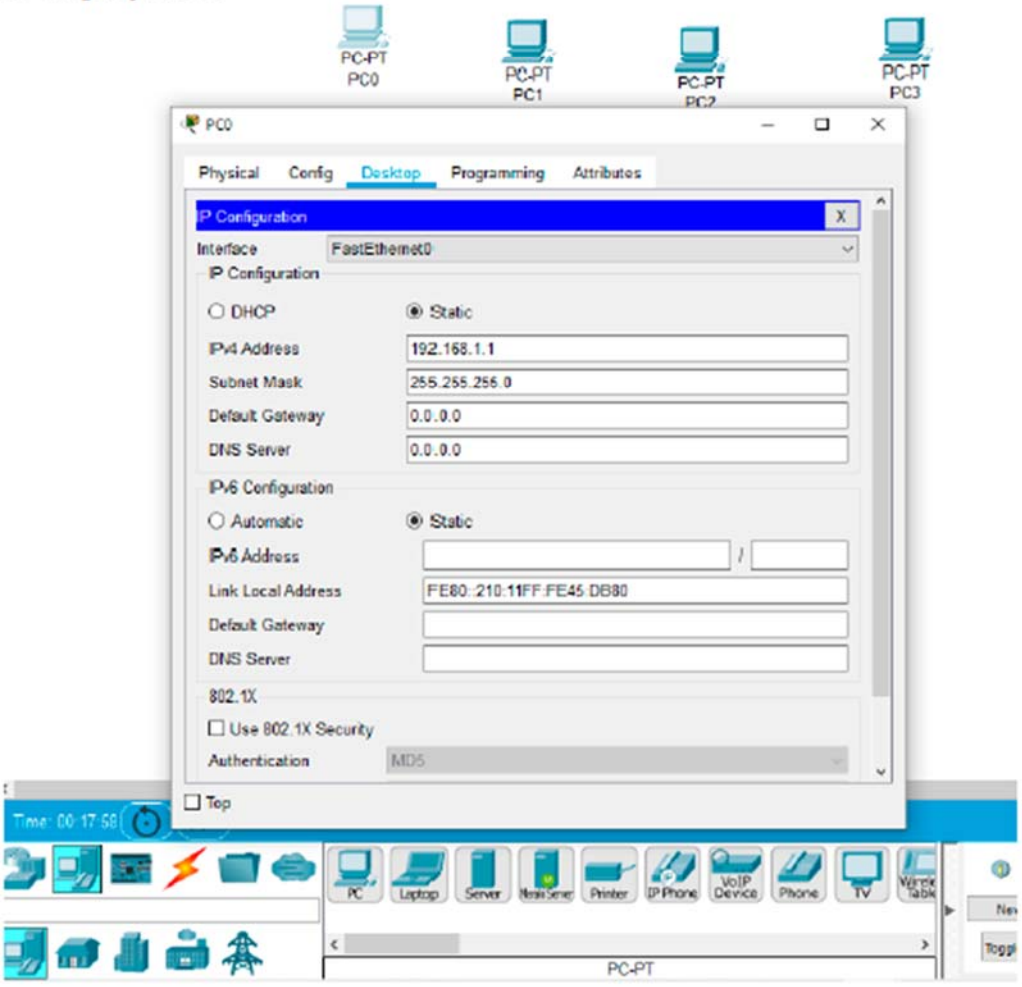
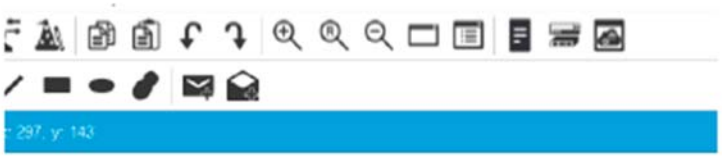


Рисунок 1 – Присвоение IP- адреса для PC0

3. Далее во вкладке Network Devices выбираем коммутатор. Возьмем самый распространенный коммутатор компании Cisco (Switch 2960 -24 TT). Далее выбираем тип кабеля. Выбираем прямой кабель. У PC0 берем единственный порт FastEthernet0 (рис.2). Для соединения коммутатора с PC0 выбираем на нем первый порт FastEthernet0/1 (рис. 3).

4.



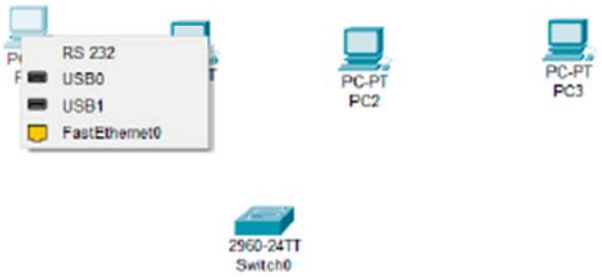


Рисунок 2 – Выбор порта FastEthernet0 на PC0 для соединения с коммутатором

Аналогично соединяем остальные компьютеры с коммутатором. В результате получаем следующую сеть. На компьютерах зеленые линии загорелись сразу (рис. 4), а коммутаторам требуется некоторое время. Как только линии загорелись зелеными, наша сеть начинает функционировать (рис. 5).

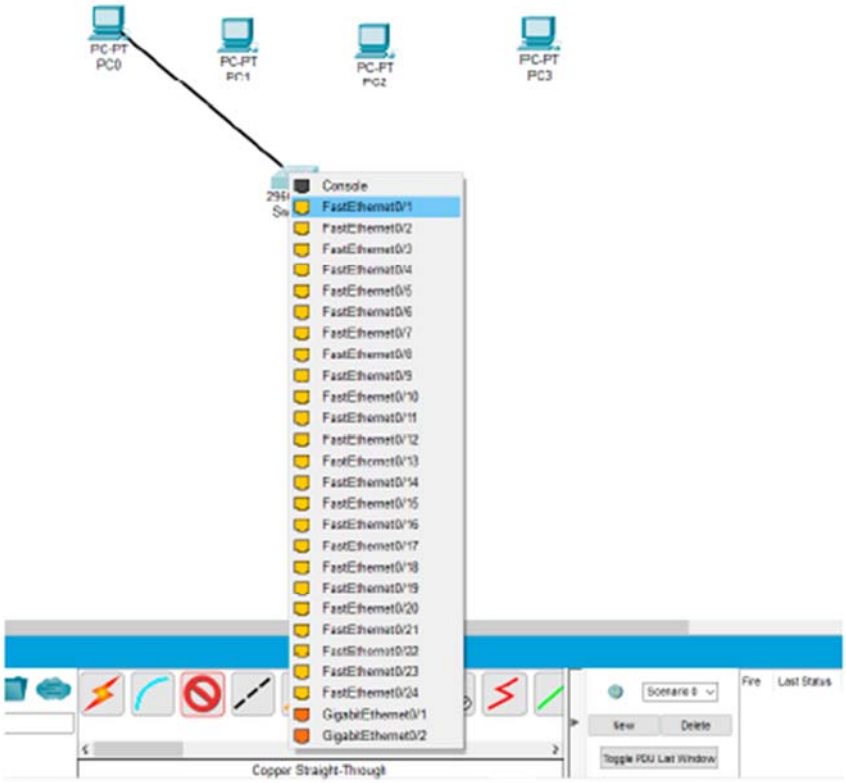


Рисунок 3 – Выбор порта FastEthernet0/1 на коммутаторе для соединения с PC0

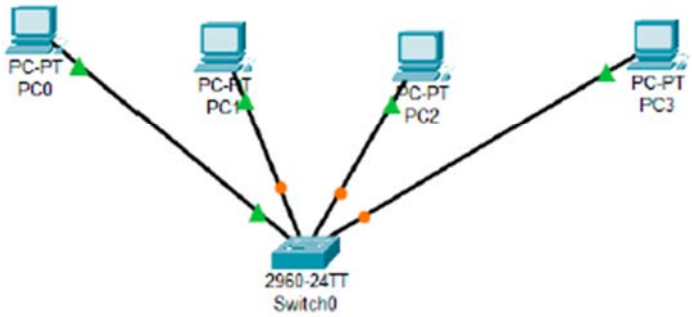


Рисунок 4 – Линии между компьютерами и коммутаторами находятся в неактивном режиме

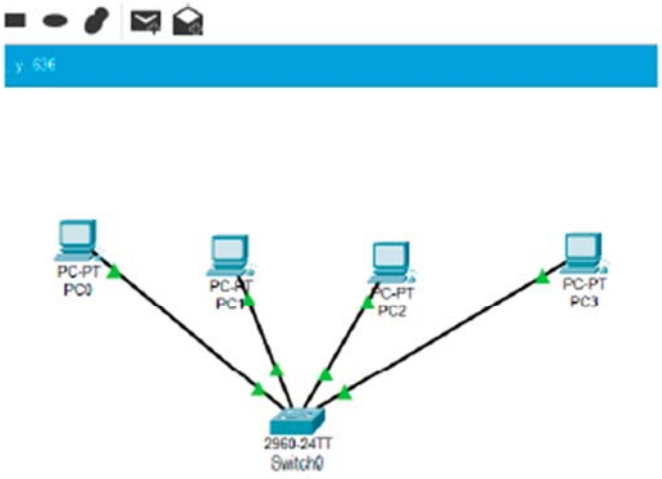


Рисунок 5 – Линии между компьютерами и коммутаторами находятся в активном режиме

Можно щелкнуть левой кнопкой мыши на коммутаторе и посмотреть его порты. Во вкладке Physical показано, что на коммутаторе имеется 24 порта FastEthernet и 2 порта GigabitEthernet (рис. 6).

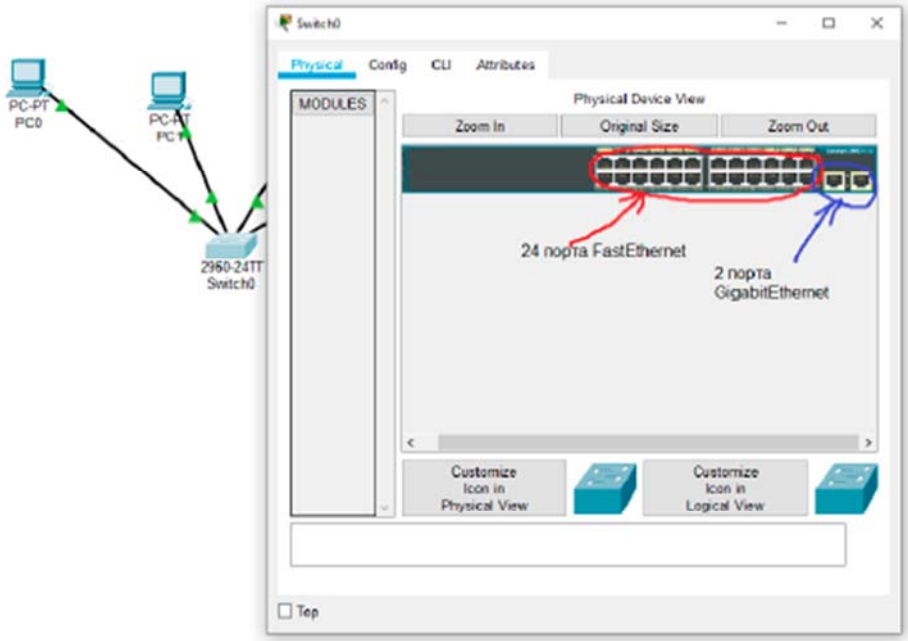


Рисунок 6 – Порты на коммутаторе

Далее необходимо проверить работоспособность этой сети. Эту функцию мы уже проверяли в лабораторной работе №1. Для этого один раз

нажмите левой кнопкой мыши на устройстве PC0 и перейдите в закладку Desktop, а затем нажмите Command Prompt . Введите команду:

C:\>ping 192.168.1.2

Аналогично проверьте взаимодействие с другими компьютерами сети и введите их IP- адреса:

C:\>ping 192.168.1.3

C:\>ping 192.168.1.4.

Результат выполнения данной команды приведен на рисунке 7.

Аналогичную проверку можно осуществить и на других компьютерах сети.

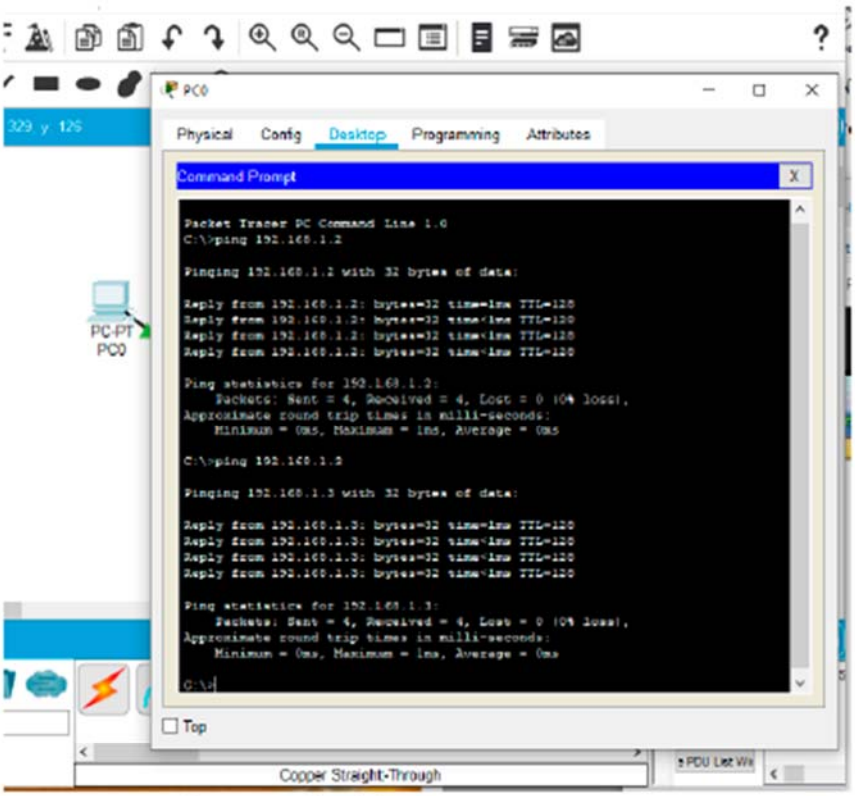


Рисунок 7 – Проверка связности построенной сети

Теперь построим вторую сеть на концентраторе (Hub). Чтобы ускорить процесс создания сети, выделяем 4 компьютера (рис. 8), нажимаем Ctrl и перетаскиваем их вниз (рис. 9). Далее заходим во вкладку Hubs и выбираем концентратор (рис. 10).

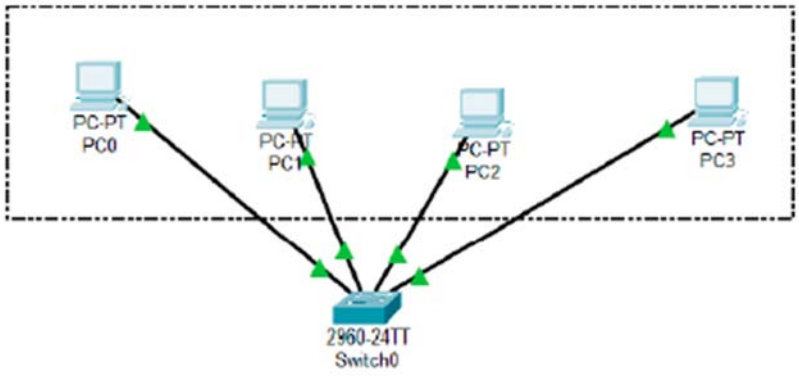


Рисунок 8 – Выделяем компьютеры для создания второй сети

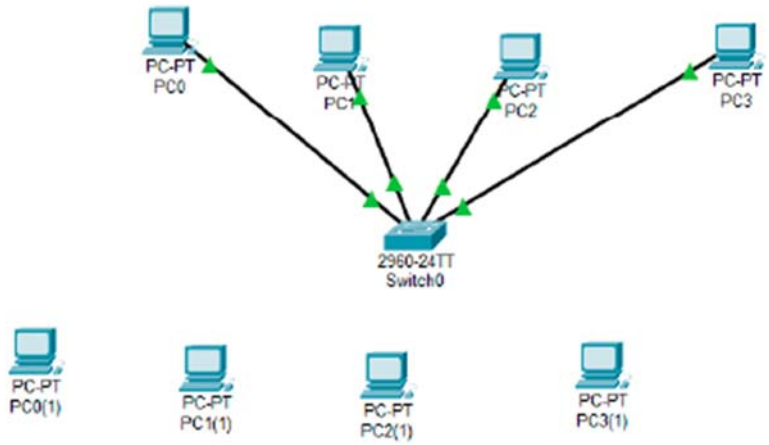


Рисунок 9 – Четыре вновь созданных компьютера для второй сети

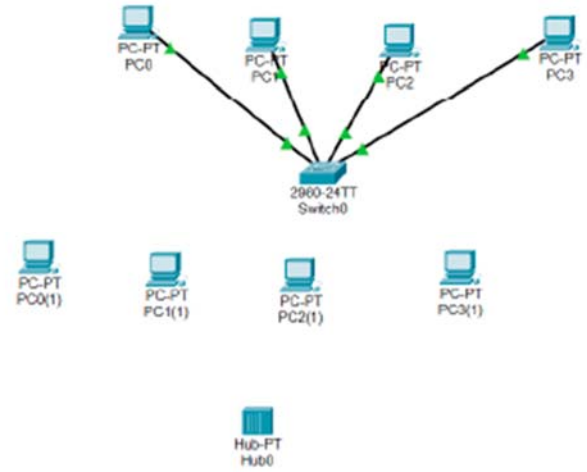


Рисунок 10 – Выбор концентратора (Hub) для второй сети

Далее соединяем компьютеры с концентратором с помощью кабеля. В Cisco Packet Tracer можно автоматически выбрать кабель (рис. 11). Выбираем автоматический выбор и подключаем компьютеры к концентратору (рис.12).

Рисунок 11 – Автоматический выбор кабеля в Cisco Packet Tracer

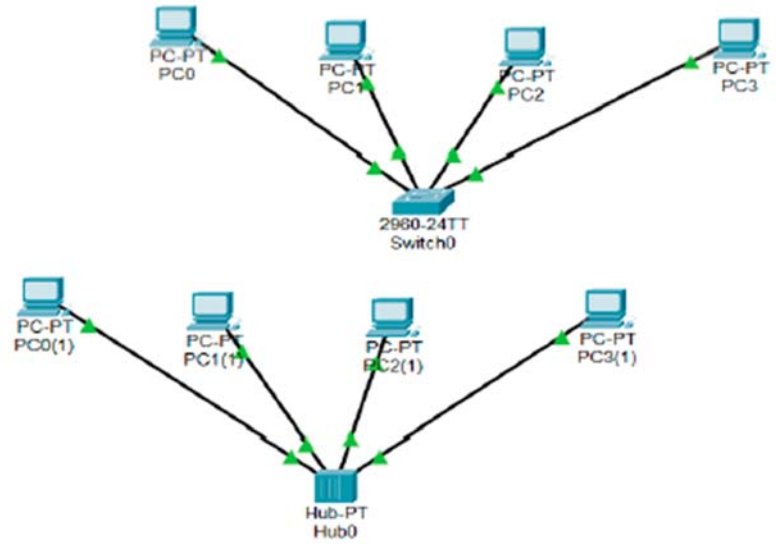


Рисунок 12 – Построение двух компьютерных сетей

Здесь линии сразу загораются зеленым цветом. Проверим работоспособность второй сети (рис. 13). Сеть успешно функционирует.

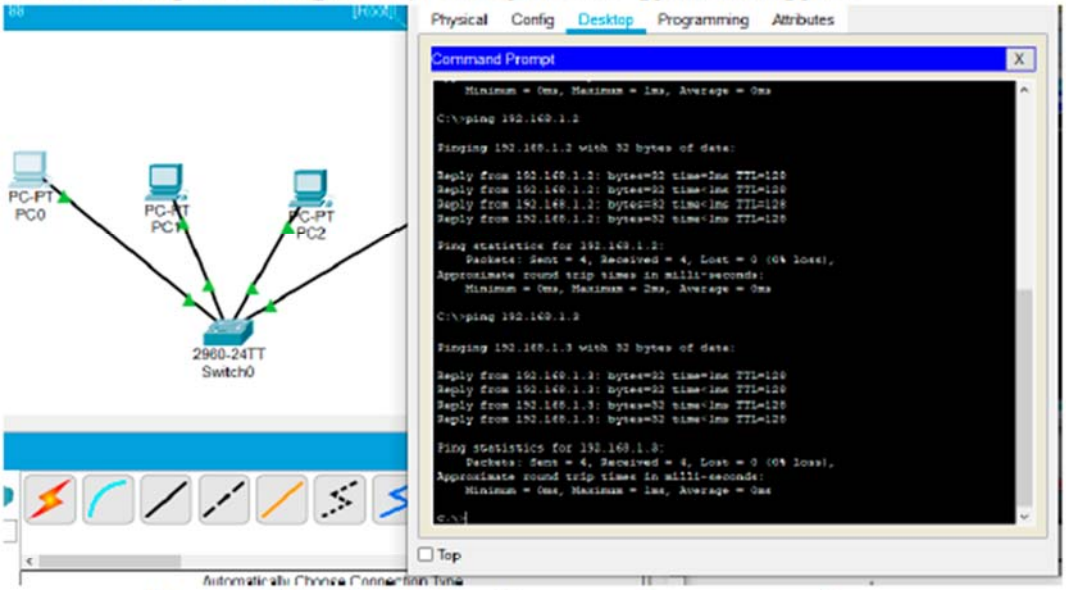


Рисунок 13 – Проверка работоспособности второй сети

Для визуализации процесса прохождения пакета воспользуемся функцией Add Simple PDU. Предположим, что компьютер PC0 отправляет пакет на компьютер PC1. То же самое будет происходить и во второй сети.

Для того, чтобы задать маршрут следования пакета необходимо нажать сначала на PC0, а затем на PC1, т.е. пакеты будут отправлены от компьютера PC0 к PC1.

Далее переходим во вкладку Simulation Mode (Режим моделирования), перетаскиваем синий ползунок влево и можем детально просмотреть передвижение пакета. Переходим во вкладку Play Controls и нажимаем на кнопку Capture then forward для анимации пакета (рис. 14). Пакет начинает передвигаться от PC0 к PC1. Пакет в первой сети приходит на коммутатор, а во второй сети на концентратор. После этого опять нажимаем на кнопку Capture then forward и пакет продолжает свое движение.

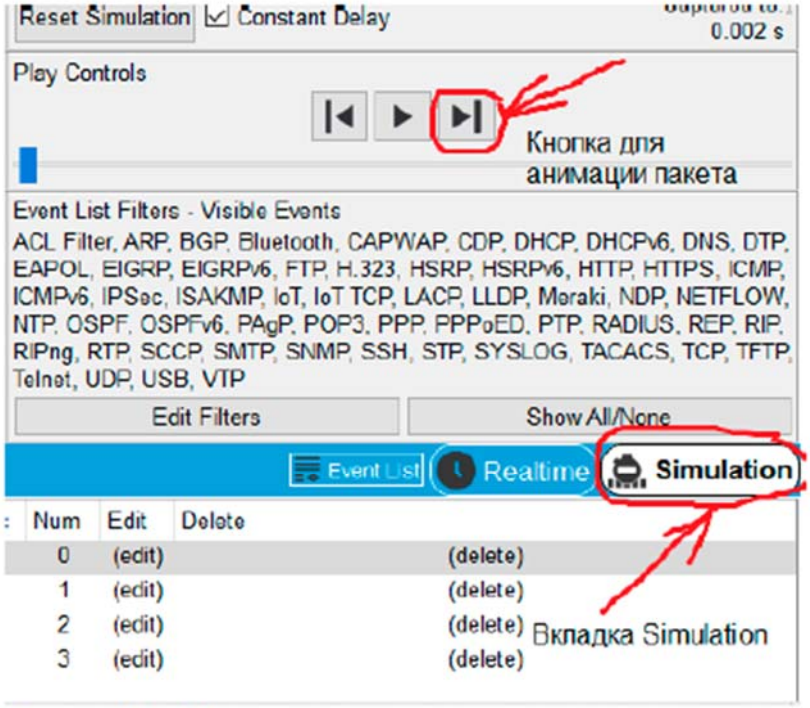


Рисунок 14 – Управление передвижением пакета

На рисунке 15 показано, что коммутатор отправляет пакет только в нужный порт, а концентратор (Hub) во все доступные порты, кроме порта источника. Вторая схема является небезопасной, так как если на компьютерах PC2 и PC3 будут находиться злоумышленники, то они могут получать информацию, которая им не предназначена.

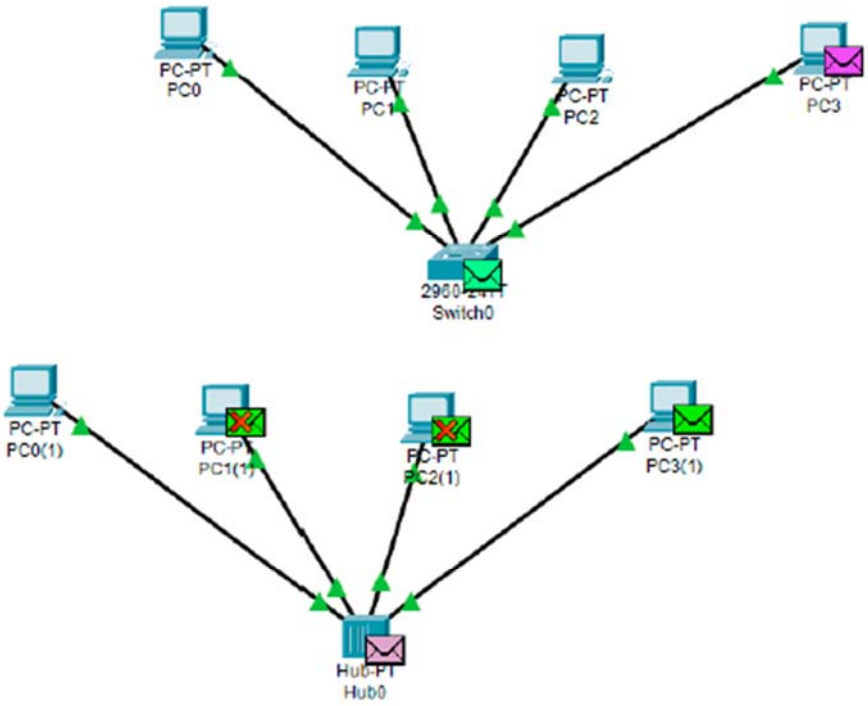


Рисунок 15 – Сравнение принципов работы первой и второй сетей

Мы можем заглянуть в пакет и посмотреть его содержимое (рис.16). Для этого надо на него нажать левой кнопкой мыши.

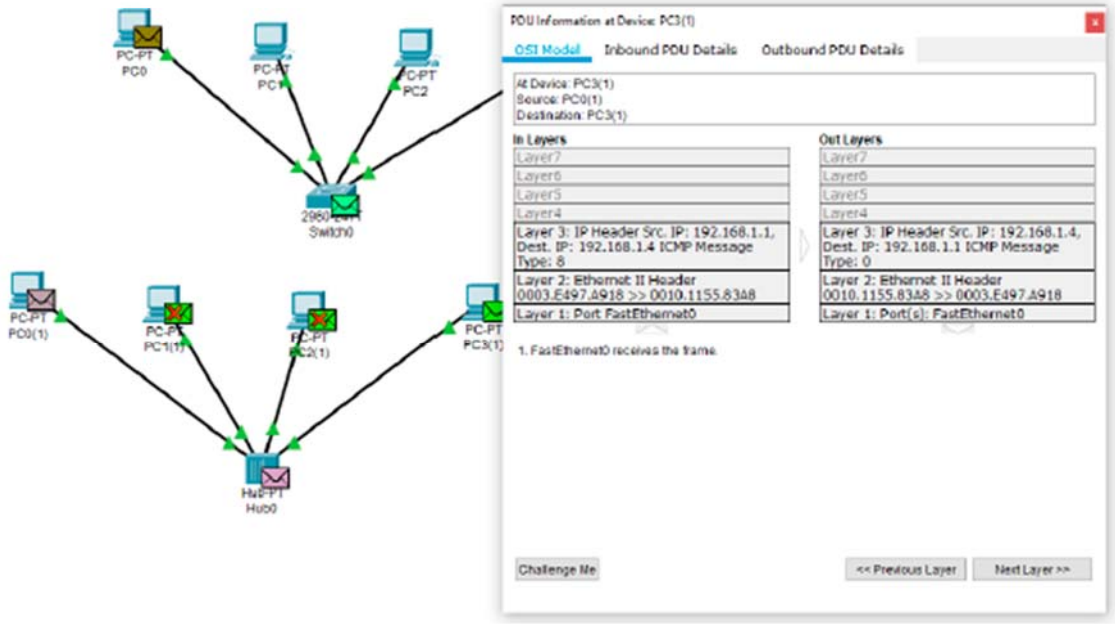


Рисунок 16 – Содержимое отправленного пакета

Теперь компьютер PC4 отправляет обратно пакет PC0. При отправке производим аналогичные действия с помощью кнопки Capture then forward для анимации пакета (рис. 14). Происходит точно такое же явление. Т.е. ком-мутатор отправляет пакет в

определенный порт, куда подключен PC0, а кон-центратор (hub) во все доступные порты. Убедитесь в этом самостоятельно.

Содержание отчета

В индивидуальном отчёте должны быть указаны цель, задание, представлены необходимые снимки экрана и пояснения к ним. Следует проанализировать полученные данные и дать ответы на контрольные вопросы.

Контрольные вопросы

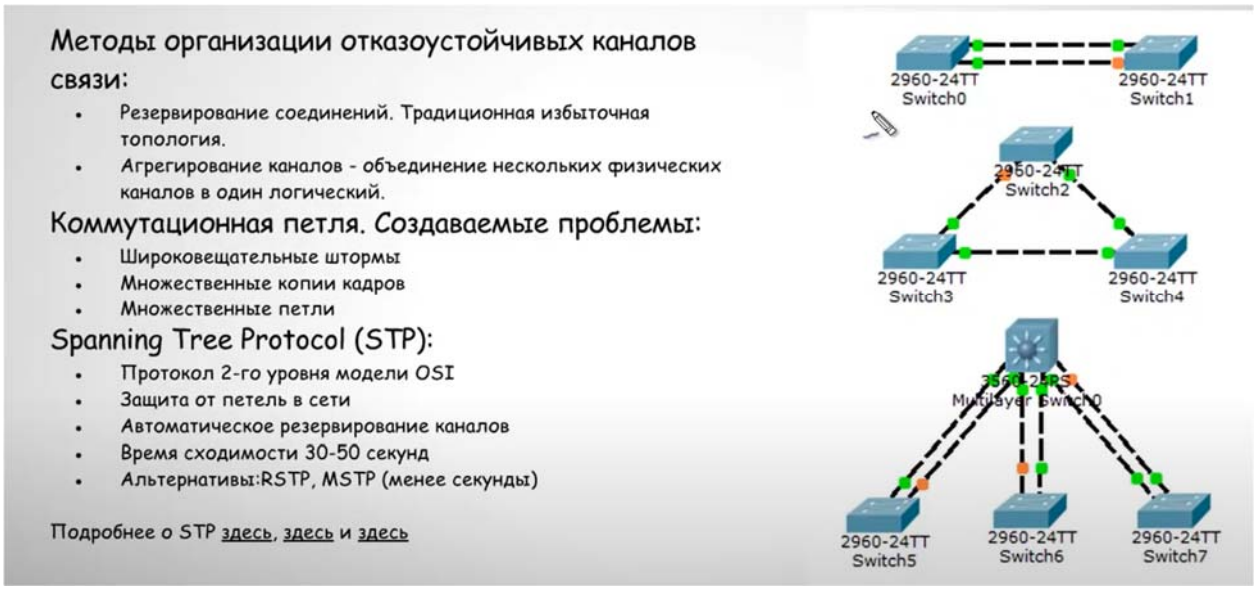
1. В чем отличие коммутатора от концентратора?
2. Для чего нужна таблица коммутации?
3. Как происходит заполнение таблицы коммутации?
4. Что представляет собой MAC- адрес?
5. Почему строить сеть на концентраторе небезопасно?
6. Как можно посмотреть содержимое пакета с помощью Cisco Packet Tracer?
7. Как проверить работоспособность спроектированной сети в Cisco Packet Tracer?
8. Как быстро построить вторую сеть в Cisco Packet Tracer?
9. Какие устройства относятся к физическим средствам физического уровня?
10. Какие устройства относятся к физическим средствам канального уровня?
11. Какие устройства относятся к физическим средствам сетевого уровня?
12. Сравните содержимое отправленных пакетов на концентраторе и коммутато-ре относительно модели OSI.

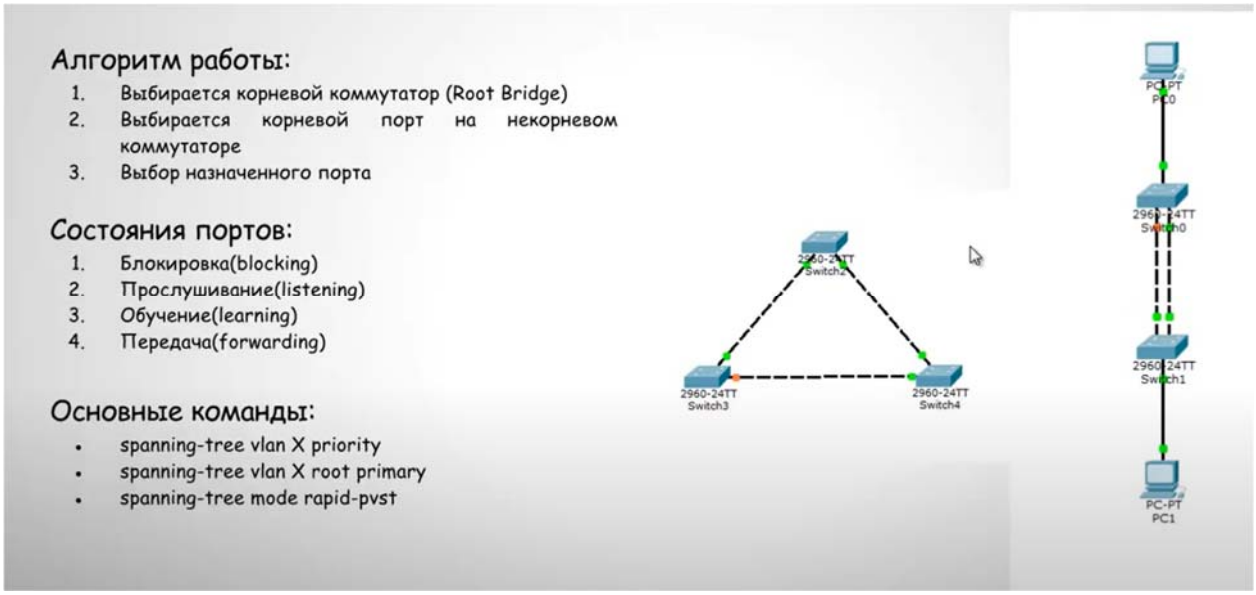
Практическое занятие № 3 - Протокол STP

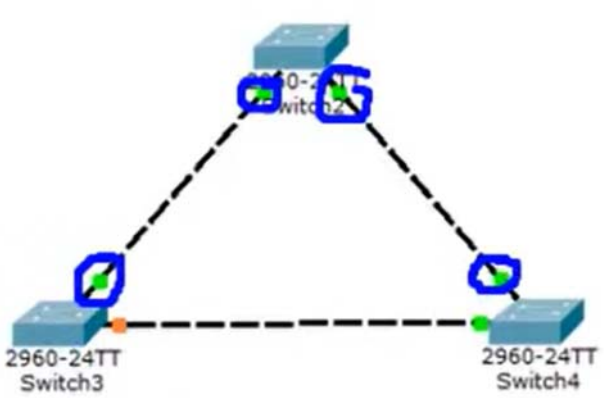
Протокол STP

Задание: Отчет по теме

№3 STP








```
Switch>en
Switch#sw
Switch#sh
Switch#show s
Switch#show sp
Switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0001.C992.4759
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0001.C992.4759
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/3            Desg FWD 19        128.3    P2p

Switch#
```

Проверяем следующий

```
Switch#show sp
Switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0001.C992.4759
             Cost        19
             Port        1(FastEthernet0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0030.A32C.28EE
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.1    P2p
Fa0/2            Altn BLK 19        128.2    P2p

Switch#
```

```
Switch>en
Switch#sh
Switch#show sp
Switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0001.C992.4759
              Cost        19
              Port        3(FastEthernet0/3)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     0006.2A90.4D82
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/3            Root FWD 19        128.3    P2p

Switch#
```

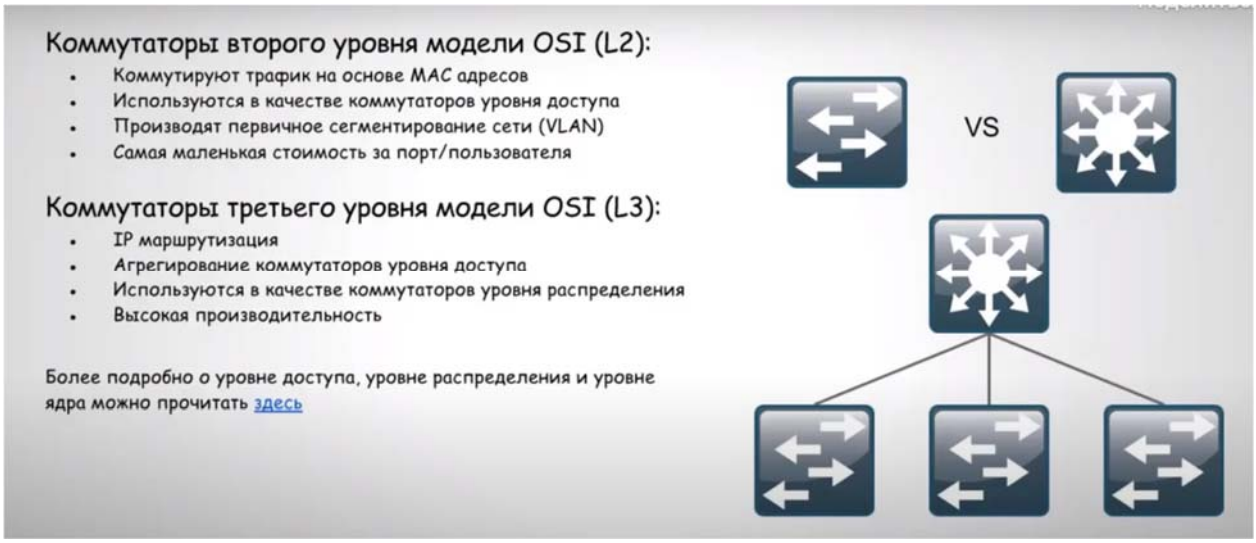
Отключаем порт Fa0/1 на Switch1

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int
Switch(config)#interface fa0/1
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#shut
Switch(config-if)#shutdown

Switch(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively do
wn

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state t
o down
```

```
Switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0001.6417.5771
              Cost        19
              Port        2(FastEthernet0/2)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     00D0.FF04.5D86
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg LSN 19        128.1    P2p
Fa0/2            Root FWD 19        128.2    P2p

Switch#
```

Практическое занятие № 4 - Коммутатор 3-го уровня

№4 Коммутатор 3-го уровня

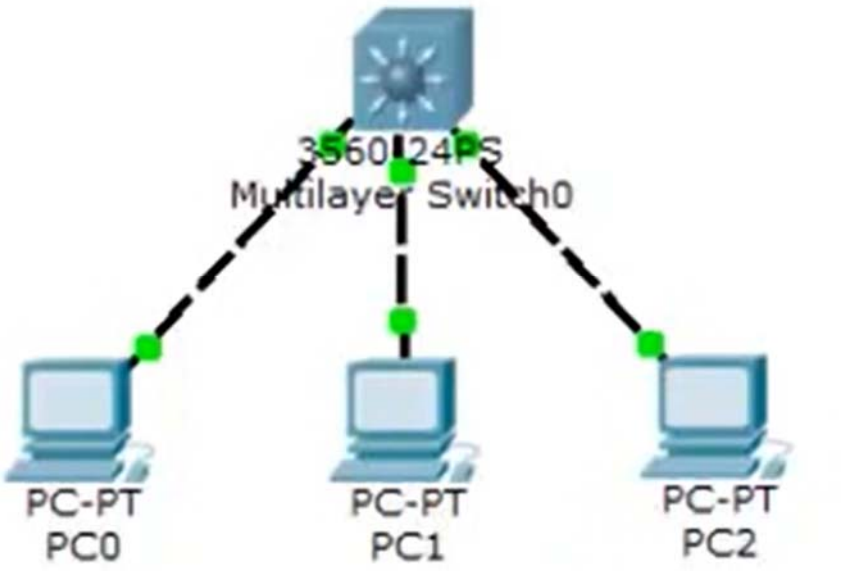


Рассмотрим 2 примера

Типовые настройки:

```
Switch(config)#vlan 2
Switch(config-vlan)#name VLAN2
Switch(config)#vlan 3
Switch(config-vlan)#name VLAN3
Switch(config)#vlan 4
Switch(config-vlan)#name VLAN4
Switch(config)#interface FastEthernet0/1
Switch(config-if)#switchport access vlan 2
Switch(config-if)#switchport mode access
Switch(config)#interface FastEthernet0/2
Switch(config-if)#switchport access vlan 3
Switch(config-if)#switchport mode access
Switch(config)#interface FastEthernet0/3
Switch(config-if)#switchport access vlan 4
Switch(config-if)#switchport mode access
Switch(config)#interface vlan 2
Switch(config-if)#ip address 2.2.2.1 255.255.255.0
Switch(config)#interface vlan 3
Switch(config-if)#ip address 3.3.3.1 255.255.255.0
Switch(config)#interface vlan 4
Switch(config-if)#ip address 4.4.4.1 255.255.255.0
Switch(config)#ip routing
```

Первый пример



Создадим 3 сегмента (Vlan 2,3,4)

```
Switch#conf t
Enter configuration commands, one per line.  End
Switch(config)#
Switch(config)#vlan 2
Switch(config-vlan)#name VLAN2
Switch(config-vlan)#exit
Switch(config)#vlan 3
Switch(config-vlan)#nam
Switch(config-vlan)#name VLAN3
Switch(config-vlan)#exit
Switch(config)#vla
Switch(config)#vlan 4
Switch(config-vlan)#na
Switch(config-vlan)#name VLAN4
Switch(config-vlan)#
Switch(config-vlan)#
Switch(config-vlan)#
```

Определяем порты куда подключаются пользователи

Vlan 2

```
Switch#
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
Switch(config)#
Switch(config)#int fa0/1
Switch(config-if)#sw
Switch(config-if)#switchport mod
Switch(config-if)#switchport mode acc
Switch(config-if)#switchport mode access
Switch(config-if)#sw
Switch(config-if)#switchport acc
Switch(config-if)#switchport access vl
Switch(config-if)#switchport access vlan 2
```

Vlan 3

```
Switch(config-if)#exit
Switch(config)#int fa0/2
Switch(config-if)#sw
Switch(config-if)#switchport mod
Switch(config-if)#switchport mode acc
Switch(config-if)#switchport mode access
Switch(config-if)#sw
Switch(config-if)#switchport acc
Switch(config-if)#switchport access vl
Switch(config-if)#switchport access vlan 3
Switch(config-if)#exit
Switch(config)#
```

Vlan 3

```
Switch(config)#int fa0/3
Switch(config-if)#sw
Switch(config-if)#switchport mod
Switch(config-if)#switchport mode acc
Switch(config-if)#switchport mode access
Switch(config-if)#sw
Switch(config-if)#switchport acc
Switch(config-if)#switchport access vl
Switch(config-if)#switchport access vlan 3
Switch(config-if)#switchport access vlan 4
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

SHOW RUN

```
!
interface FastEthernet0/1
 switchport access vlan 2
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 3
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 4
 switchport mode access
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
```

НАЗНАЧАЕМ IP адреса

Настраиваем VLAN2

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int vla
Switch(config)#int vlan 2
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, changed state to up

Switch(config-if)#
```

```
Switch(config-if)#ip add
Switch(config-if)#ip address 2.2.2.1 255.255.255.0
Switch(config-if)#exit
Switch(config)#
```

Vlan 3

```
Switch(config-if)#ip add
Switch(config-if)#ip address 2.2.2.1 255.255.255.0
Switch(config-if)#exit
Switch(config)#int vla
Switch(config)#int vlan 3
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan3, changed state to up

Switch(config-if)#ip add
Switch(config-if)#ip address 3.3.3.1 255.255.255.0
Switch(config-if)#exit
```

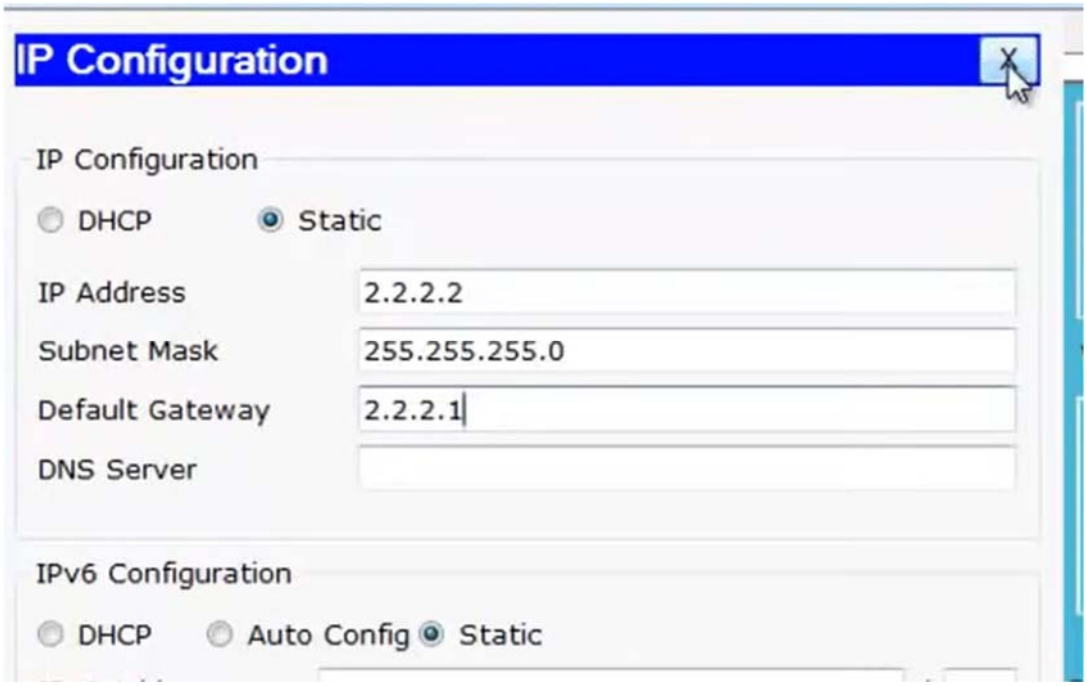
```
Switch(config)#int vla
Switch(config)#int vlan 4
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan4, changed state to up

Switch(config-if)#
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#ip add
Switch(config-if)#ip address vl
Switch(config-if)#ip address 4.4.4.1 255.255.255.0
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#end
Switch#
```

\

Show run

```
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan2
 ip address 2.2.2.1 255.255.255.0
!
interface Vlan3
 ip address 3.3.3.1 255.255.255.0
!
interface Vlan4
 ip address 4.4.4.1 255.255.255.0
!
```

Настраиваем ПК1



Пинг на коммутатор

```
Pinging 2.2.2.1 with 32 bytes of data:

Reply from 2.2.2.1: bytes=32 time=33ms TTL=255
Reply from 2.2.2.1: bytes=32 time=0ms TTL=255
Reply from 2.2.2.1: bytes=32 time=0ms TTL=255

Ping statistics for 2.2.2.1:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 33ms, Average = 11ms

Control-C
^C
PC>
```

Аналогично ПК 1 ПК2

Заходим в коммутатор

```
Switch#
Switch#
Switch#
Switch#
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
Switch(config)#ip rou
Switch(config)#ip rout
Switch(config)#ip routi
Switch(config)#ip routing
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

Сохр. Конфигурацию

```
Switch#
Switch#wr mem
Building configuration...
[OK]
Switch#
```

Пинг с ПК 2 На ПК1

```
Control-C
^C
PC>ping 2.2.2.2

Pinging 2.2.2.2 with 32 bytes of data:

Reply from 2.2.2.2: bytes=32 time=0ms TTL=127
Reply from 2.2.2.2: bytes=32 time=0ms TTL=127
Reply from 2.2.2.2: bytes=32 time=0ms TTL=127
Reply from 2.2.2.2: bytes=32 time=0ms TTL=127

Ping statistics for 2.2.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>
```

Практическое занятие № 5 - Построение схемы компьютерной сети с

использованием прикладных программных средств

Тема: Построение схемы компьютерной сети с использованием прикладных программных средств.

Задачи

Понять основные принципы работы с Packet Tracer.

Создание/имитация простой сети Ethernet с помощью двух узлов и концентратора.

Наблюдение поведения трафика в сети.

Наблюдение за потоком данных широковещательных рассылок по протоколу ARP и обменов пакетами данных (ping).

Подсказка. Чтобы инструкции во время выполнении упражнения отображались, поставьте флажок «Top» (вверх) в нижнем левом углу окна с инструкциями.

Шаг 1. Создание логической схемы сети с двумя ПК и концентратором.

В нижнем левом углу окна Packet Tracer отображены восемь значков, представляющих категории или группы устройств, например, Routers (маршрутизаторы), Switches (коммутаторы) или End Devices (конечные устройства).

При перемещении курсора над категориями устройств отображается имя категории в окне. Для выбора определенного устройства выберите сначала категорию. После выбора категории устройств рядом со значками категорий появится список устройств. Выберите нужное устройство.

а. Выберите пункт **End Devices** (конечные устройства) из списка вариантов в левом нижнем углу. Перетащите два однотипных ПК на область проектирования сети.

б. Выберите **Hubs** (концентраторы) из списка вариантов в левом нижнем углу. Добавьте концентратор к прототипу сети, перетащив типовой концентратор на область проектирования сети.

в. Выберите значок **Connections** (соединения) из списка вариантов в левом нижнем углу. Выберите тип кабеля **Copper Straight-through**(медный прямой). Щелкните первый узел **PC0** и назначьте выбранный кабель разъему интерфейса **FastEthernet**. Щелкните концентратор **Hub0** и выберите порт соединения **Port0** для соединения с **PC0**.

г. Повторите этот шаг для второго ПК **PC1** для его подключения к **Port1**на концентраторе.

*На концах кабельного соединения должны появиться зеленые точки. Если этого не произошло, проверьте выбранный тип кабеля.

Шаг 2. Настройка имен узлов и IP-адресов на компьютерах

а. Щелкните значок PC0. Появится окно PC0.

б. В окне PC0 выберите вкладку **Config** (конфигурация). Измените**Display Name** (отображаемое имя) ПК на **PC-A**. (Откроется окно с сообщением о том, что изменение имени устройства может оказать влияние на оценку упражнения. Не обращайте внимания на это окно с сообщением об ошибке.) Выберите вкладку **FastEthernet** слева и добавьте IP-адрес **192.168.1.1** и маску подсети **255.255.255.0**. Закройте окно конфигурации PC-A, нажав на кнопку **x** в правом верхнем углу окна.

в. Щелкните значок PC1.

г. Выберите вкладку **Config** (конфигурация). Измените **Display Name**(отображаемое имя) ПК на **PC-B**. Выберите вкладку**FastEthernet** слева и добавьте IP-адрес **192.168.1.2** и маску подсети**255.255.255.0**. Закройте окно конфигурации PC-B.

Шаг 3. Наблюдение за потоком данных от PC-A к PC-B при создании сетевого трафика

а. Включите режим **Simulation** (моделирование), выбрав вкладку, частично скрытую за вкладкой **Realtime** (в реальном времени) в нижнем правом углу. На вкладке изображен секундомер.

б. Нажмите кнопку **Edit Filters** (редактировать фильтры) в области**Event List Filters** (фильтры списка событий). После нажатия кнопки**Edit Filters** (редактировать фильтры) откроется всплывающее окно. Во всплывающем окне щелкните пункт **Show All/None** (показать все/ничего) для отмены выделения всех фильтров. Выберите только фильтры **ARP** и **ICMP**.

Выберите **Simple PDU** (простой PDU), щелкнув значок с изображением закрытого конверта на вертикальной панели инструментов. Переместите курсор в область отображения на экране. Щелкните **PC-A** для определения источника. Переместите курсор на **PC-B** и щелкните для определения адресата.

в. **Обратите внимание, что два конверта теперь находятся рядом с PC-A. Один конверт - это сообщение, передаваемое по протоколу ICMP, другой - сообщение, передаваемое по протоколу ARP. Event List (список событий) на панели «Simulation» (панель моделирования) точно отобразит, какой из конвертов представляет сообщение, передаваемое по протоколу ICMP, а какой - сообщение, передаваемое по протоколу ARP.

г. Нажмите кнопку **Auto Capture / Play** (автозахват / воспроизведение) в области **Play Controls** (регуляторы воспроизведения) на панели «Simulation» (панель моделирования). Под кнопкой **Auto Capture / Play** (автозахват / воспроизведение) имеется горизонтальная полоса с вертикальной кнопкой (ползунком), регулирующей скорость моделирования. При перетаскивании ползунка вправо/влево увеличивается/снижается скорость моделирования.

д. Воспроизведение анимации закончится при появлении окна с сообщением *No More Events* (больше событий нет). Это означает, что все запросы событий выполнены. Нажмите кнопку **OK** для закрытия окна с сообщением.

е. Нажмите кнопку **Reset Simulation** (восстановить моделирование) на панели «Simulation» (панель моделирования). Обратите внимание, что конверт типа ARP отсутствует. Процесс моделирования вернулся в исходное состояние, но при этом изменения конфигурации или записи в динамической таблице, например, записи в ARP-таблице, отменены не были. ARP-запрос не обязателен для выполнения команды **ping**, поскольку PC-A уже имеет MAC-адрес в ARP-таблице.

ж. Нажмите кнопку **Capture / Forward** (захват / вперед). ICMP-конверт переместится от отправителя к концентратору и остановится. Кнопка **Capture / Forward** (захват / вперед) позволяет запустить моделирование на один шаг вперед. Нажимайте кнопку **Capture / Forward** (захват / вперед) до тех пор, пока не выполните событие.

з. Нажмите кнопку **Power Cycle Devices** (силовые устройства) снизу слева, над значками устройств.

и. Откроется окно с запросом подтвердить сброс. Нажмите кнопку **Yes**(да). ICMP- и ARP-конверты появятся снова. Кнопка **Reset Network**(сброс сети) отменит все несохраненные изменения конфигурации и сотрет все записи в динамической таблице, например, записи ARP- и MAC-таблицы.

Шаг 4. Отображение ARP-таблицы на каждом ПК

а. Нажмите кнопку **Auto Capture / Play** (автозахват / воспроизведение) для заполнения ARP-таблицы на ПК. Нажмите кнопку **OK** при появлении окна *No More Events* (событий больше нет).

б. Выберите инструмент масштабирования с изображением увеличительного стекла на вертикальной панели инструментов.

в. Щелкните значок **PC-A**. Появится ARP-таблица для PC-A. Обратите внимание, что PC-A не имеет записи в ARP-таблице для PC-B. Отобразите ARP-таблицу для PC-B. Закройте все окна с ARP-таблицами.

г. Щелкните **инструмент Select** (выбор) на вертикальной панели инструментов справа. (Это первый по счету значок на панели инструментов.)

д. Щелкните **PC-A** и выберите вкладку **Desktop** (рабочий стол).

е. Выберите **Command Prompt** (командная строка), введите команду **arp -a** и нажмите клавишу *ВВОД*, чтобы отобразить ARP-таблицу на рабочем столе. Закройте окно конфигурации PC-A.

ж. Изучите ARP-таблицу для **PC-B**.

з. Закройте окно конфигурации PC-B.

и. Нажмите кнопку **Check Results** (проверить результаты) внизу данного окна с инструкциями для проверки правильности топологии.

Контрольные вопросы:

1. Что называется компьютерной сетью?
2. Какие устройства необходимы для создания простейшей компьютерной сети?
3. Как происходит конфигурирование устройств сети в среде Cisco PT?

Практическое занятие № 6 - Изучение технологии виртуальных локальных сетей VLAN (Virtual Local Area Network). Часть 1

24.11.2023 -1 час

Цель работы

Изучить технологию VLAN.

Задание

1. Ознакомиться с преимуществами технологии VLAN;
2. Изучить, как могут быть построены сети VLAN ;
3. Ответить на вопросы.

Виртуальными локальными сетями VLAN (Virtual Local Area Network) называются локальные сети, созданные на единой аппаратной базе (т. е. на коммутаторах, соединенных между собой физическими каналами), но логи-чески изолированные друг от друга.

VLAN имеет те же свойства, что и физическая локальная сеть, но поз-воляет конечным членам группироваться вместе, даже если они не находятся в одной физической сети. Такая организация может быть сделана на основе программного обеспечения вместо физического перемещения устройств.

VLAN дает возможность значительно оптимизировать работу локаль-ной сети за счет разгрузки отдельных ее сегментов от "лишнего" трафика и решить некоторые вопросы безопасности в сети, разграничив доступ пользо-вателей. Сети VLAN имеют следующие преимущества:

- помогает структурировать сеть;
- используется для обеспечения безопасности;
- используют для объединения;
- уменьшает количество широковещательного трафика.

Широковещательный трафик используется для ряда протоколов (ARP, DHCP и т.д.). В случае большой сети широковещательный трафик может привести к нерациональному использованию канала. При организации VLAN, пользователи, находящиеся в разных сегментах, не будут получать широковещательные кадры, которые предназначены пользователям других VLAN.

С помощью технологии VLAN можно создавать рабочие группы, основываясь на функциональности, а не на физическом расположении сегментов. Она позволяет администратору логически создавать, группировать и перегруппировывать сетевые сегменты без изменения физической инфраструктуры и отсоединения пользователей и серверов. VLAN обеспечивает дополнительные преимущества для безопасности. Пользователи одной рабочей группы не могут получить доступ к данным другой группы, потому что каждая VLAN – это закрытая и логически определенная группа.

Представьте компанию, в которой отдел кадров, работающий с конфиденциальной информацией, расположен на трех этажах здания. Инженерный департамент и отдел Маркетинга также размещаются на трех этажах (рис. 1). Каждый этаж в здании обеспечен сетью Ethernet средствами этажных коммутаторов: по одному коммутатору на этаж.

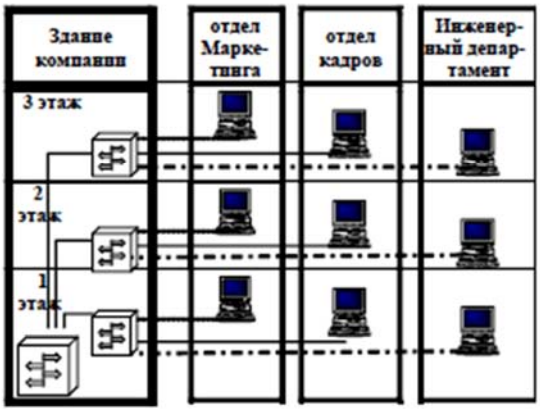


Рисунок -1 Пример построения VLAN для компании

Используя технологию VLAN, работники Инженерного отдела и отдела Маркетинга могут быть расположены на всех трех этажах здания, а их ПК будут входить в состав двух VLAN (VLAN1, VLAN2). Сотрудники отдела кадров, которые также размещаются на всех трех этажах, будут использовать ПК, входящие в состав VLAN3. Сетевой трафик, создаваемый отделом кадров, будет доступен только сотрудникам этого департамента, а группы инженерного отдела и маркетинга не смогут получить доступ к конфиденциаль-

ным данным отдела кадров. Очевидно, есть другие требования для обеспечения полной безопасности, и VLAN может быть частью общей стратегии сетевой безопасности.

Таким образом, в VLAN группа устройств, имеют возможность взаимодействовать между собой напрямую на канальном уровне, хотя физически при этом они могут быть подключены к разным сетевым коммутаторам. И наоборот, устройства, находящиеся в разных VLAN, невидимы друг для друга на канальном уровне, даже если они подключены к одному коммутатору, и связь между этими устройствами возможна только на сетевом и более высоких уровнях.

По умолчанию на каждом порту коммутатора имеется сеть VLAN1 или VLAN управления. Сеть управления не может быть удалена, однако могут быть созданы дополнительные сети VLAN и этим альтернативным VLAN могут быть дополнительно назначены порты.

У коммутатора может быть два типа портов:

access port используется для подключения оконечных устройств (компьютеры, ноутбуки, IP-телефоны, видеокамеры, сервера и т.д.). Любой кадр, который проходит через access-порт, помечается номером, принадлежащим этому VLAN.

Второй тип портов это **trunk port.** Он необходим для соединения между собой коммутаторов.

Trunk port — порт, передающий трафик одного или нескольких VLAN. По умолчанию в транке разрешены все VLAN. Для того чтобы через соответствующий VLAN в транке передавались данные, как минимум, необходимо чтобы VLAN был активным. Активным VLAN становится тогда, когда он создан на коммутаторе и в нём есть хотя бы один порт в состоянии up/up.

Сети VLAN могут быть определены по:

- номеру порта (наиболее частое использование);
- MAC адресу (редко применяется);
- идентификатору пользователя User ID (очень редко применяется);
- сетевому IP-адресу (редко в связи с ростом использования DHCP).

VLAN, базирующаяся на номере порта, позволяет определить конкретный порт в VLAN. Это наиболее простой и часто используемый метод определения VLAN. VLAN, построенная на портах, применяется в тех случаях, когда рабочие станции используют протокол динамической настройки TCP/IP (DHCP).

Технология VLAN, базирующаяся на MAC адресах, позволяет пользователям находиться в той же VLAN, даже если они перемещаются с одного места на другое. Этот метод требует, чтобы администратор определил MAC-адрес каждой рабочей станции и затем внес эту информацию в коммутатор. Данный метод может вызвать большие трудности при поиске неисправностей, если пользователь изменил MAC-адрес.

Виртуальные сети, базирующиеся на сетевых IP-адресах, позволяют пользователям находиться в той же VLAN, при перемещении их с одного места на другое. Этот метод перемещает VLAN, связывая ее с сетевым IP-адресом рабочей станции для каждого коммутатора, к которому пользователь подключен.

Контрольные вопросы

1. Что такое технология VLAN? Какие ее основные преимущества?
2. Какие типы портов используются при настройке VLAN?
3. Как необходимо настроить коммутаторы для соединения с ПК и с другим коммутатором?
4. Почему компьютеры, подключенные в разные коммутаторы, но находящиеся в одном VLAN, перестают взаимодействовать между собой при исключении этого VLAN из trunk-порта?
5. Какая команда позволяет определить, в каком режиме работает порт коммутатора?
6. Перечислите основные способы назначения VLAN.
7. Что выполняет команда **switchport mode access**?
8. Какую команду необходимо ввести, чтобы назначить trunk-порт?
9. Какая команда позволяет вывести информацию по всем интерфейсам коммутатора?
10. Что позволяет сделать trunk-режим портов?

Практическое занятие № 6 - Изучение технологии виртуальных локальных сетей VLAN. Часть 2

24.11.2023 -2 часа

Цель работы

Изучить и практически освоить процесс настройки технологии вирту-альных локальных сетей VLAN (Virtual Local Area Network) с использовани-ем сетевого симулятора Cisco Packet Tracer. Научиться настраивать порты коммутатора в режимы access.

Задание

1. Ознакомиться с основными понятиями технологии виртуальных локаль-ных сетей VLAN (Virtual Local Area Network);

2. Запустить Cisco Packet Tracer;

3. Собрать необходимую топологию сети, запустить и настроить виртуаль-ное оборудование;

4. Согласно пунктам выполнения практической работы, сделать необходи-мые снимки экрана. Изучить полученную информацию и оформить ее в соответствии с требованиями раздела «Содержание отчета».

Порядок выполнения работы

Открываем Cisco Packet Tracer. Находим коммутатор 2960. Добавляем его в рабочую область. Затем добавляем четыре персональных компьютера PC0-PC1. Для того чтобы ускорить процесс, можно нажать на клавишу Ctrl, на экране появится крестик. И затем нажимаем этим крестиком в те места, где мы хотим расположить наши компьютеры. В результате получаем сле-дующую топологию сети (рис. 1).

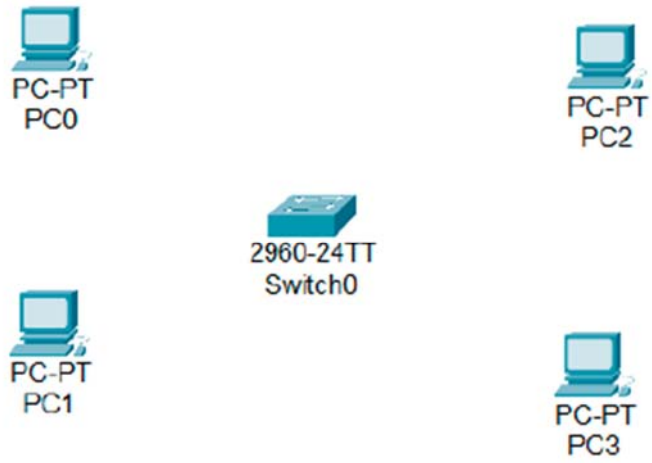


Рисунок 1 - Топология сети

Далее приступаем к соединению между устройствами. Так как здесь соединяются устройства разных уровней модели OSI, то используем прямой кабель. Также зажимаем клавишу Ctrl, нажимаем на значок компьютера и подключаем каждый компьютер. При этом выбираем на коммутаторе необходимые порты FastEthernet. На рисунке 2 показано подключение PC0 к порту FastEthernet 0/1 коммутатора 2960. Аналогично подключаем остальные PC. Коммутатор PC3 подключается к порту FastEthernet 0/4.

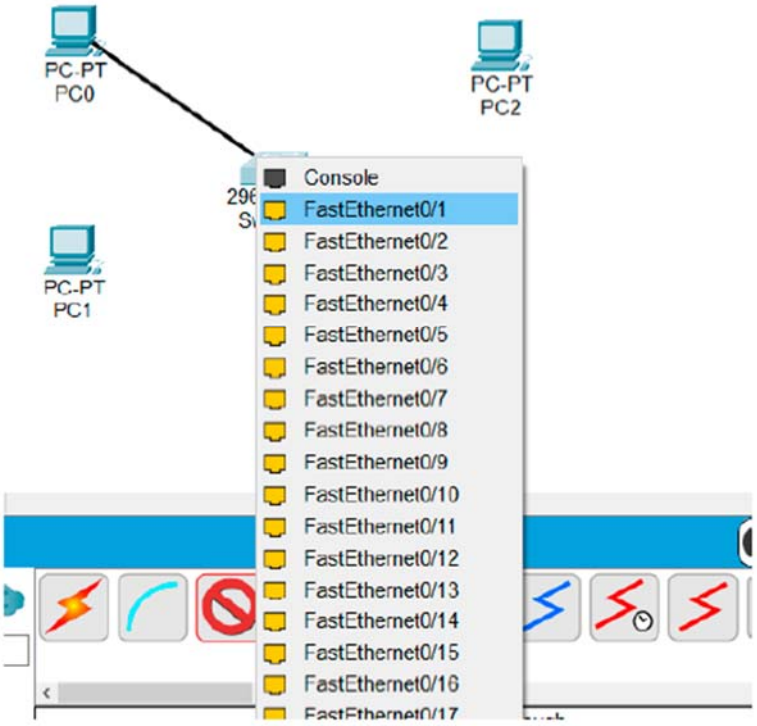


Рисунок 2 – Подключение компьютера PC1 к коммутатору 2960

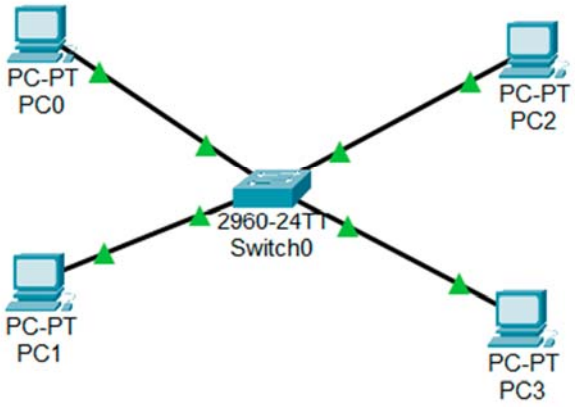


Рисунок 3 - Соединение между элементами сети

Далее разобьем нашу сеть на 2 сегмента. Пусть компьютеры PC0 и PC2 принадлежат к одному сегменту, а PC1 и PC3 к другому. Выбираем сверху фигуру Прямоугольник (Draw rectangle) и нужный цвет фигуры (рис.4), далее делим сеть нам 2 сегмента разного цвета (рис. 5).

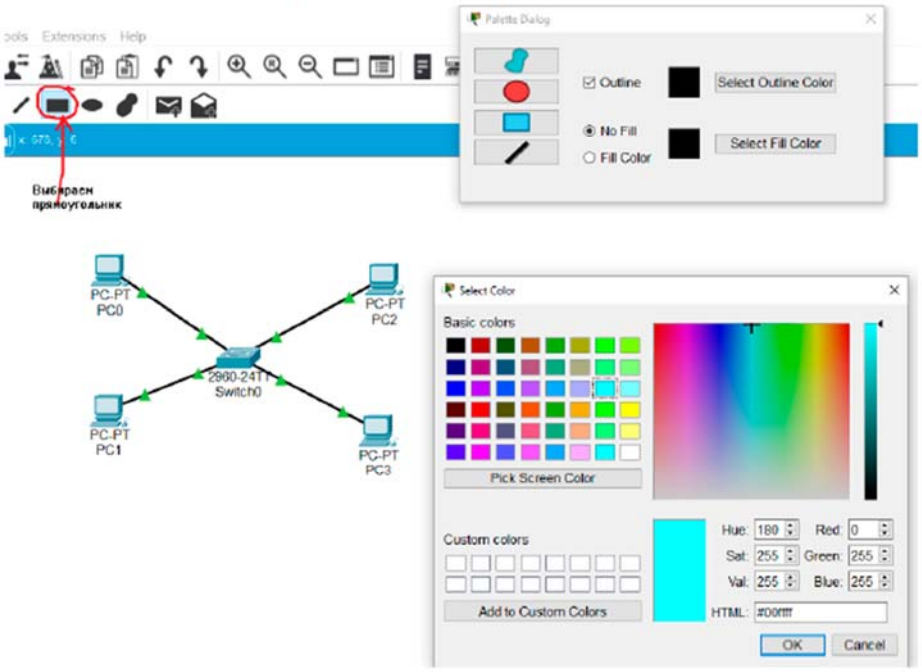


Рисунок 4 - Деление сети на сегменты с помощью значка Draw rectangle

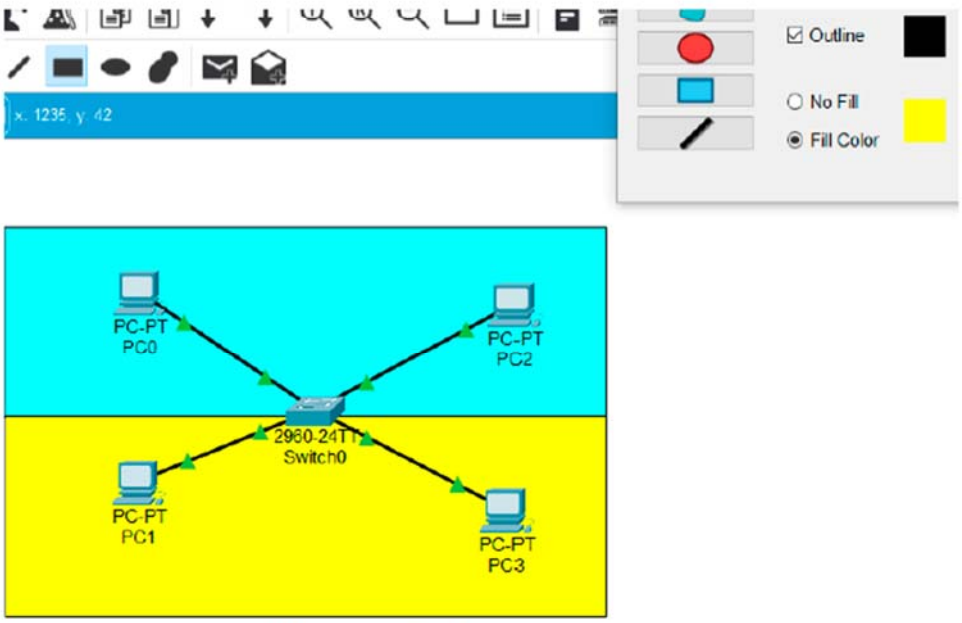


Рисунок 5 - Сеть с двумя сегментами

Для того, чтобы проверить номера интерфейсов FastEthernet для коммутатора, необходимо до создания VLAN проверить номера всех интерфейсов коммутатора, которые подключены к компьютерам. Для этого, необходимо подвести курсор к зеленым треугольникам на линиях, соединяющих компьютеры с коммутаторами. Номера интерфейсов высветятся рядом с зелеными треугольниками (рис. 6).

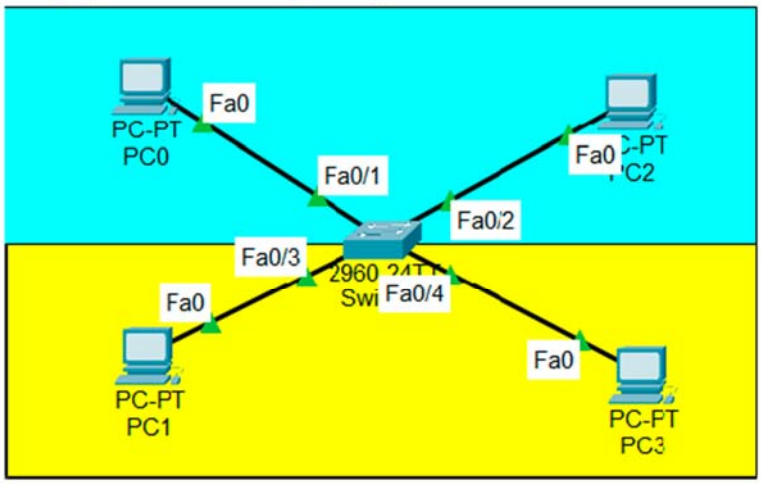


Рисунок 6 - Проверка номеров интерфейсов FastEthernet

Теперь нам нужно отделить данные одного сегмента от другого. Выходим в настройки коммутатора и входим в консоль (CLI) (рис. 7).

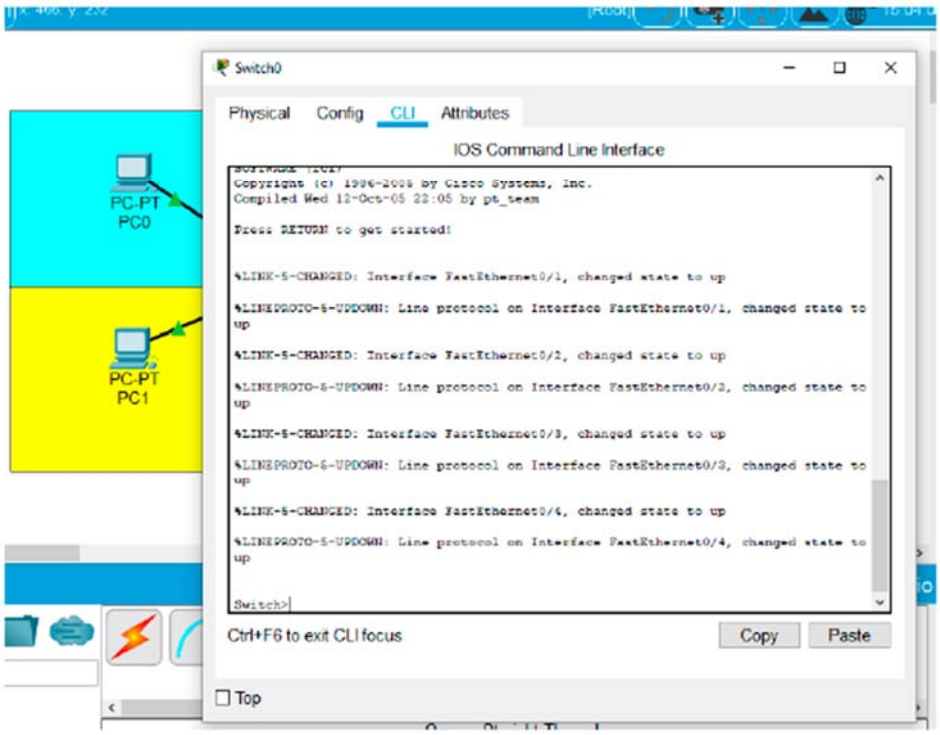


Рисунок 7- Консоль коммутатора

Набираем команду **Switch>enable**

И входим в привилегированный режим. Далее вводим команду

Switch#configure terminal

Создайте новый VLAN, назовем его VLAN 2, дайте ему название **professors** и назначьте портам коммутатора, к которым подключены компьютеры, режим передачи трафика и VLAN 2:

Switch(config)#vlan 2
Switch(config-vlan)#name professors
Switch(config-vlan)#exit

Настройка портов коммутатора :

Switch(config)#interface FastEthernet 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config-if)# exit
Switch(config)#interface FastEthernet 0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config-if)# end

На этом настройка портов закончена.

Проверьте правильность настроек с помощью команды :

Switch#show vlan

Она выводит основную информацию о VLAN, (рисунок 8).

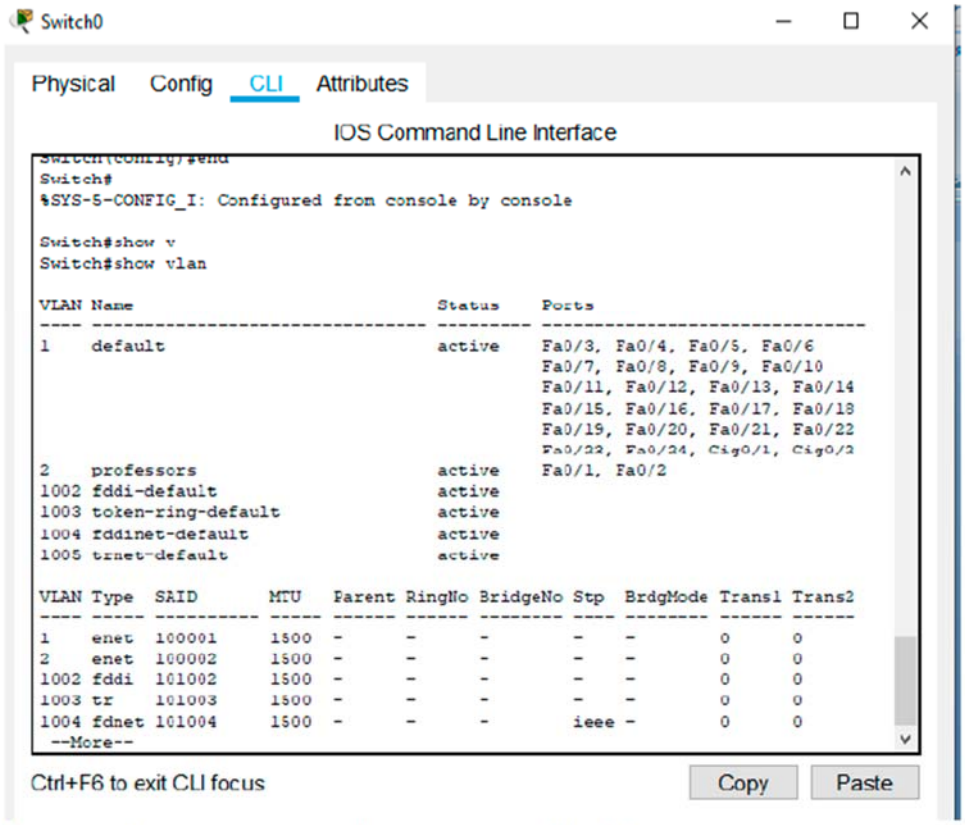


Рисунок 8 - Основная информация по VLAN

Здесь показана вся информация по VLAN. Видно, что первый VLAN, который существует на всех коммутаторах CISCO по умолчанию (default) выставлен на всех портах кроме портов FastEthernet 0/1 и FastEthernet 0/2, которые мы определили в VLAN 2.

Для вывода краткой информации по созданным VLAN введите команду (рисунок 9):

Switch# show vlan brief

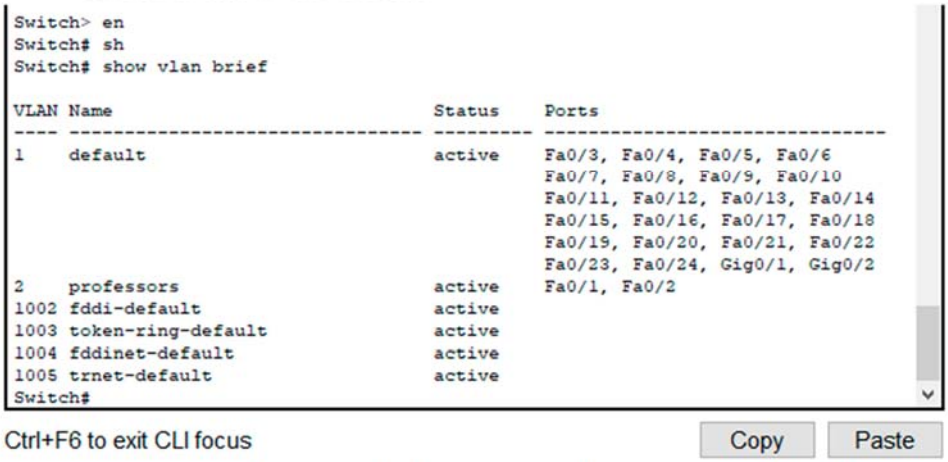


Рисунок 9 - Краткая информация по VLAN

Проделаем аналогичные действия для второго сегмента. Назовем его **students**. Пусть это будет VLAN 3.

Далее набираем команды:

Switch#configure terminal

Switch(config)#vlan 3
Switch(config-vlan)#name students
Switch(config-vlan)#exit
Настройка интерфейсов:
Switch(config)#interface FastEthernet 0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 3
Switch(config-if)#exit
Switch(config)#interface FastEthernet 0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 3
Switch(config-if)#end

Для вывода краткой информации по созданным VLAN введите команду (рисунок 10):

Switch# show vlan brief

```
Switch>en
Switch#sh
Switch#show v
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
2    professors                       active    Fa0/1, Fa0/2
3    students                         active    Fa0/3, Fa0/4
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Switch#
```

Рисунок 10 - Краткая информация по VLAN 3

Перейдем к настройке компьютеров и зададим им IP-адреса (Табл. 1). В IP- адресах компьютеров третья цифра IP-адреса соответствует номеру VLAN. Для этого выйдем в настройки PC0 и во вкладке Desktop выбираем IP-Configuration (рис. 11).

Таблица №1 Сетевые адреса компьютеров

Сетевой элемент	Интерфейс	IP-адрес	VLAN
PC0	FastEthernet0	192.168.2.1	2
PC1	FastEthernet0	192.168.3.1	3
PC2	FastEthernet0	192.168.2.2	2
PC3	FastEthernet0	192.168.3.2	3

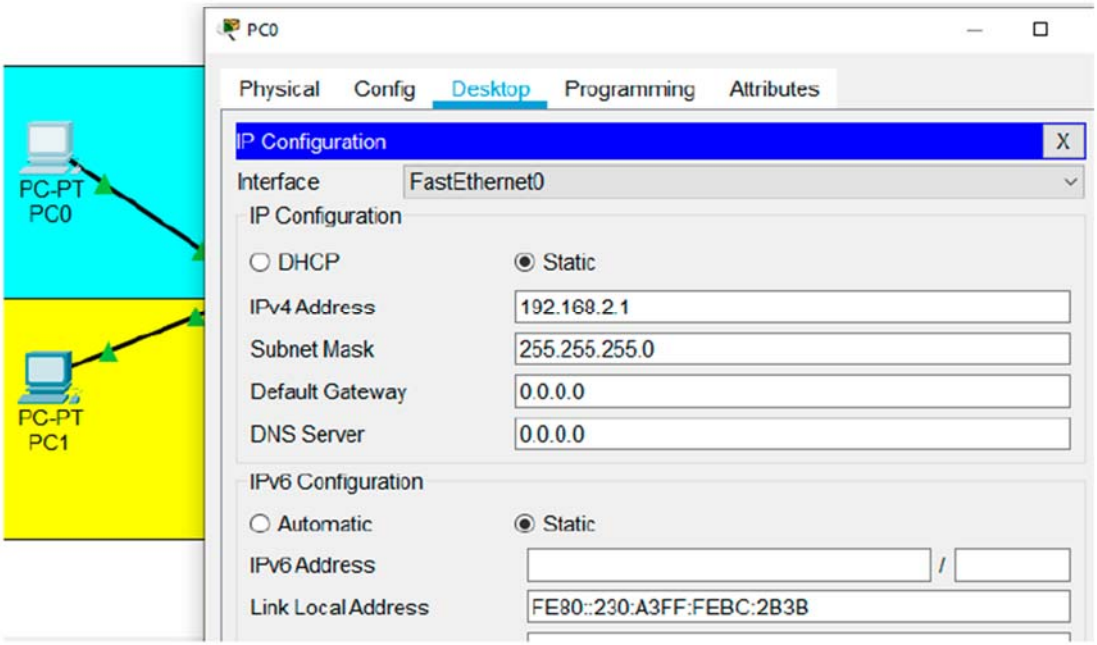


Рисунок 11- Настройка компьютера PC0

В соответствии с таблицей 1 настраиваем и остальные компьютеры сети.

Проверим связность компьютеров в первом сегменте (рис. 12).

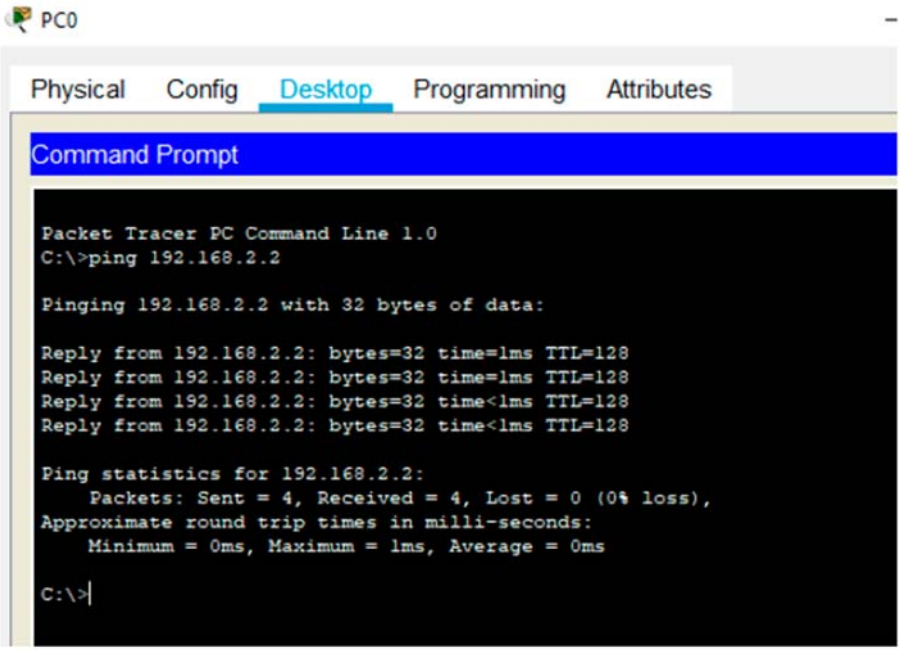


Рисунок 12 - Проверка связности компьютеров в одном сегменте

Попробуем проверить связь компьютеров в разных сегментах. Пакеты между ними не пересылаются (рис. 13). Т.е. связность между компьютерами разных сегментов отсутствует.

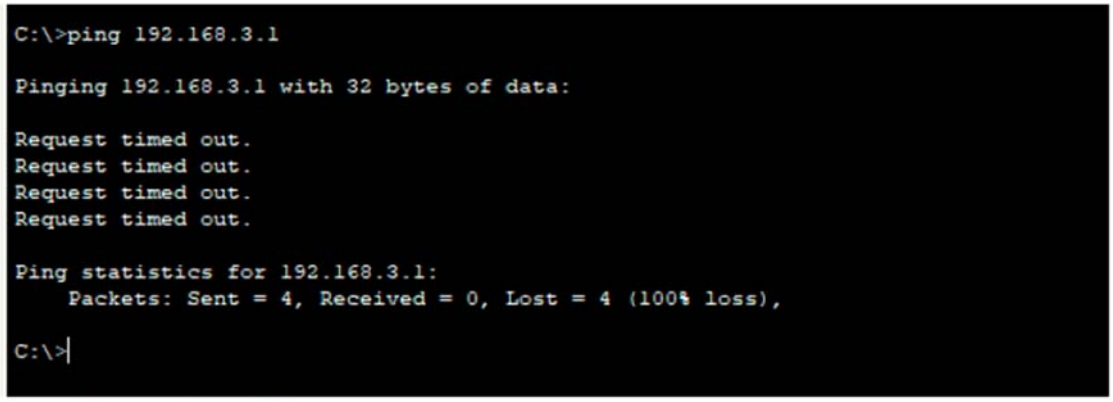


Рисунок 13 - Проверка связности компьютеров в разных сегментах

Произведем аналогичную проверку у компьютеров из второго сегмента. Таким образом, мы убедились, что между сегментами professors и students связность отсутствует. Т.е. мы сделали 2 независимые VLAN. Рекомендуется сохранить данную конфигурацию для выполнения лабораторной работы «Изучение технологии виртуальных локальных сетей VLAN». Часть 2.

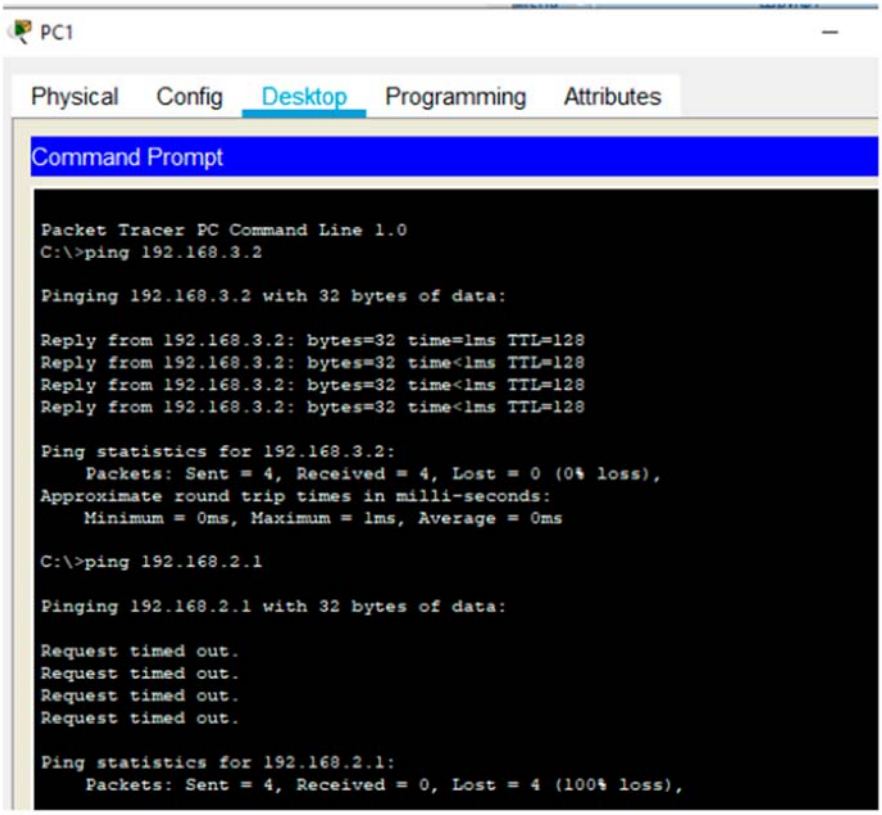


Рисунок 14 - Проверка связности компьютеров во втором сегменте

Содержание отчета

В индивидуальном отчёте должны быть указаны цель, задание, представлены необходимые снимки экрана и пояснения к ним. Следует проанализировать полученные данные и дать ответы на контрольные вопросы.

Контрольные вопросы

1. Опишите последовательность создания VLAN?
2. Как проверить связность компьютеров в разных VLAN?
3. Для чего используется команда **Switch# show vlan brief?**
4. Как проверить правильность настройки компьютеров?
5. Для чего применяется команда **Switch(config-if)#switchport mode access?**
6. Что обозначает аббревиатура TTL на рисунке 12?
7. Почему для соединения ПК и коммутатора используется прямой кабель?
8. Какого класса IP- адреса используются в данной работе?
9. Продемонстрируйте продвижение пакета внутри одного VLAN в данной работе.
10. Что выполняет команда switchport access vlan 3?

Практическое занятие № 6 - Изучение технологии виртуальных локальных сетей VLAN. Часть 3

24.11.2023 -2 часа

Цель работы

Изучить и практически освоить процесс настройки технологии виртуальных локальных сетей VLAN (Virtual Local Area Network) с использованием сетевого симулятора Cisco Packet Tracer. Научиться настраивать порты коммутатора в режимы trunk.

Задание

1. Ознакомиться с основными понятиями технологии виртуальных локальных сетей VLAN (Virtual Local Area Network).

2. Запустить сеть, которая использовалась в предыдущей работе

3. Собрать новую топологию сети, запустить и настроить виртуальное оборудование.

4. Согласно пунктам выполнения практической работы, сделать необходимые снимки экрана. Изучить полученную информацию и оформить ее в соответствии с требованиями раздела «Содержание отчета».

Порядок выполнения работы

В данной работе мы будем использовать схему сети из предыдущей лабораторной работы. Необходимо удалить сегменты. Сделаем это с помощью значка delete в левом верхнем углу (рис. 1).

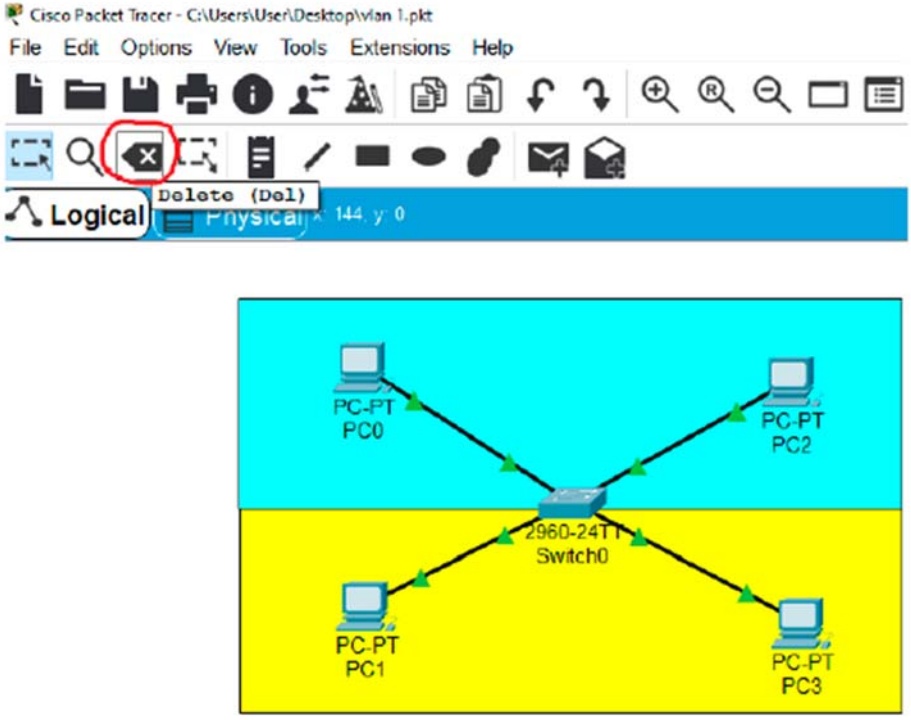


Рисунок 1 – Значок для удаления элементов сети

С помощью появившегося крестика удаляем 2 сегмента. Для этого необходимо щелкнуть крестиком на сегменте. Далее щелкаем на значок Select и выделяем всю область сети (рис. 2). После этого нажимаем на кнопку Ctrl, нажимаем на нашу сеть и перетаскиваем ее вправо, для того, чтобы сделать точно такую же копию нашей сети (рис. 3).

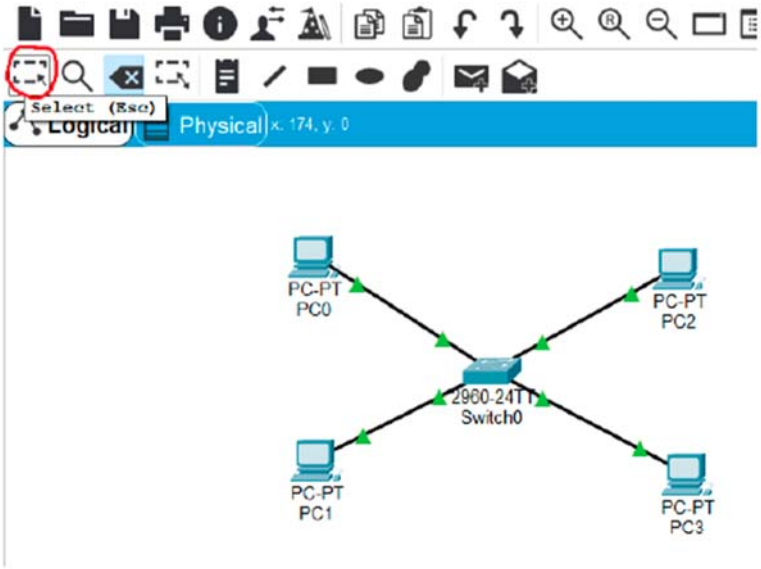


Рисунок 2 - Значок для копирования элементов сети

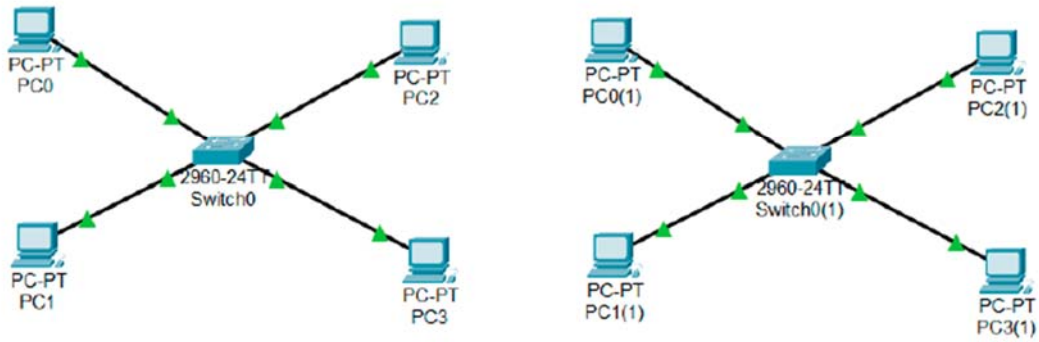


Рисунок 3 - Вторая сеть, полученная после операции копирования

Рисунок 3 - Вторая сеть, полученная после операции копирования

Теперь необходимо соединить два коммутатора 2960. Так как они от-носятся к одному уровню модели OSI, то соединять их нужно перекрестным кабелем. Пусть они будут соединены портами GigabitEthernet. Для соедине-ния коммутаторов лучше брать самые высокопроизводительные порты (рис.

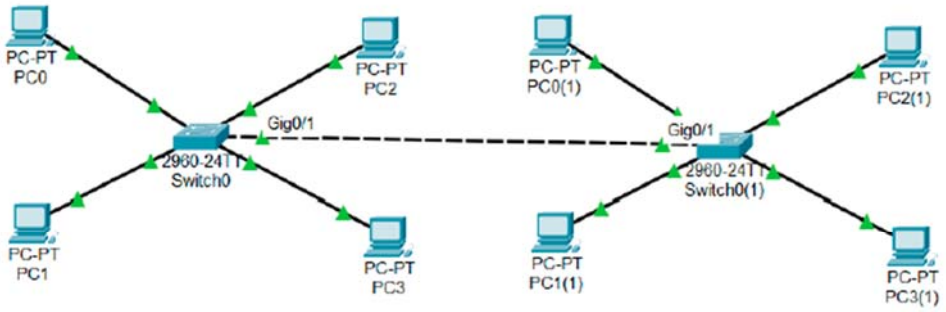


Рисунок 4 - Соединение двух коммутаторов с помощью высокопроизводительных портов GE

Поскольку мы сделали точную копию наших компьютеров PC0-PC3, то необходимо изменить IP-адресацию на вновь созданных компьютерах в соответствии с таблицей 1. Таблица №1. IP-адресация для компьютеров сети

Сетевой элемент	IP-адрес	VLAN
PC0	192.168.2.1	2
PC1	192.168.3.1	3
PC2	192.168.2.2	2
PC3	192.168.3.2	3
PC0 (1)	192.168.2.3	2
PC1 (1)	192.168.3.3	3
PC2 (1)	192.168.2.4	2
PC3 (1)	192.168.3.4	3

Пример изменения IP-адреса для компьютера PC0(1) показан на рисунке 5.

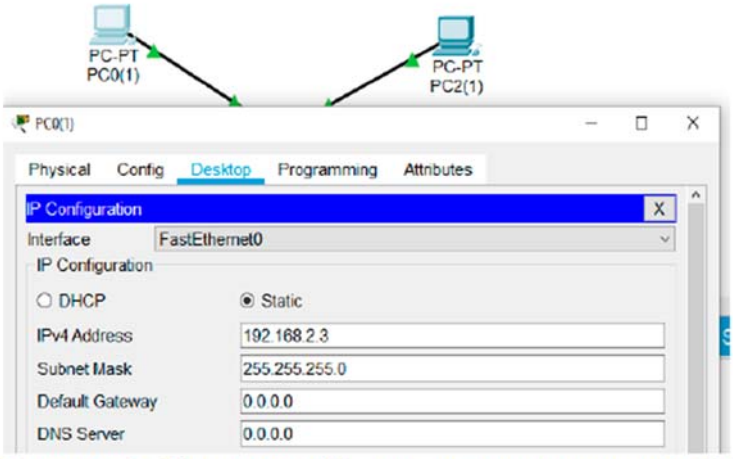


Рисунок 5 - Изменение IP- адреса для компьютера PC0(1)

На рисунке 6 показана схема компьютерной сети, которая разделена на 2 фрагмента.

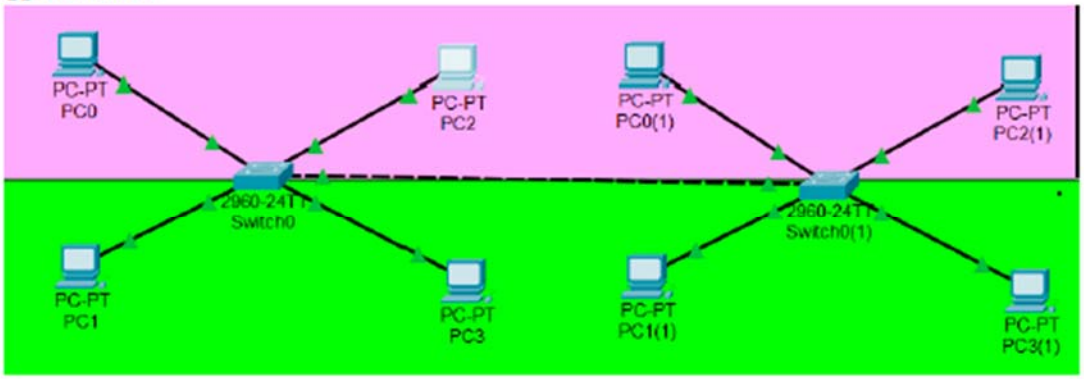
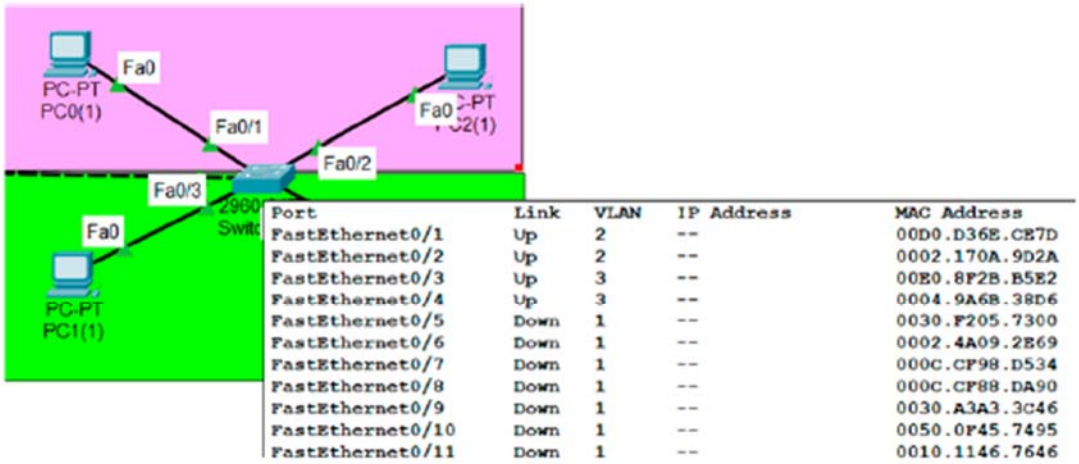


Рисунок 6 - Схема компьютерной сети, состоящая их двух фрагментов

Для того, чтобы проверить настройки второго коммутатора, то наводим на него курсор и смотрим порты и в каком они VLAN.



Port	Link	VLAN	IP Address	MAC Address
FastEthernet0/1	Up	2	--	00D0.D36E.CE7D
FastEthernet0/2	Up	2	--	0002.170A.9D2A
FastEthernet0/3	Up	3	--	00E0.8F2B.B5E2
FastEthernet0/4	Up	3	--	0004.9A6B.38D6
FastEthernet0/5	Down	1	--	0030.F205.7300
FastEthernet0/6	Down	1	--	0002.4A09.2E69
FastEthernet0/7	Down	1	--	000C.CF98.D534
FastEthernet0/8	Down	1	--	000C.CF88.DA90
FastEthernet0/9	Down	1	--	0030.A3A3.3C46
FastEthernet0/10	Down	1	--	0050.0F45.7495
FastEthernet0/11	Down	1	--	0010.1146.7646

Рисунок 7 - Проверка портов второго коммутатора

Таким образом, access – порты у нас уже настроены.

Для организации взаимодействия компьютеров, подключенных к разным коммутаторам, но находящихся в одном VLAN необходимо настроить trunk-порты, которые позволяет разбить физическое соединение на несколько сегментов. Далее переходим в режим конфигурирования для Switch0, для этого необходимо открыть вкладку CLI и ввести следующие команды:

Switch#configure terminal
Switch(config)#interface gigabitEthernet 0/1
Switch(config-if)#switchport mode trunk

Switch(config-if)#switchport trunk allowed vlan 2,3 (эта команда разрешает проходить через этот порт трафику VLAN 2 и 3)

Exit

Такие же настройки сделайте на коммутаторе Switch0(1).

Далее необходимо проверить связность между компьютерами. На рисунке 8 показана проверка связности между компьютером PC0 и PC0(1) а также между PC0 и PC1. Проверьте самостоятельно связность между другими компьютерами и объясните результаты.

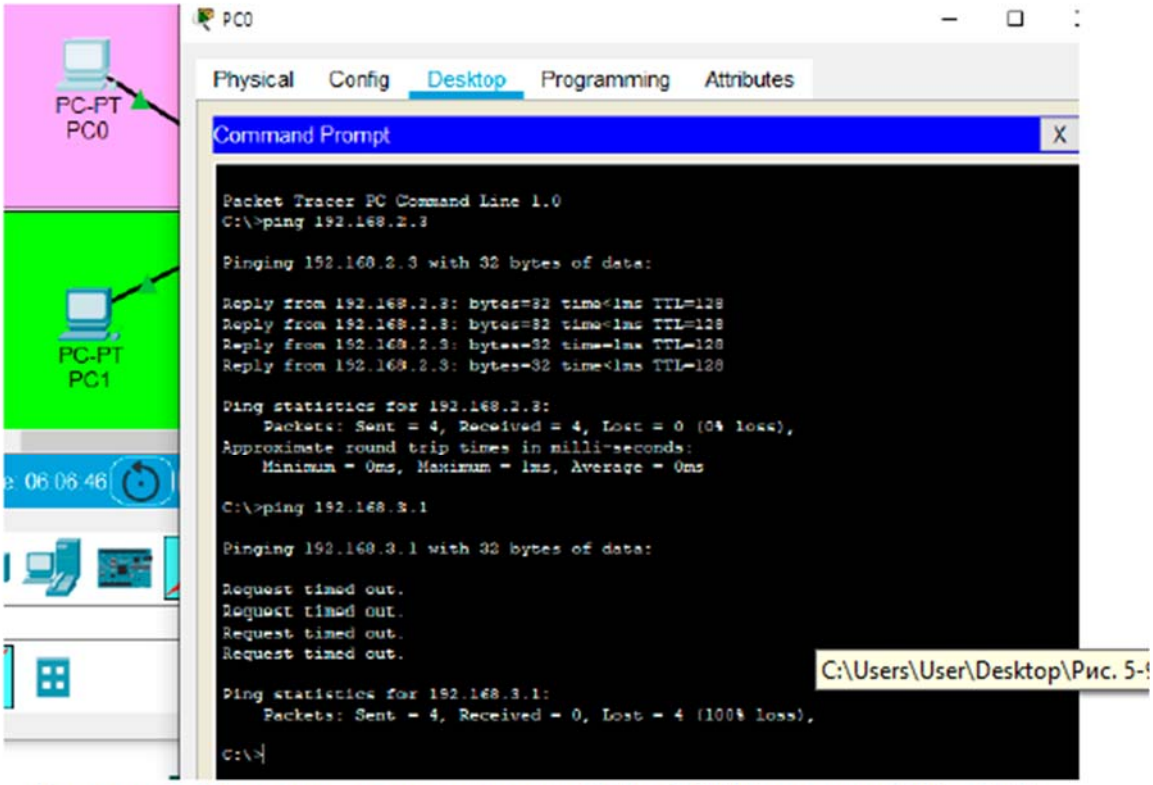


Рисунок 8 - Проверка связности между PC0 и PC0(1) и между PC0 и PC1

Содержание отчета

В индивидуальном отчёте должны быть указаны цель, задание, представлены необходимые снимки экрана и пояснения к ним. Следует проанализировать полученные данные.

Контрольные вопросы

1. Для чего применяется команда **Switch(config-if)#switchport trunk allowed vlan 2,3** в данной практической работе?
2. Как проверить связность компьютеров в одной VLAN?
3. Опишите последовательность настройки **access** портов**?**
4. Как настроить trunk- порты между коммутаторами?
5. Могут ли абоненты VLAN 3 получать широковещательный трафик, предназначенный для абонентов VLAN 2**?**
6. Опишите функцию trunk- порта?
7. Какого класса IP- адреса используются в данной работе?
8. Как можно определить номера интерфейсов на коммутаторе?
9. В какой подсети находится компьютер с адресом 192.168.3.2?
10. Что означает команда **Switch(config)#**?

Практическое занятие № 7 - Маршрутизатор (роутер).

24.11.2023, 25.11.2023 -4 часа

Тема: Маршрутизатор (роутер).

Как только в сети появляются два сегмента (сегмент пользователей и сегмент серверов) то возникает необходимость использования маршрутизирующего оборудования (оборудования которое функционирует на 3 уровне модели OSI).

В этом случае у нас 2 варианта:

1 – коммутатор 3-го уровня OSI;

2 – маршрутизатор (роутер).

Коммутаторы 3-го уровня (или маршрутизаторы локальных сетей) – это коммутаторы, в которые встроены функции маршрутизации пакетов.

Основной особенностью коммутаторов 3-го уровня является высокая скорость выполнения операций маршрутизации за счет их перенесения на аппаратный уровень – уровень БИС/ASIC.

Изначально у этих двух устройств различное предназначение.

Коммутатор 3-го уровня (L3 switch) - это прежде всего устройство для локальной вычислительной сети (LAN - Local Area Network). Т.е. данный коммутатор должен маршрутизировать трафик в локальной сети между существующими сегментами. Обычно он используется на уровне распределения (Distribution Layer) в иерархической модели сети.

Маршрутизатор предназначен для подключения локальной сети (LAN) к Глобальной компьютерной сети (WAN - Wide Area Network), т.е. осуществляет маршрутизацию трафика во внешний мир (Интернет, филиалы, удаленные сотрудники) и обратно.

Может возникнуть вопрос: “Зачем нужен коммутатор 3-го уровня, если его функции может выполнять маршрутизатор?”

Если не вдаваться в подробности, то коммутатор третьего уровня можно сравнить с очень быстрым маршрутизатором. Он также умеет работать с протоколами динамической маршрутизации (OSPF, RIP) и абсолютно совместим с обычным маршрутизатором. Доступна настройка списков доступа (так называемые access листы) и многое другое.

Ответ кроется в производительности и цене. Дело в том, что современные коммутаторы 3-го уровня превосходят по производительности маршрутизаторы в десятки и даже сотни раз. Обусловлено это применением в коммутаторах набора специализированных микросхем (ASIC). Маршрутизация (обработка пакетов) происходит на аппаратном уровне, а программная поддержка остается для процедур, которые напрямую не связаны с обработкой трафика: расчет таблиц маршрутизации, списки доступа и т.д.

У обычного маршрутизатора этот механизм (обработка пакетов) реализован программно, и он как правило функционирует на процессоре общего назначения. Однако стоит отметить, что некоторые современные маршрутизаторы так же имеют специальные выделенные микросхемы для ускорения обработки пакетов без использования процессора, но такие маршрутизаторы гораздо дороже коммутаторов 3-го уровня.

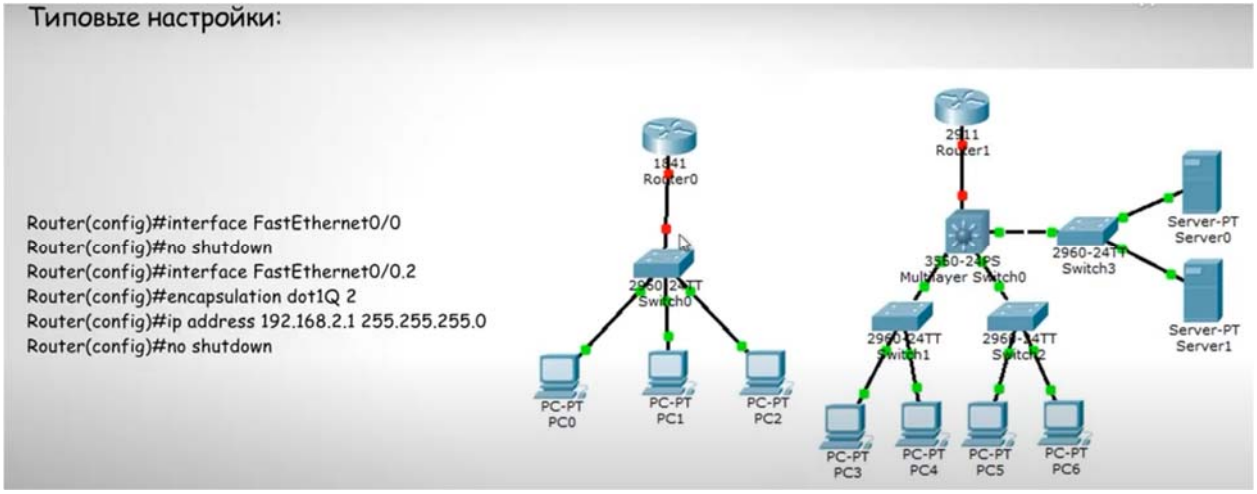
Представьте ситуацию, когда у вас в организации расположен датацентр и требуется маршрутизация трафика на больших скоростях - десятки Гигабит в секунду. В этом случае вам подходит только коммутатор 3-го уровня. Маршрутизатор с такой пропускной способностью просто не справится или будет стоить огромных денег.

И опять может возникнуть вопрос: “Зачем использовать маршрутизатор, если его функции может выполнять коммутатор 3-го уровня? Ведь он быстрее и дешевле?”

Не вдаваясь в технические подробности, если более детально рассматривать функции маршрутизации, то коммутатор третьего уровня проигрывает по возможностям традиционному маршрутизатору. Современный маршрутизатор можно с легкостью превратить в полноценный Межсетевой экран (МЭ) с помощью дополнительных лицензий (отличие маршрутизатора от межсетевого экрана мы рассмотрим чуть позже).

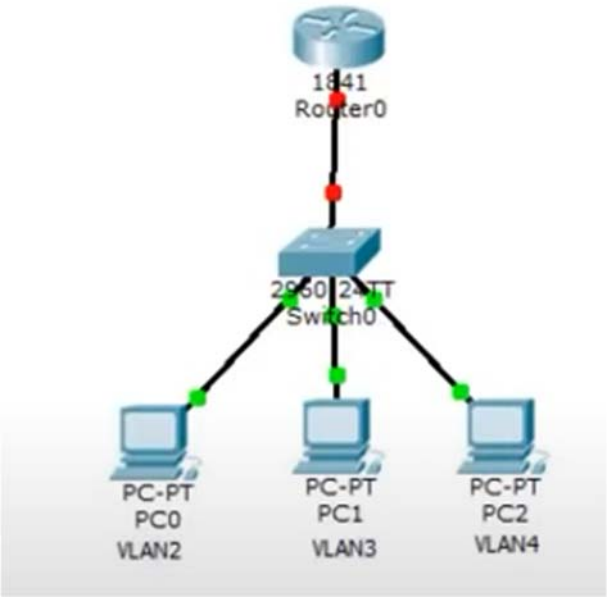
Со временем грань между коммутаторами и маршрутизаторами становится все тоньше. Не исключено что в скором времени ее и вовсе не будет видно.

Таким образом, в случае подключения локальной сети к Интернет или построении VPN канала с удаленными филиалами (а так же удаленное подключение пользователей) необходимо использовать маршрутизатор.



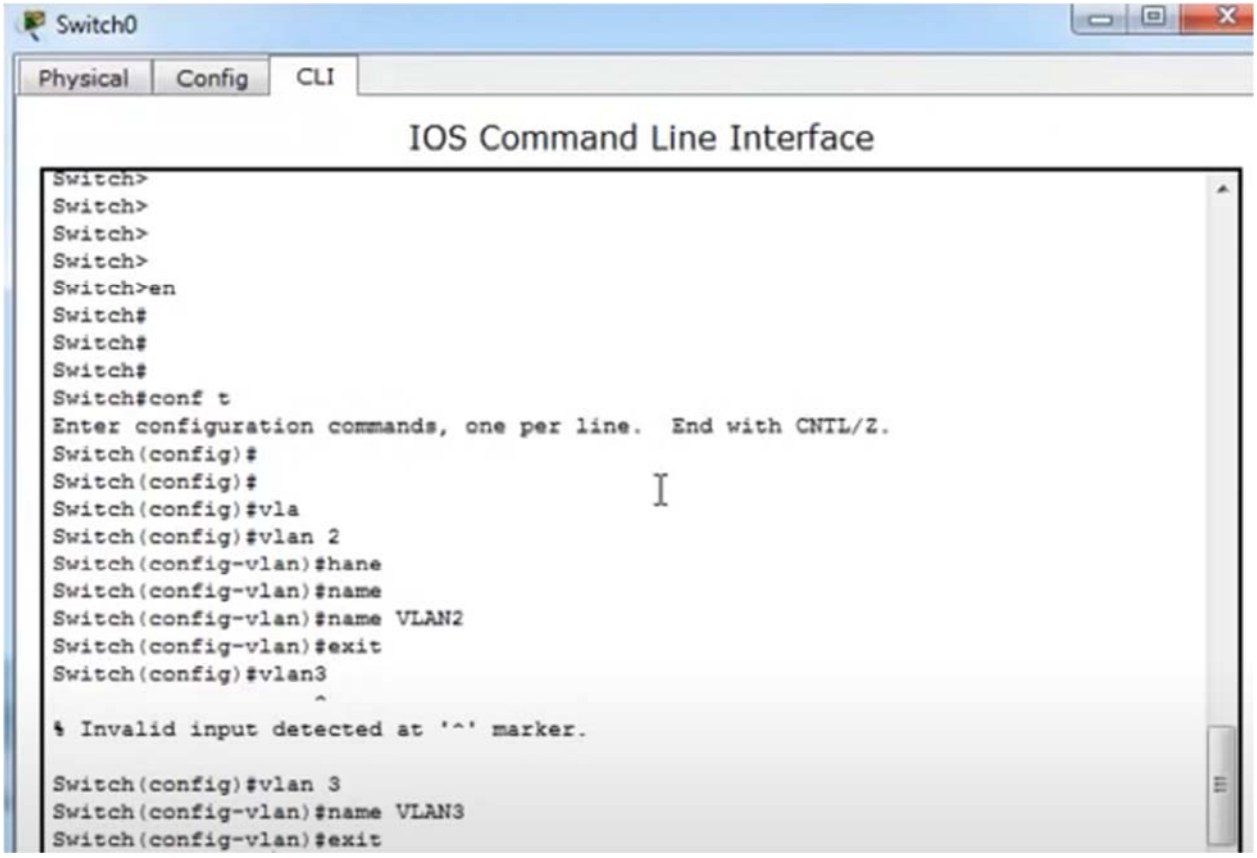
1 случай «Небольшой офис»

Маленький трафик и отсутствие серверов-Нет необходимости ставить L3 коммутатор (от 1000$).



Значит ставим маршрутизатор (5000р)

Настраиваем Коммутатор 2-го уровня

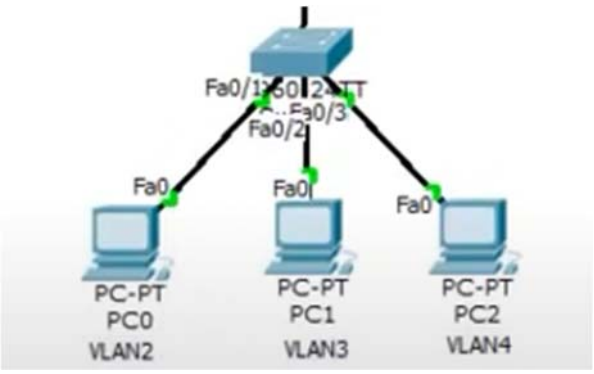


Определяем порты к которым подключены

ПК1-Fa0/1

ПК2-Fa0/2

ПК3-Fa0/3



Настраиваем интерфейсы на коммутаторе

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int fa
Switch(config)#int fastEthernet 0/1
Switch(config-if)#sw
Switch(config-if)#switchport mod
Switch(config-if)#switchport mode acc
Switch(config-if)#switchport mode access
Switch(config-if)#sw
Switch(config-if)#switchport acc
Switch(config-if)#switchport access vl
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
```

```
Switch(config)#int fa0/2
Switch(config-if)#sw
Switch(config-if)#switchport mod
Switch(config-if)#switchport mode acc
Switch(config-if)#switchport mode access
Switch(config-if)#sw
Switch(config-if)#switchport acc
Switch(config-if)#switchport access vl
Switch(config-if)#switchport access vlan 3
Switch(config-if)#exit
```

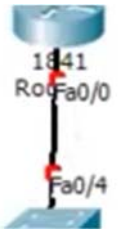
```
Switch(config)#int fa
Switch(config)#int fastEthernet 0/3
Switch(config-if)#sw
Switch(config-if)#switchport mod
Switch(config-if)#switchport mode acc
Switch(config-if)#switchport mode access
Switch(config-if)#sw
Switch(config-if)#switchport acc
Switch(config-if)#switchport access vl
Switch(config-if)#switchport access vlan 4
```

exit

Настраиваем trunk порт до маршрутизатора

Хочу заострить внимание на том, что тегирование кадров осуществляется между сетевыми устройствами (коммутаторы, маршрутизаторы и т.д.), а между конечным узлом (компьютер, ноутбук) и сетевым устройством кадры не тегируются. Поэтому порт сетевого устройства может находиться в 2-х состояниях: **access** или **trunk**.

- **Access port или порт доступа** — порт, находящийся в определенном VLAN и передающий не тегированные кадры. Как правило, это порт, смотрящий на пользовательское устройство.
- **Trunk port или магистральный порт** — порт, передающий тегированный трафик. Как правило, этот порт поднимается между сетевыми устройствами.



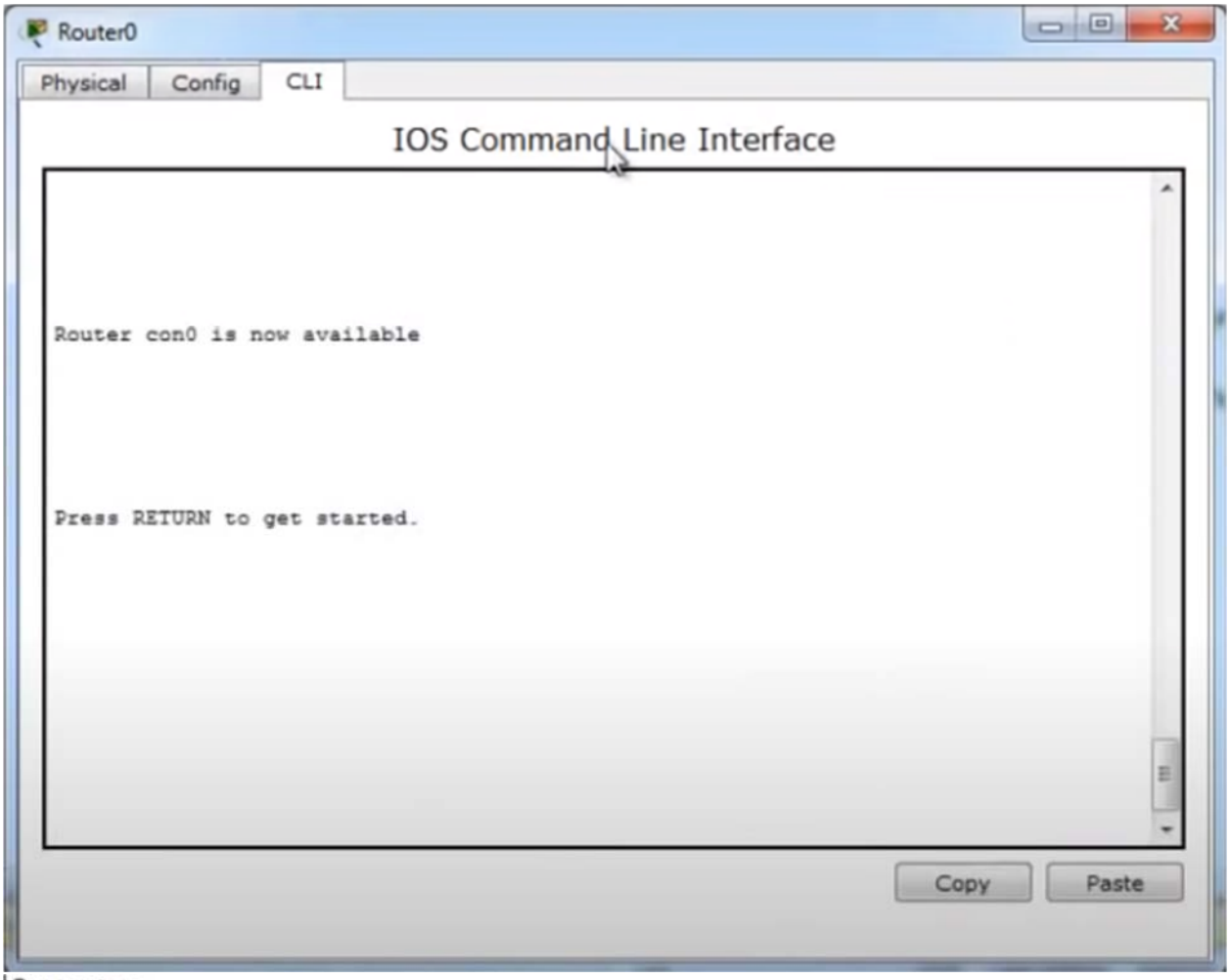
Это у коммутатора fa 0/4

```
Switch(config)#int fa0/4
Switch(config-if)#sw
Switch(config-if)#switchport mod
Switch(config-if)#switchport mode tr
Switch(config-if)#switchport mode trunk
Switch(config-if)#sw
Switch(config-if)#switchport tr
Switch(config-if)#switchport trunk vl
Switch(config-if)#switchport trunk all
Switch(config-if)#switchport trunk allowed vl
Switch(config-if)#switchport trunk allowed vlan 2,3,4
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#
Switch#
```

Сохраняем конфигурацию

```
Switch#
Switch#wr mem
Building configuration...
[OK]
Switch#
```

Настраиваем Router0




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

Поднимаем физический порт. У маршрутизатора они по умолчанию выключены.
Fa 0/0

```
Router(config)#int fa
Router(config)#int fastEthernet 0/0
Router(config-if)#no shut
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
```

Exit

На роутер приходят 3 Vlan 2,3,4. На нем необходимо поднять **subinterfaces** под-интерфейсы.

(Для настройки взаимодействия между несколькими виртуальными сетями (**Vlan**), расположенными на одном коммутаторе, необходим маршрутизатор, подключенный к коммутатору через **Trunk** порт. При передаче трафика по этому порту каждый пакет помечается номером **Vlan**, которому принадлежит. Это позволяет устройствам корректно

перенаправлять пакеты.
На этом интерфейсе настраиваются сабинтерфейсы (**subinterfaces**) с соответствующими **ip** адресами для каждой из сетей **Vlan**.)

Каждому под-интерфейсу соответствует определенный Vlan.

```
Router(config)#int
Router(config)#interface fa
Router(config)#interface fastEthernet 0/0.2
Router(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.2, changed state
 to up

Router(config-subif)#
```

Указываем номер Vlan

Vlan 2

```
Router(config-subif)#
Router(config-subif)#
Router(config-subif)#enc
Router(config-subif)#encapsulation do
Router(config-subif)#encapsulation dot1Q 2
Router(config-subif)#ip add
Router(config-subif)#ip address 192.168.2.1 255.255.255.0
Router(config-subif)#no shut
Router(config-subif)#no shutdown
Router(config-subif)#
Router(config-subif)#
Router(config-subif)#
Router(config-subif)#exit
Router(config)#
```

Приземляем Vlan3

```
Router(config-subif)#sw
Router(config-subif)#enc
Router(config-subif)#encapsulation do
Router(config-subif)#encapsulation dot1Q 3
Router(config-subif)#ip add
Router(config-subif)#ip address 192.168.3.1 255.255.255.0
Router(config-subif)#no shut
Router(config-subif)#no shutdown
Router(config-subif)#
Router(config-subif)#exit
```

Приземляем Vlan 4

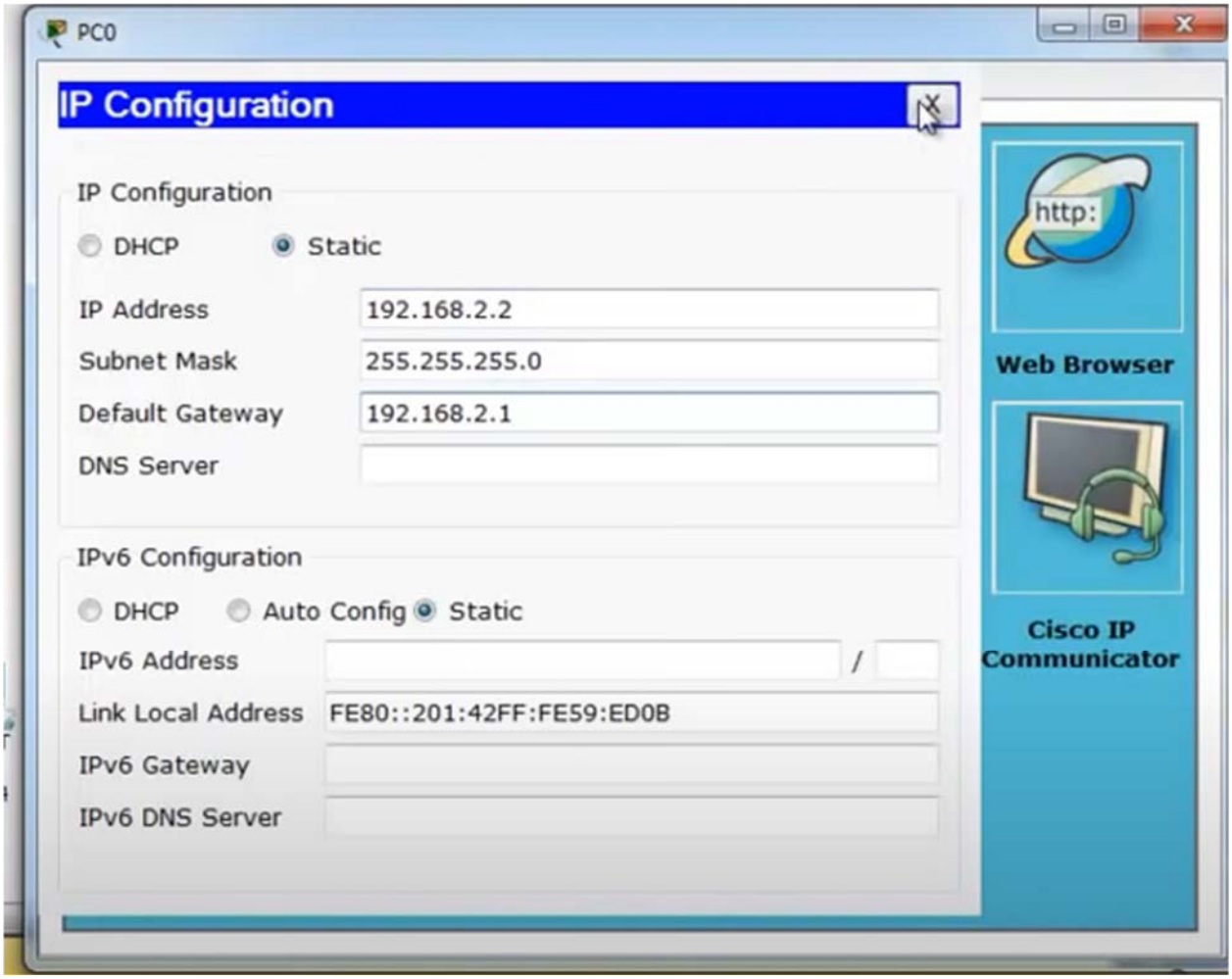
```
Router(config-subif)#enc
Router(config-subif)#encapsulation do
Router(config-subif)#encapsulation dot1Q 4
Router(config-subif)#ip add
Router(config-subif)#ip address 192.168.4.1 255.255.255.0
Router(config-subif)#no shut
Router(config-subif)#no shutdown
Router(config-subif)#
Router(config-subif)#
Router(config-subif)#
Router(config-subif)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

```
Router#wr mem
Building configuration...
[OK]
```

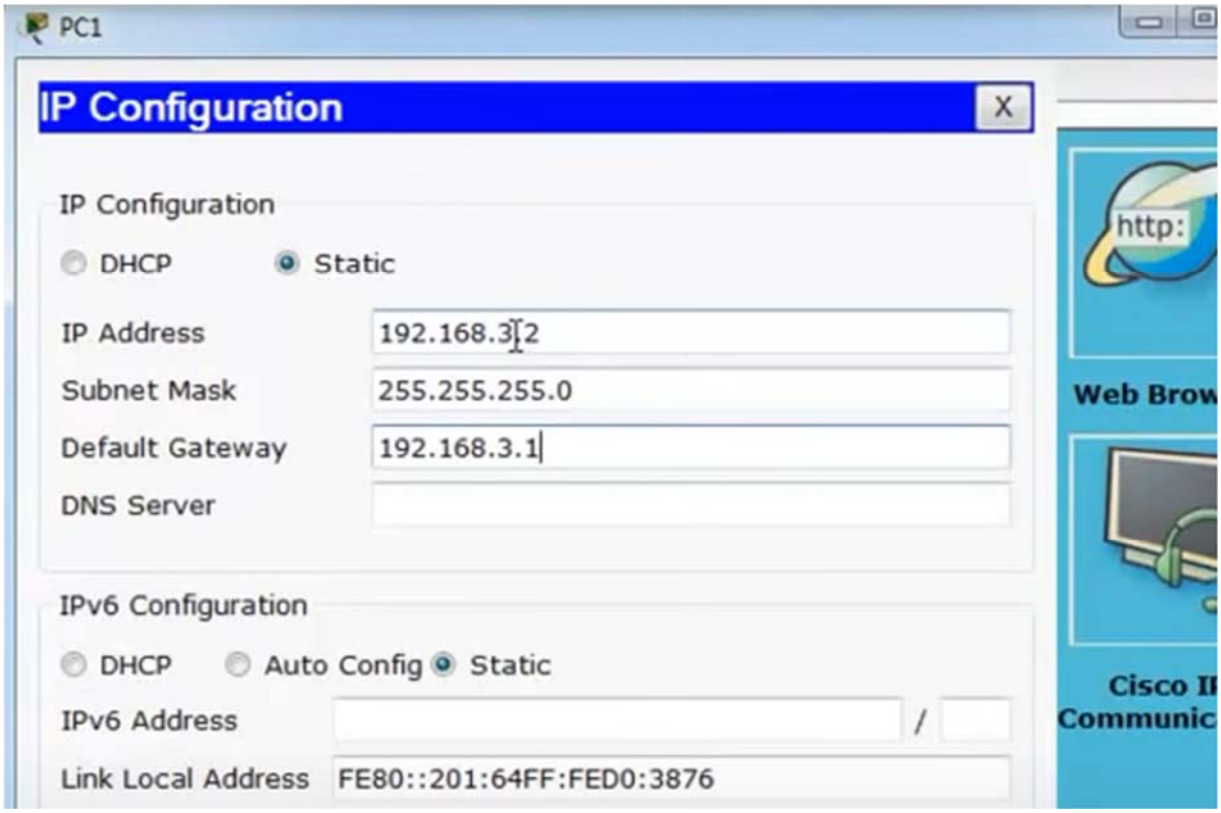
Show run

```
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.2
 encapsulation dot1Q 2
 ip address 192.168.2.1 255.255.255.0
!
interface FastEthernet0/0.3
 encapsulation dot1Q 3
 ip address 192.168.3.1 255.255.255.0
!
interface FastEthernet0/0.4
 encapsulation dot1Q 4
 ip address 192.168.4.1 255.255.255.0
!
interface FastEthernet0/1
 no ip address
```

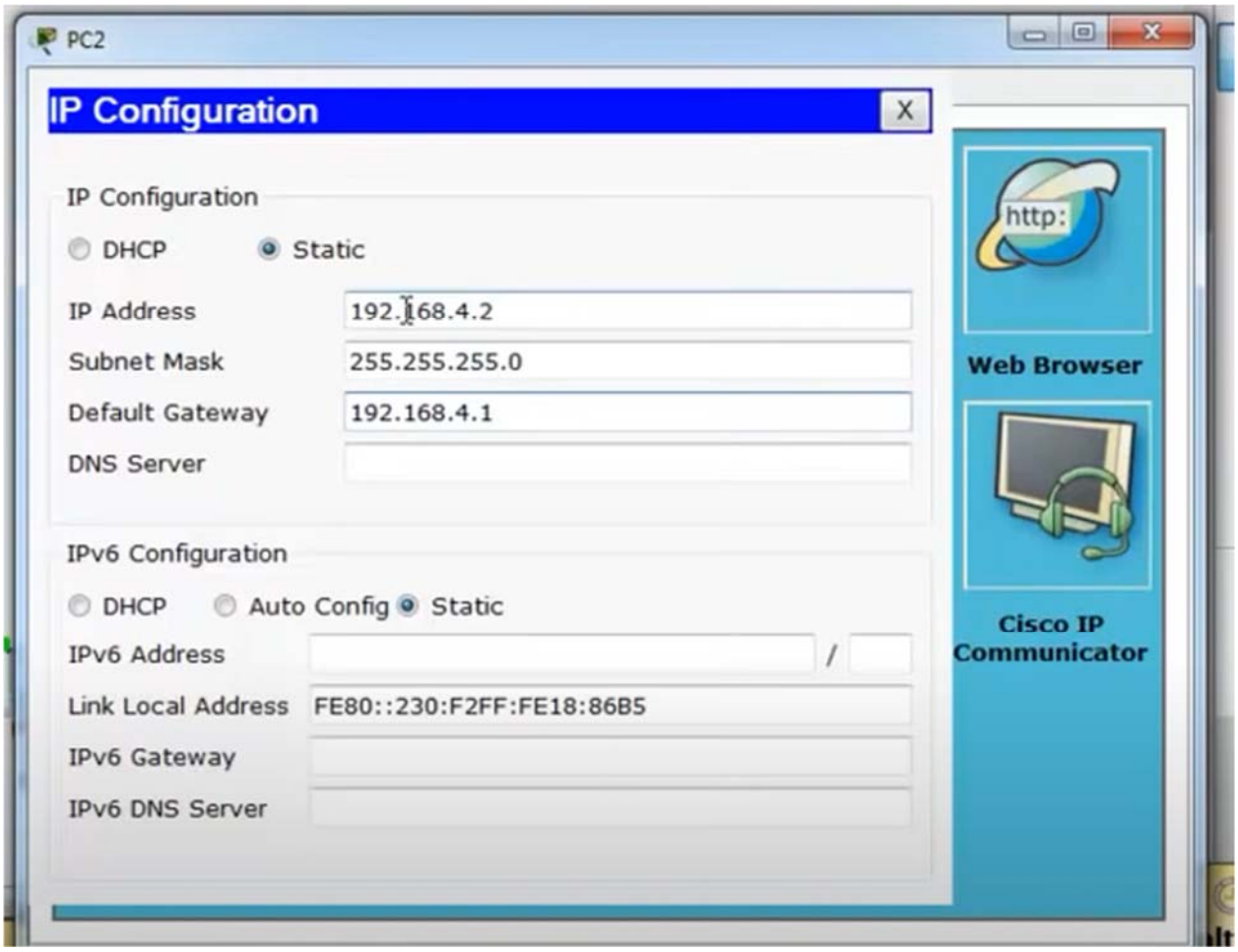
Настраиваем ПК1



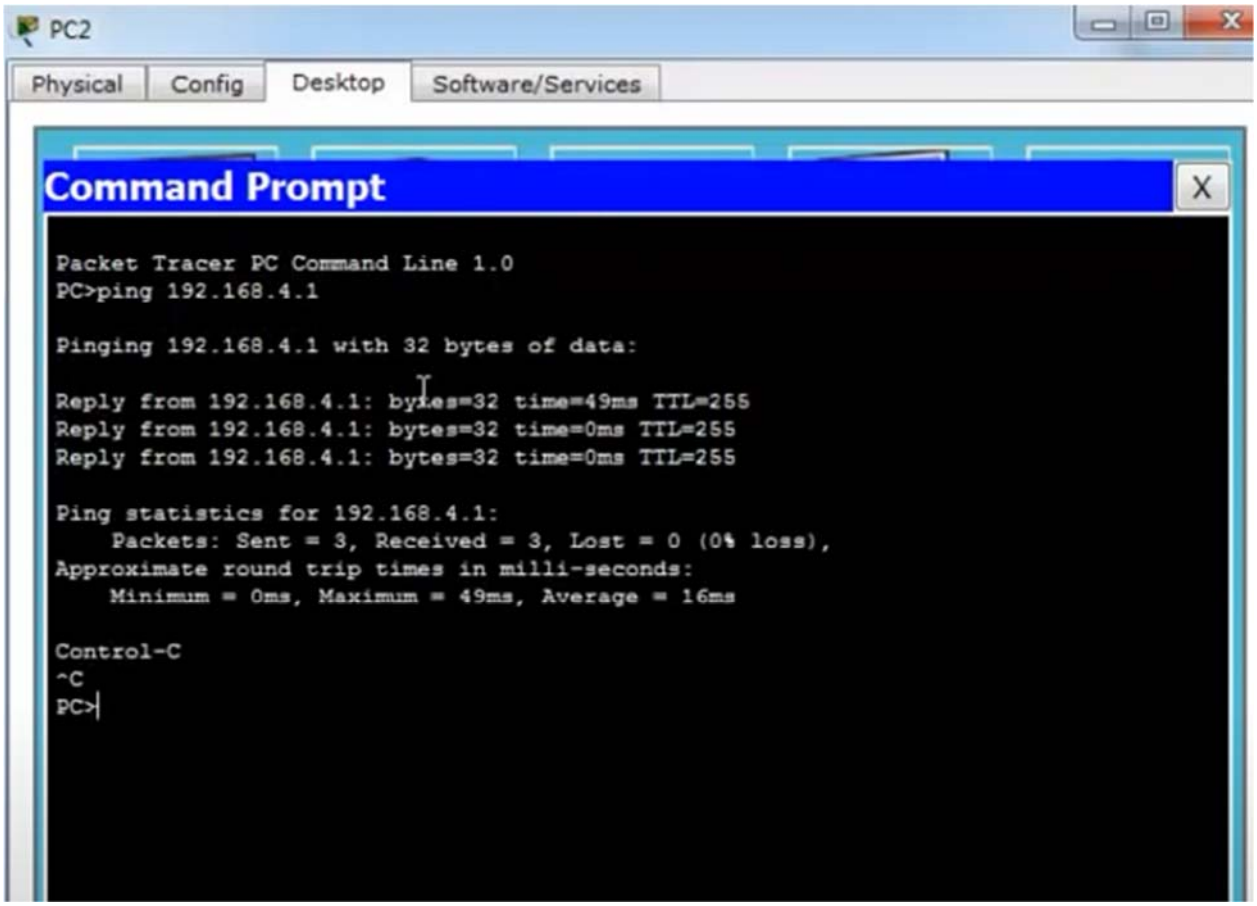
ПК2



ПК3



Пингуем шлюз



Пингуем соседние сегменты

```
PC>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Reply from 192.168.3.2: bytes=32 time=1ms TTL=127
Reply from 192.168.3.2: bytes=32 time=1ms TTL=127
Reply from 192.168.3.2: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.3.2:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

Control-C
```

```
^C
PC>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.2: bytes=32 time=0ms TTL=127
Reply from 192.168.2.2: bytes=32 time=0ms TTL=127
Reply from 192.168.2.2: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

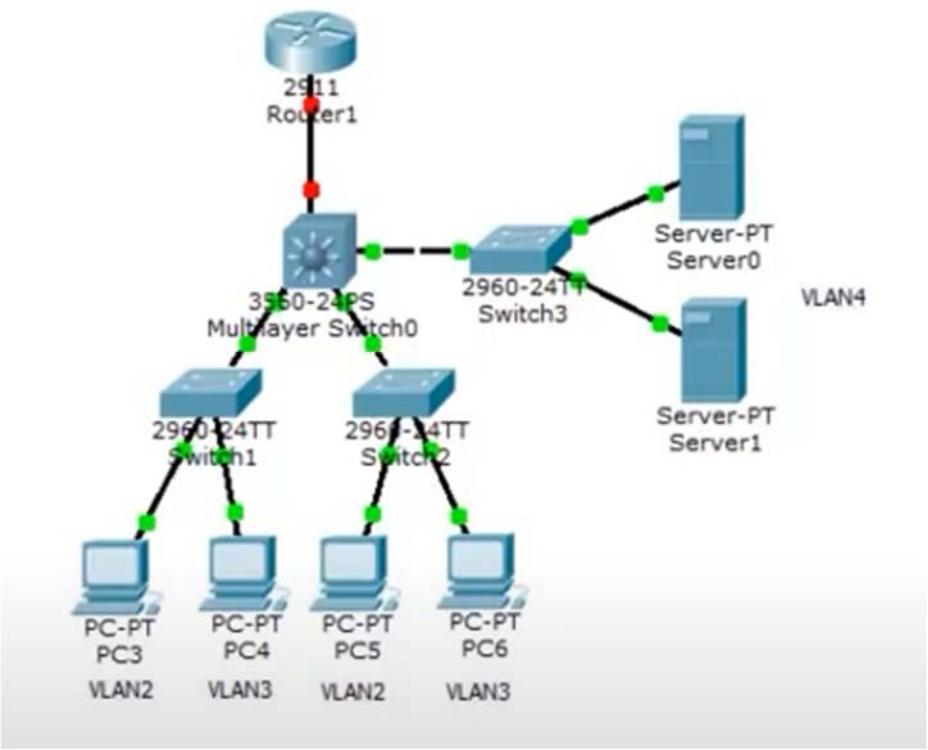
NAT

Сети обычно проектируются с использованием частных IP адресов. Это адреса 10.0.0.0/8, 172.16.0.0/12 и 192.168.0.0/16. Эти частные адреса используются внутри организации или площадки, чтобы позволить устройствам общаться локально, и они не маршрутизируются в интернете. Чтобы позволить устройству с приватным IPv4-адресом обращаться к устройствам и ресурсам за пределами локальной сети, приватный адрес сначала должен быть переведен на общедоступный публичный адрес.

И вот как раз NAT переводит приватные адреса, в общедоступные. Это позволяет устройству с частным адресом IPv4 обращаться к ресурсам за пределами его частной сети. NAT в сочетании с частными адресами IPv4 оказался полезным методом сохранения общедоступных IPv4-адресов. Один общедоступный IPv4-адрес может быть использован сотнями, даже тысячами устройств, каждый из которых имеет частный IPv4-адрес. NAT имеет дополнительное преимущество, заключающееся в добавлении степени конфиденциальности и безопасности в сеть, поскольку он скрывает внутренние IPv4-адреса из внешних сетей.

Маршрутизаторы с поддержкой NAT могут быть настроены с одним или несколькими действительными общедоступными IPv4-адресами. Эти общедоступные адреса называются пулом NAT. Когда устройство из внутренней сети отправляет трафик из сети наружу, то маршрутизатор с поддержкой NAT переводит внутренний IPv4-адрес устройства на общедоступный адрес из пула NAT. Для внешних устройств весь трафик, входящий и выходящий из сети, выглядит имеющим общедоступный IPv4 адрес.

2 случай «большой офис»



Имеются несколько коммутаторов уровня доступа и 100 компьютеров. Присутствуют выделенные серверы. Трафик высокий и маршрутизатор с данной нагрузкой не справится либо будет стоить огромных денег. В данном случае необходимо применять коммутатор 3-го уровня OSI.

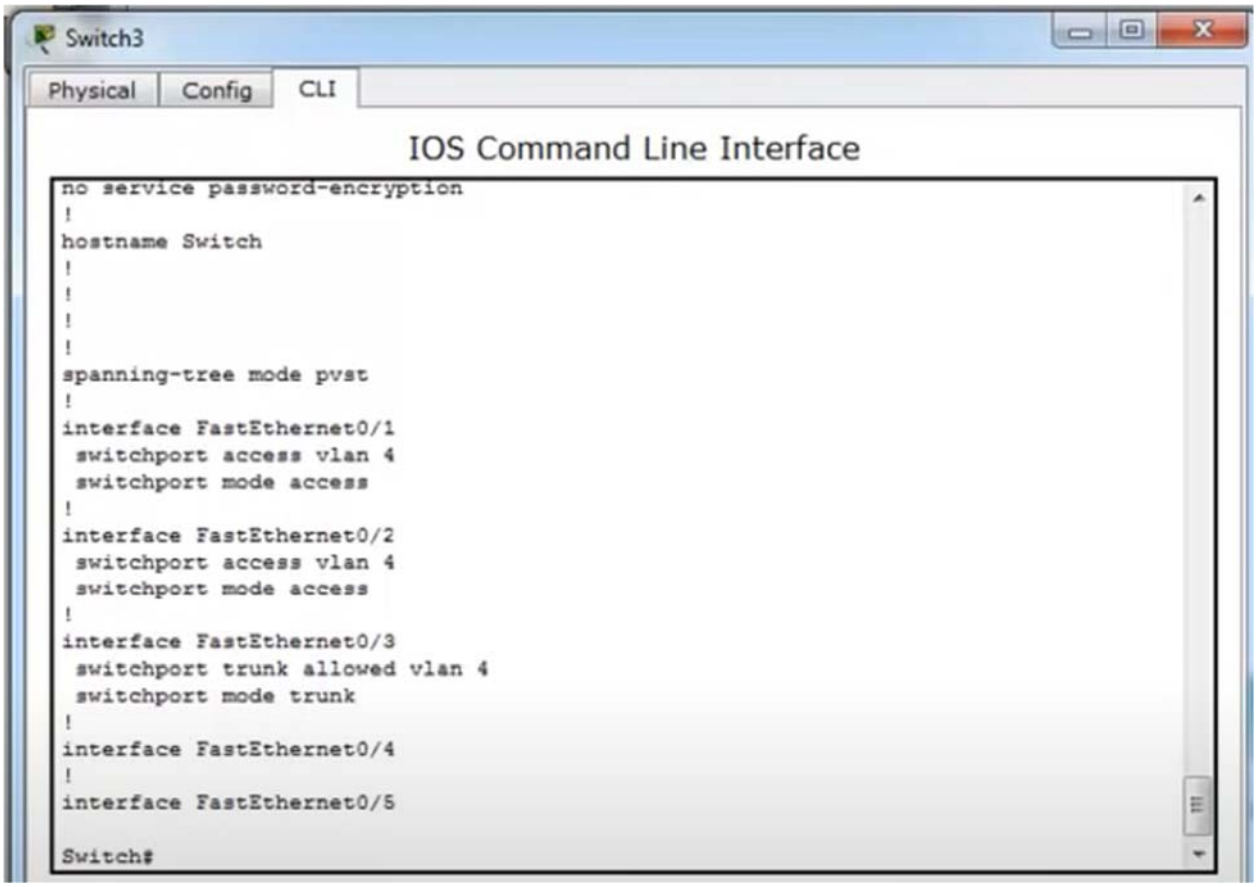
PC3, PC5 - Vlan2

PC4, PC6 – Vlan3

Server - Vlan4

Switch1

2 –Acces Порта и 1 Trunk порт на коммутатор



IP для ПК

Vlan2 сеть 192.168.22.1

PC3 192.168.22.2

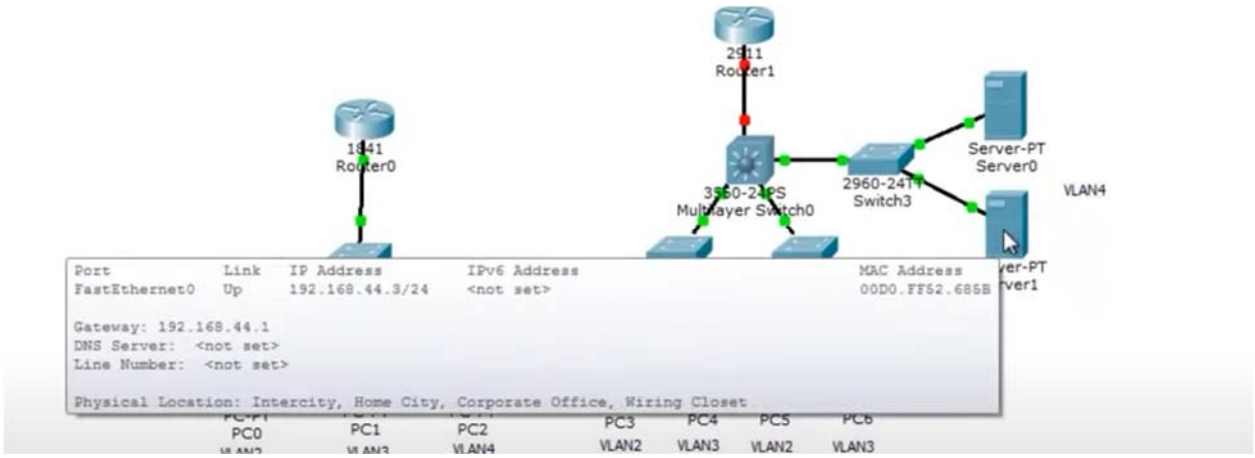
PC5 192.168.22.3

Vlan3 сеть 192.168.33.1

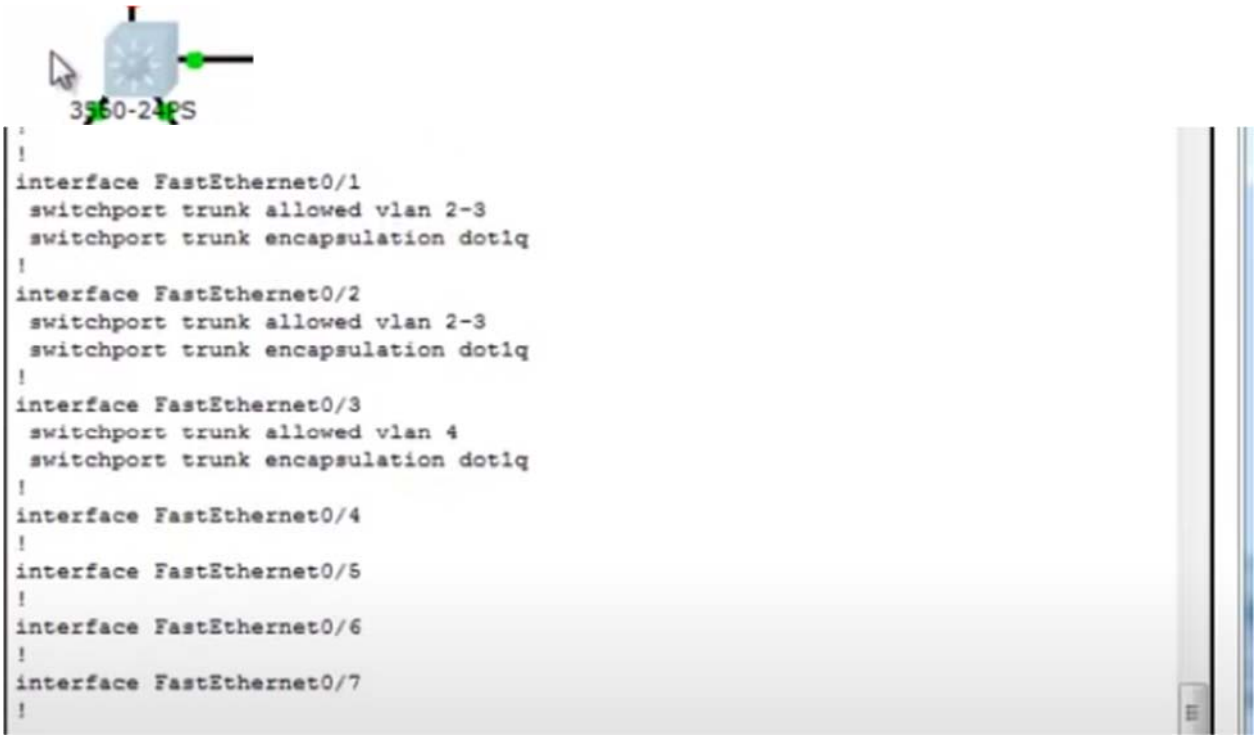
PC4 192.168.33.2

PC6 192.168.33.2

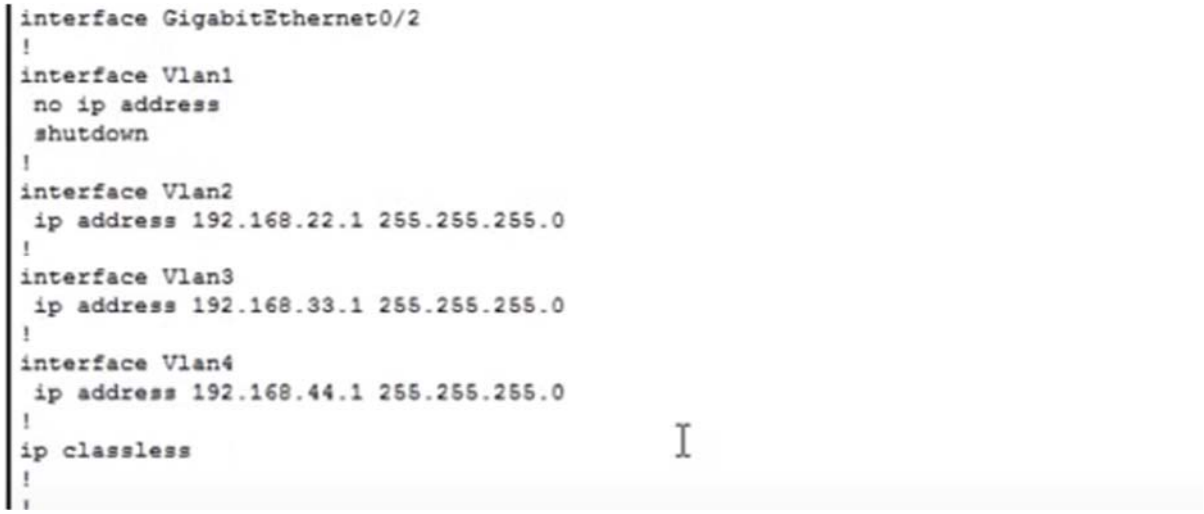
Серверы



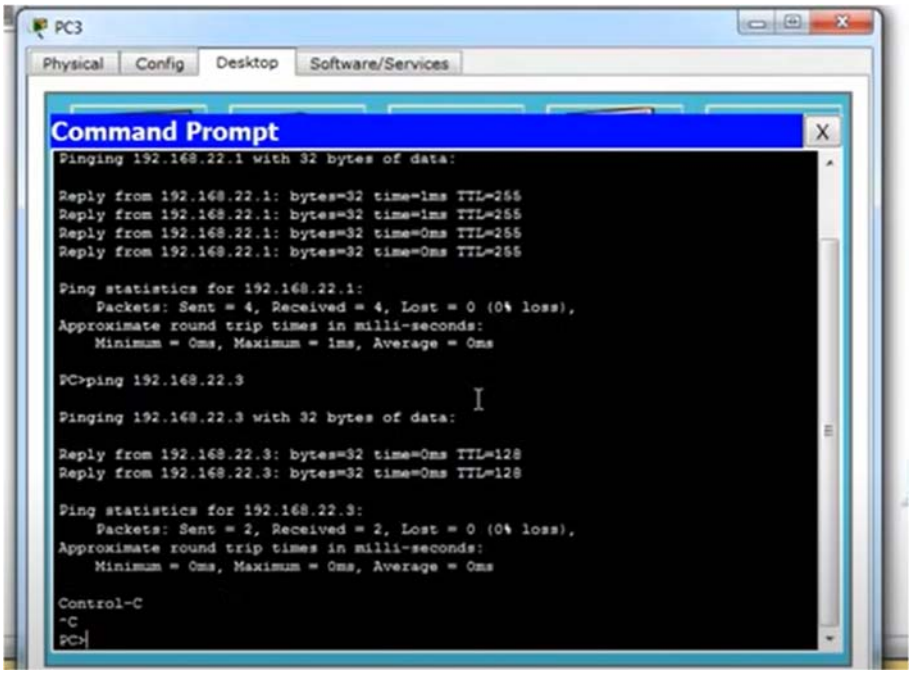
Настройка коммутатора 3-го уровня



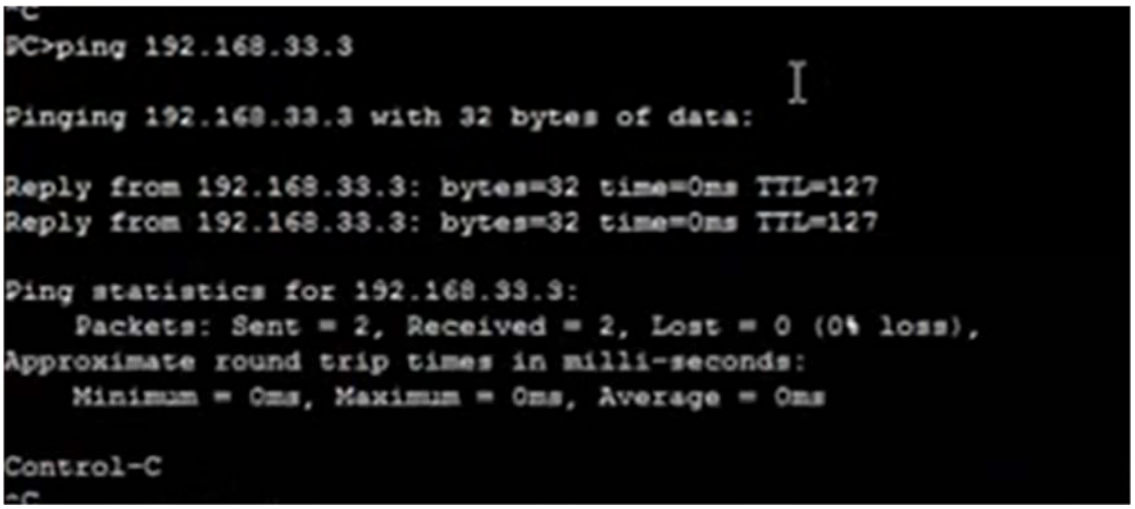
Должны быть подняты виртуальные интерфейсы см. ПР4



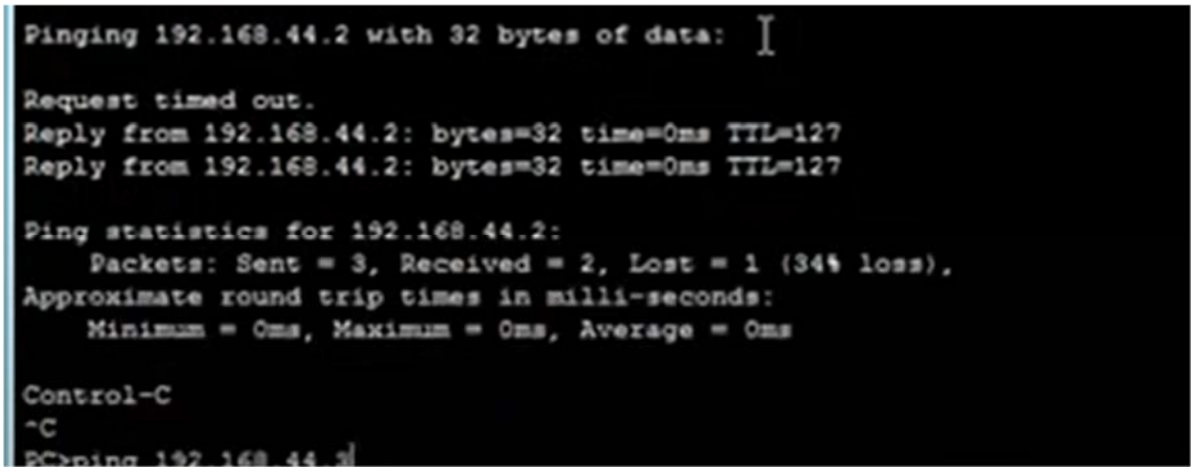
Проверяем соединения Vlan2



Vlan 3



Vlan 4

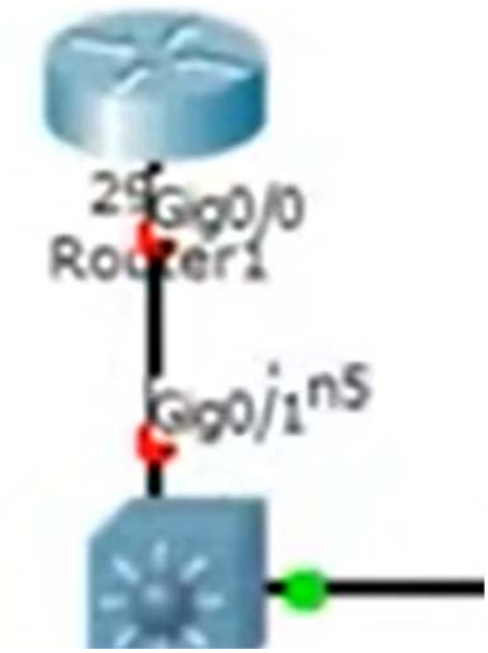


Задержка вызвана несовершенством программы

Настройка маршрутизатора

Сегмент Vlan5

Настраиваем коммутатор 3 уровня



Соединение через GigabitEthernet port

```
Switch#
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int vla
Switch(config)#int vlan 5
Switch(config-if)#anme
Switch(config-if)#name
Switch(config)#vlan 5
Switch(config-vlan)#
%LINK-5-CHANGED: Interface Vlan5, changed state to up

Switch(config-vlan)#name
Switch(config-vlan)#name vlan5
Switch(config-vlan)#
Switch(config-vlan)#exit
Switch(config)#int vla
Switch(config)#int vlan 5
Switch(config-if)#ip add
Switch(config-if)#ip address 192.168.55.2 255.255.255.
```

192.168.55.1 будет у Router1

```
Switch(config-if)#no shut
Switch(config-if)#no shutdown
Switch(config-if)#
```

```
Switch(config-if)#exit
Switch(config)#int gi0/1
Switch(config-if)#acc
Switch(config-if)#sw
Switch(config-if)#switchport mod
Switch(config-if)#switchport mode acc
Switch(config-if)#switchport mode access
Switch(config-if)#sw
Switch(config-if)#switchport acc
Switch(config-if)#switchport access vl
Switch(config-if)#switchport access vlan 5
Switch(config-if)#
```

End

Show run

```
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan2
 ip address 192.168.22.1 255.255.255.0
!
interface Vlan3
 ip address 192.168.33.1 255.255.255.0
!
interface Vlan4
 ip address 192.168.44.1 255.255.255.0
!
interface Vlan5
 ip address 192.168.55.2 255.255.255.0
!
ip classless
!
!
```

Интерфейс поднят. Сохраняем настройки

```
!

Switch#wr mem
Building configuration...
[OK]
Switch#
```

Настраиваем маршрутизатор Router1

Включаем порт

Gg0/0

```
Router#
Router#
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)#
Router(config)#int gi
Router(config)#int gigabitEthernet 0/0
Router(config-if)#no shut
Router(config-if)#no shutdown
```

Y

Назначаем IP

```
Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)#ip add
Router(config-if)#ip address 192.168.55.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#no shutdown
Router(config-if)#
Router(config-if)#
```

Проверка

```
Router#
Router#
Router#ping 192.168.55.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.55.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms

Router#ping 192.168.55.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.55.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

Router#
```

Пинг идет между маршрутизатором и коммутатором 3 уровня

Ping на ПК

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

Router#
Router#
Router#
Router#ping 192.168.22.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.22.2, timeout is 2 seconds:
```

PC-PT
PC3
VLAN2

Пинг не идет. Дело в статической маршрутизации. Это тема 27.11.2023

Вопросы к занятию

1 Коммутатор 3 - го уровня OSI

2 Маршрутизатор

3 Acces port

4 Trunk порт

5 Vlan

Практическое занятие № 8 - Агрегирование каналов в коммутаторах. Часть 1

25.11.2023 -2 часа

Цель :

Изучить принципы статического и динамического агрегирования кана-лов.

Задание

1.Ознакомиться с принципами статического агрегирования каналов;

2. Ознакомиться с принципами динамического агрегирования каналов. 3.Ответить на вопросы.

Краткая теория

Часто для повышения пропускной способности и коммутатора удобно объединить несколько каналов. Это позволит также обеспечить резервирование в случае выхода из строя одного из каналов. Такая группа каналов рассматривается как единый интерфейс, а нагрузка равномерно распределяется между ними. Технология, которая позволяет это сделать называется Link Aggregation (объединение звеньев) (рис. 1). При этом для равномерного распре-деления трафика требуется, чтобы физические характеристики звеньев были одинаковы. На рисунке 1 три физических соединения между коммутаторами объединяются в одно логическое. Все соединения агрегированного канала являются активными и передают информацию.

Важным моментом при реализации объединения портов в агрегированный канал является распределение трафика по ним. Если пакеты одного сеанса будут передаваться по разным портам агрегированного канала, то может возникнуть проблема на более высоком уровне модели OSI. Например, если два или более смежных кадров одного сеанса станут передаваться через разные порты агрегированного канала, то из-за неодинаковой длины очередей в их буферах может возникнуть ситуация, когда из-за неравномерной задержки передачи кадра более поздний кадр обгонит предыдущий.

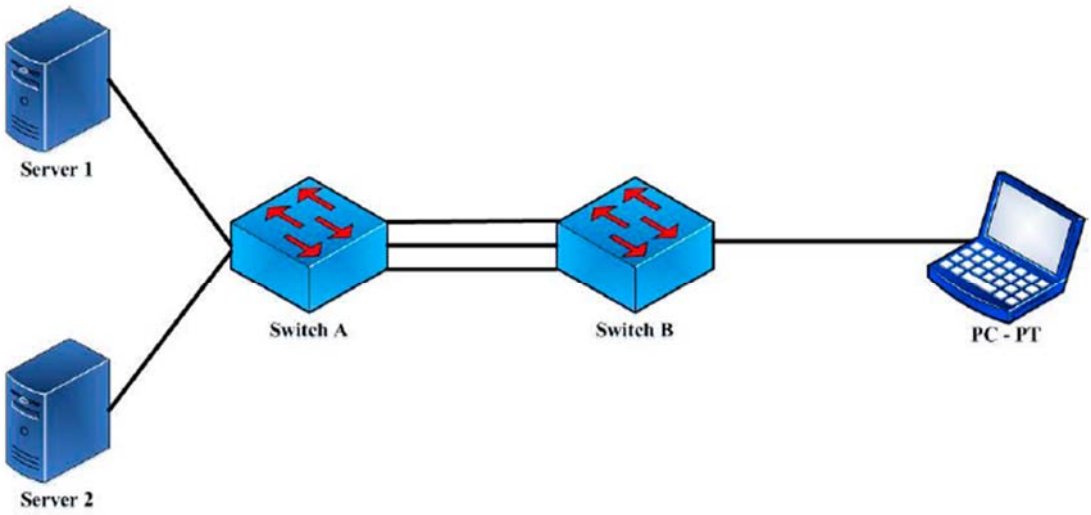


Рисунок 1 - Агрегирование каналов в коммутаторах

Поэтому в большинстве реализаций механизмов агрегирования используются методы статического, а не динамического распределения кадров по портам, т.е. закрепление за определенным портом агрегированного канала потока кадров определенного сеанса между двумя узлами. В этом случае все кадры будут проходить через одну и ту же очередь и их последовательность не изменится.

Объединение каналов следует рассматривать как вариант настройки сети, используемый преимущественно для соединений «коммутатор – коммутатор» или «коммутатор – сервер», требующих более высокой скорости передачи, чем может обеспечить одиночная линия связи. Также эту функцию можно применять для повышения надежности важных каналов связи. В случае повреждения линии связи объединенный канал быстро перенастраивается (не более чем за 1 сек.), а риск дублирования и изменения порядка кадров незначителен.

Обычно коммутаторы поддерживают два типа агрегирования каналов связи:

• статическое;

• динамическое.

При статическом агрегировании каналов (установлено по умолчанию), все настройки на коммутаторах выполняются вручную, и они не допускают динамических изменений в агрегированной группе. Его преимуществом яв-ляется отсутствие дополнительных задержек при поднятии агрегированного канала и изменении его настроек. Недостаток – отсутствие согласования настроек с удаленной стороной.

Для организации динамического агрегирования каналов между комму-таторами и другими сетевыми устройствами используется протокол управле-ния агрегированным каналом – Link Aggregation Control Protocol (LACP). Протокол LACP определяет метод управления объединением нескольких физических портов в одну логическую группу и предоставляет сетевым устрой-ствам возможность автосогласования каналов (их добавления или удаления) путем отправки управляющих кадров протокола LACP непосредственно под-ключенным устройствам с поддержкой LACP. Пакеты LACP отправляются устройством через все порты, на которых активизирован протокол. Порты, на которых активизирован протокол LACP, могут быть настроены для работы в одном из двух режимов:

активном (*active*) или **пассивном** (*passive*). Это стандартный протокол, он поддерживается такими коммутаторами, как Cisco, D-Link, HP и др. Т.е. данный протокол можно настроить не только между коммутаторами Cisco, но и Cisco - D-Link, Cisco – HP и т.д.

При работе в активном режиме порты выполняют обработку и рассыл-ку управляющих кадров протокола LACP. При работе в пассивном режиме порты выполняют только обработку управляющих кадров LACP. Для того чтобы динамический канал обладал функцией автосогласования, рекоменду-ется порты, которые входят в агрегированную группу, с одной стороны кана-ла настраивать как активные, а с другой канала – как пассивные.

Следует отметить, что у портов, объединяемых в агрегированный ка-нал, нижеперечисленные характеристики должны обладать одинаковыми настройками:

• тип среды передачи;

• скорость;

• режим работы;

• метод управления потоком (Flow Control) .

Преимущества протокола LACP – согласование настроек с удаленной стороной, что позволяет избежать ошибок в сети. Недостатки - дополнитель-ная задержка при поднятии агрегированного канала или изменении его настроек.

В следующей практической работе рассмотрим пример статического агрегирования коммутаторов.

Контрольные вопросы

1. Для чего применяется агрегирование каналов?

2. Какие требования предъявляются к агрегированным каналам?

3. Какие методы агрегирования каналов вы знаете?

4. Опишите принципы статического агрегирования каналов.

5. Опишите принципы динамического агрегирования каналов.

6. Как происходит распределение нагрузки между каналами при статиче-ском агрегировании?

7. Как происходит распределение нагрузки между каналами при динами-ческом агрегировании?

8. На каком участке сети может применяться агрегирование каналов?

9. Опишите преимущества и недостатки статического агрегирования ка-налов?

10. Опишите преимущества и недостатки

Практическое занятие № 8 - Агрегирование каналов в коммутаторах. Часть 2

25.11.2023 -2 часа

Статическое агрегирование каналов

Цель работы

Изучить статическое агрегирование каналов.

Задание

Создать высокопроизводительную сеть путём статического агрегирования каналов двух коммутаторов и проверить ее работоспособность.

Порядок выполнения работы

1.Открываем Cisco Packet Tracer.

2. Добавляем 2 коммутатора 2960 и два компьютера PC0 и PC1. Затем соединяем их с помощью кабеля. При этом компьютеры присоединяем к портам FastEthernet 0/3 каждого коммутатора (рис. 1). Для агрегирования ка-налов будем использовать порты FastEthernet 0/1 и FastEthernet 0/2 коммута-торов.

3. Перед объединением двух коммутаторов настроим порты FastEther-net 0/1 и FastEthernet 0/2. Для этого переходим во вкладку CLI, заходим в привилегированный режим – **Switch #.** Затем выходим в режим глобального конфигурирования – **Switch(config) #** с помощью сокращенной команды **conf t**. Поскольку интерфейсы будут иметь одинаковые настройки, то мы можем их настроить с помощью одной команды **interface range fa0/1-2.**

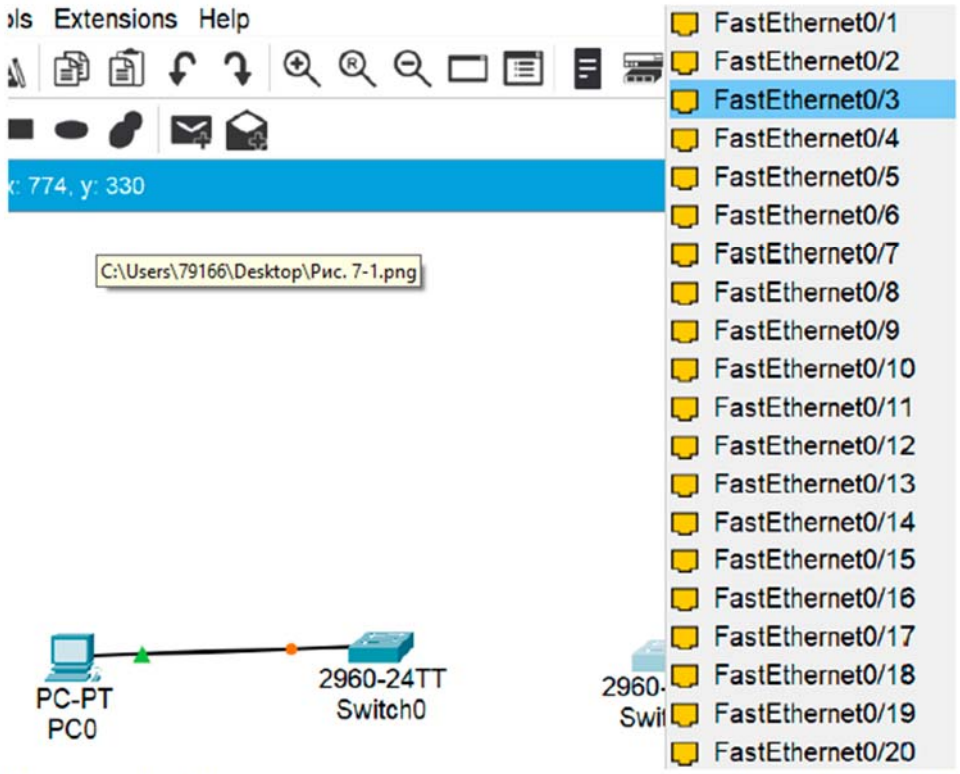


Рисунок 1 – Подключение компьютеров к портам FastEthernet 0/3

Таким образом, настройка коммутаторов во вкладке CLI должны выглядеть следующим образом:

Switch >
Switch >en
Switch #
Switch #conf t
Switch(config)#
Switch(config)#interface range fa0/1-2

Switch(config-if-range)#channel-group 1 mode ? (знак ? показывает все доступные режимы, мы выбираем режим **on**)
Switch(config-if-range)#channel-group 1 mode on
Как видно на рисунке 2, создался логический интерфейс Port-channel 1, кото-рый объединяет 2 физических интерфейса.
Switch(config-if-range)#end – заканчиваем настройку
Switch**# wr mem –** сохраним результаты.

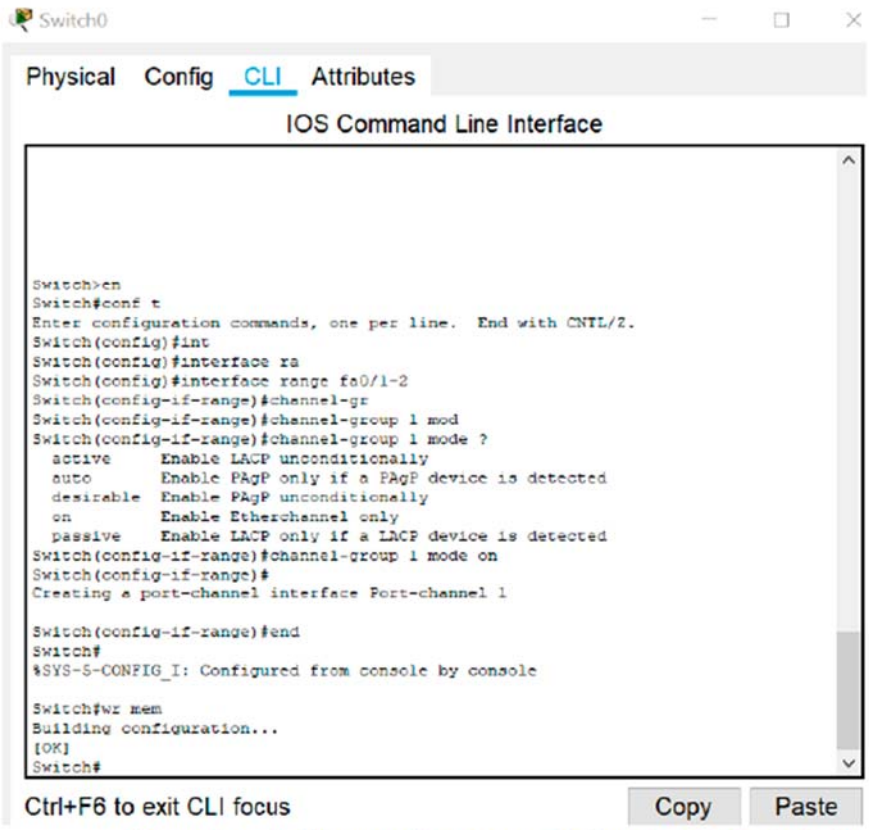


Рисунок 2- Настройка интерфейсов для Switch 0

Произведем аналогичные настройки для второго коммутатора (рис. 3).

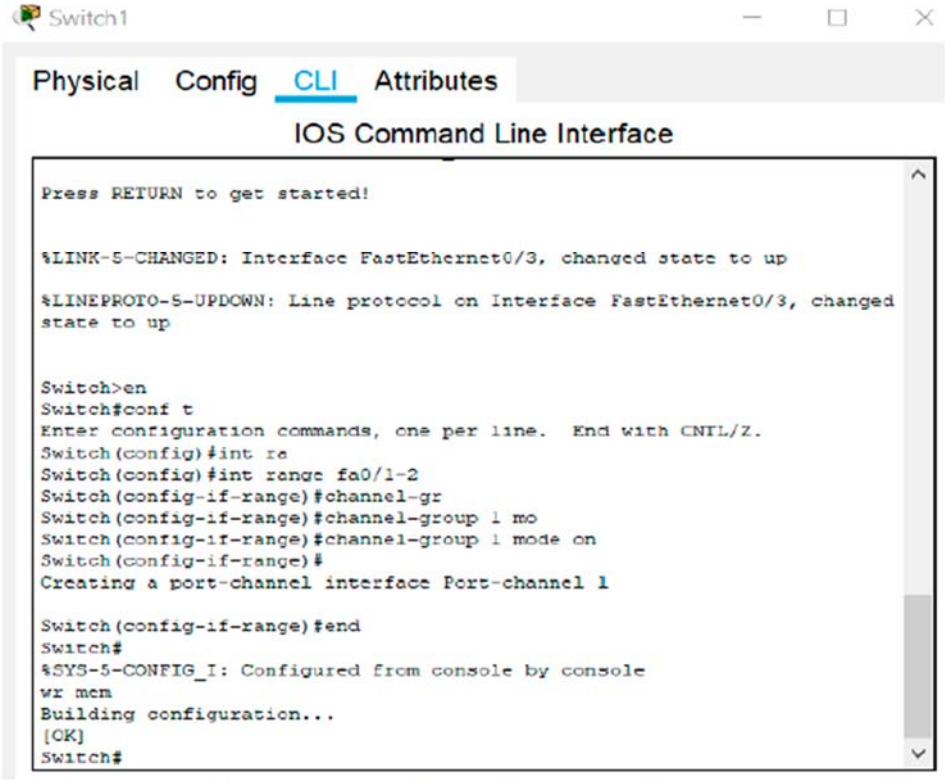


Рисунок 3 – Настройка интерфейсов для Switch 1

4. Соединим два коммутатора с помощью интерфейсов FastEthernet 0/1 и FastEthernet 0/2 и пропишем IP-адреса для каждого компьютера (рис. 4).

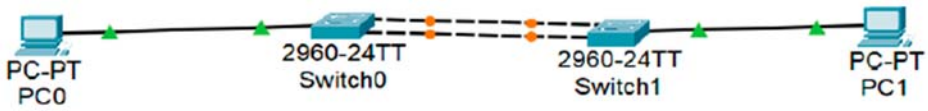


Рисунок 4 - Соединение коммутаторов с помощью интерфейсов FastEthernet 0/1 и FastEthernet 0/2

Для компьютеров PC0 и PC1 задаем следующие IP-адреса (табл. 1).

Таблица 1. IP- адреса для PC0 и PC1

Сетевой элемент	IP-адрес	Маска
PC0	192.168.1.1	255.255.255.0
PC1	192.168.1.2	255.255.255.0

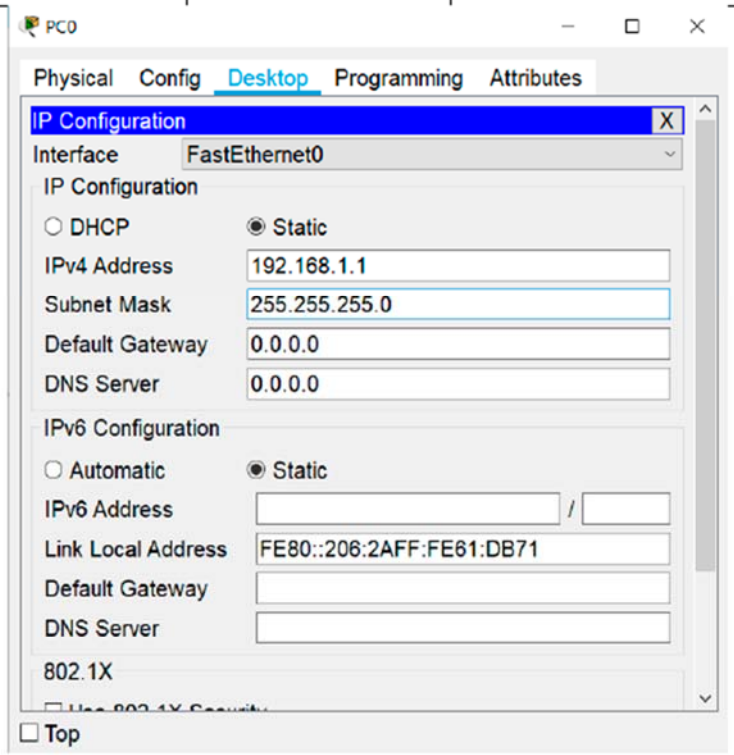


Рисунок 5 – Назначение IP- адреса для PC0

Проверим соединение между коммутаторами с помощью команды ping (рис. 6). Проверка показала, что команда ping прошла успешно. Таким образом, мы получили агрегированный канал между двумя коммутаторами, Но пропускная способность этого канала не 100 Мбит/с, а в 2 раза больше.

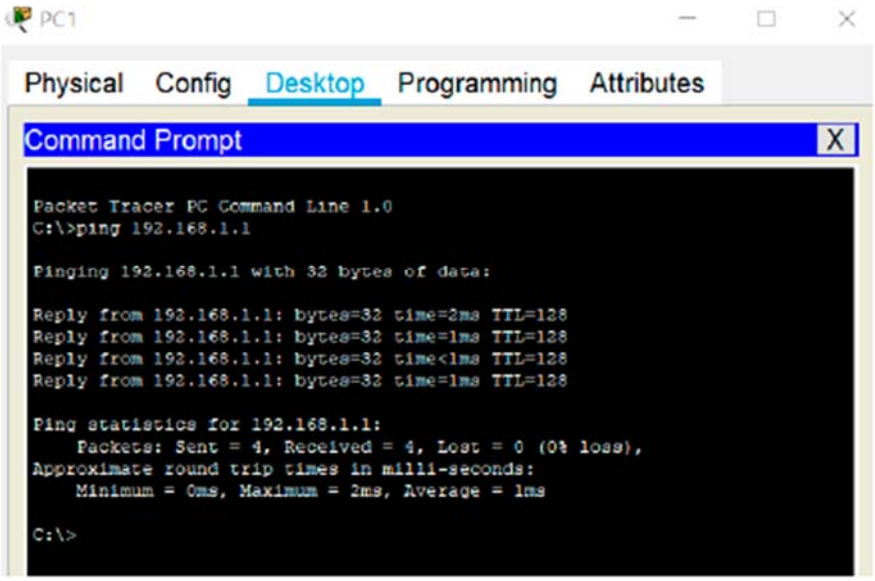


Рисунок 6 - Проверка соединения между коммутаторами

5. Для проверки отказоустойчивости агрегированного звена выведем из строя один из интерфейсов. Пусть это будет FastEthernet 0/2 на Switch 1.

Switch >
Switch >en
Switch #
Switch #conf t
Switch(config)#
Switch(config)#interface fa0/2
Switch(config-if)#shutdown

После этого видно, что второй интерфейс находится в нерабочем состоянии. Проверим связность между коммутаторами с помощью команды ping . Команда выполнена успешно, так второй интерфейс находится в рабочем состоянии (рис. 7).

Рисунок 7 - Интерфейс FastEthernet 0/2 выведен из работы

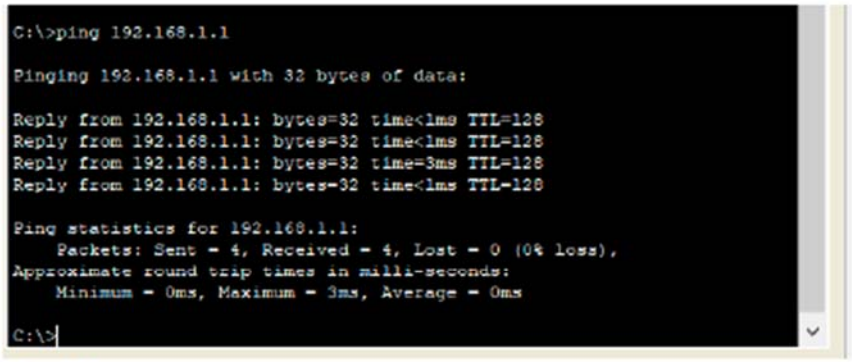


Рисунок 8 - Проверка соединения между коммутаторами после вывода из работы интерфейса FastEthernet 0/2

Содержание отчета

В индивидуальном отчёте должны быть указаны цель, задание, представлены необходимые снимки экрана и пояснения к ним. Следует проанализировать полученные данные и дать ответы на контрольные вопросы.

Контрольные вопросы

1. Как может осуществляться передача пакетов одной сессии, если они будут передаваться по разным портам агрегированного канала? Приведите примеры.
2. Что произойдет, если в агрегированном канале, один выйдет из строя?
3. Чем отличается статическое агрегирование каналов связи от динамического агрегирования?
4. Что нужно сделать для проверки отказоустойчивости агрегированного звена?
5. Какой вид агрегирования каналов установлен в коммутаторе по умолчанию?
6. Опишите функции логического интерфейса Port-channel 1?
7. Для каких целей применяется агрегация каналов?
8. Как распределяется трафик по каналам при объединении портов?
9. Какие характеристики должны быть у портов, агрегированных в канал?
10. Почему в большинстве реализаций механизмов агрегирования используются методы статического, а не динамического распределения кадров по портам?
11. Как называется технология, которая позволяет обеспечить резервирование в случае выхода из строя одного из каналов?
12. Что представляет собой технология агрегирования каналов?

Лабораторная работа №8. Динамическое агрегирование каналов. Часть 3

Цель работы

Рассмотреть сеть, построенную по топологии «Звезда», когда коммутаторы 2-го уровня подключаются к коммутатору 3-го уровня. Изучить динамическое агрегирование каналов.

Задание

Создать высокопроизводительную сеть путём динамического агреги-рования каналов коммутаторов и проверить ее работоспособность.

Порядок выполнения работы

1.Открываем Cisco Packet Tracer.

2. Добавляем 3 коммутатора 2960 и один коммутатор 3-го уровня - 3560. Для соединения каждого коммутатора 2960 с коммутатором 3560 перейдем в

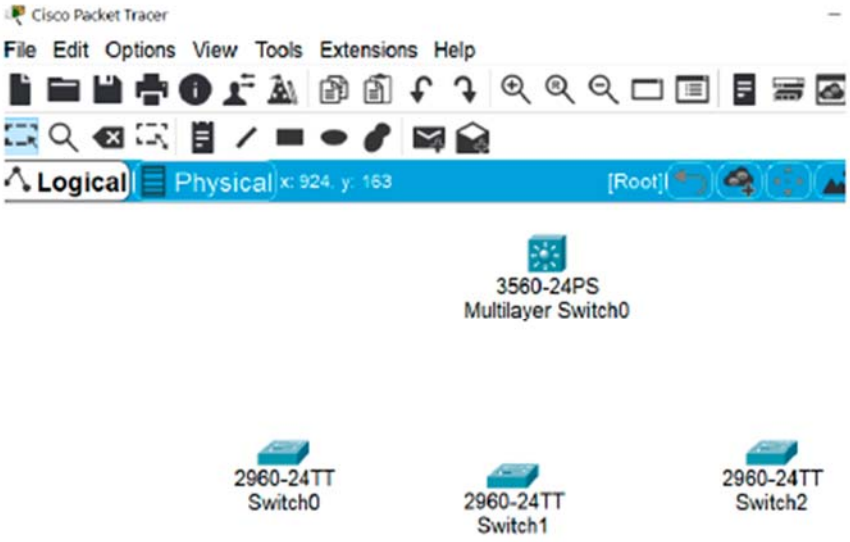


Рисунок 1 – Коммутаторы 2 и 3 уровня

3. Настроим порты FastEthernet на коммутаторе 3560. Для этого переходим во вкладку CLI, заходим в привилегированный режим – **Switch #**. Затем выходим в режим глобального конфигурирования – **Switch(config) #** с помощью сокращенной команды **conf t**. Поскольку интерфейсы будут иметь одинаковые настройки, то мы можем их настроить с помощью одной команды **interface range fa0/1-2.**

Таким образом, настройка коммутаторов во вкладке CLI должны выглядеть следующим образом:

настройки коммутатора 3-го уровня (рис. 1).

Switch >

Switch >en

Switch #

Switch #conf t

Switch(config)#

Switch(config)#interface range fa0/1-2

Switch(config-if-range)#channel-protocol ? (знак ? показывает все доступные протоколы, мы выбираем протокол LACP)

Switch(config-if-range)#channel- protocol lacp

Далее присваиваем ему channel-group 1

Switch(config-if-range)#channel-group 1 mode active

Switch(config-if-range)#exit

Как видно на рисунке 2, создался логический интерфейс channel-group 1, который объединяет 2 физических интерфейса FastEthernet 0/1-2.

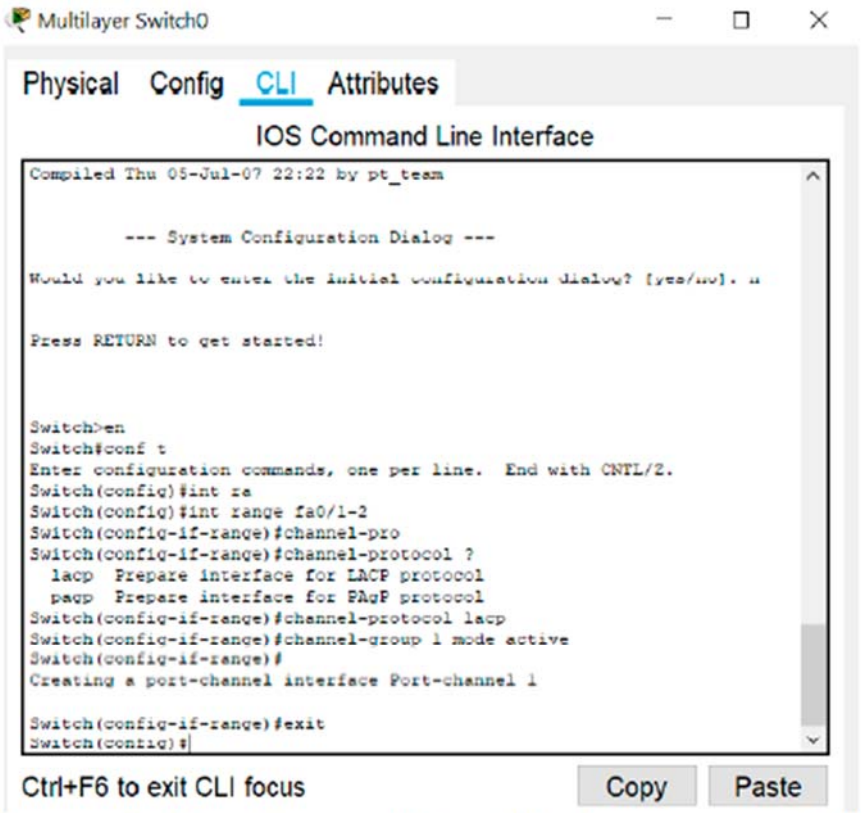


Рисунок 2 - Настройка интерфейсов fa0/1-2 на коммутаторе 3560

Далее аналогичным образом настраиваем интерфейсы FastEthernet 0/3-4 и FastEthernet 0/5-6 и создаем channel-group 2 и channel-group 3.

Switch(config)#interface range fa0/3-4
Switch(config-if-range)#channel-protocol ?
Switch(config-if-range)#channel- protocol lacp
Switch(config-if-range)#channel-group 2 mode active
Switch(config-if-range)#exit

Switch(config)#interface range fa0/5-6
Switch(config-if-range)#channel-protocol ?
Switch(config-if-range)#channel- protocol lacp
Switch(config-if-range)#channel-group 3 mode active

Далее заканчиваем настройки и сохраняем их.

Switch(config-if-range)#end
Switch# wr mem

Результаты настройки интерфейсов fa0/3-4 и fa0/5-6 показаны на рисунке 3.

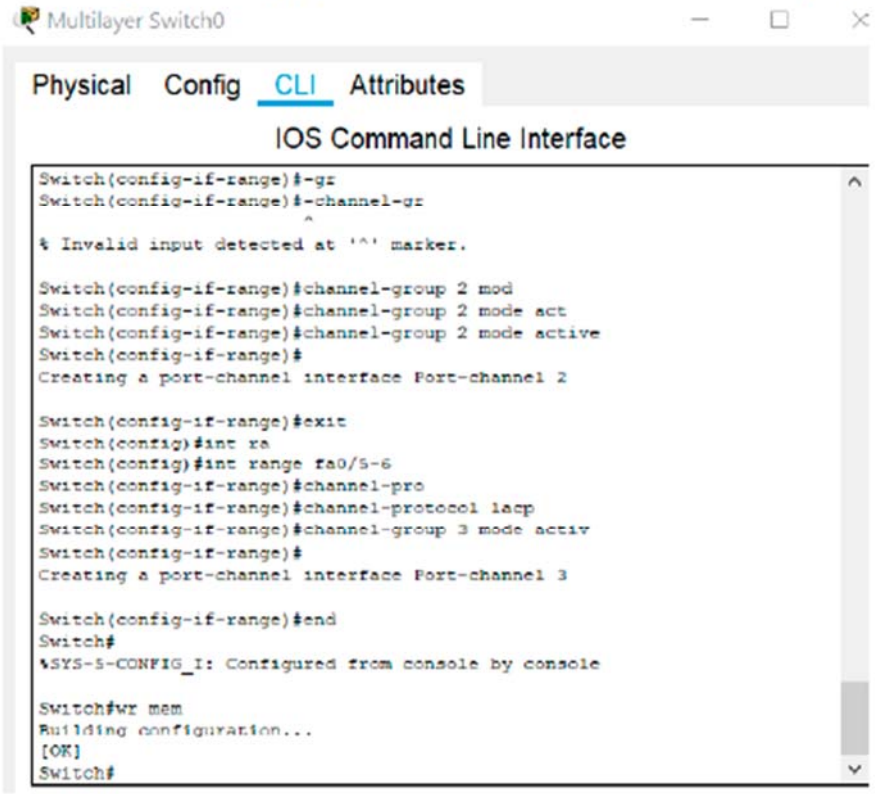


Рисунок 3 - Настройка интерфейсов fa0/3-4 и fa0/5-6 на коммутаторе 3560

4.Теперь произведем настройки для коммутаторов 2960. Настройку проводим для портов fastEthernet 0/1-2, при настройке channel-group выбираем режим passive, так как рекомендуется использовать параметр active только с одной стороны. Но поскольку мы его уже использовали на центральном коммутаторе, то здесь настраиваем passive (рис. 4).

Switch >en
Switch #
Switch #conf t
Switch(config)#
Switch(config)#interface range fastEthernet 0/1-2
Switch(config-if-range)#channel- protocol lacp
Switch(config-if-range)#channel-group 1 mode passive
Switch(config-if-range)#end
Switch# wr mem

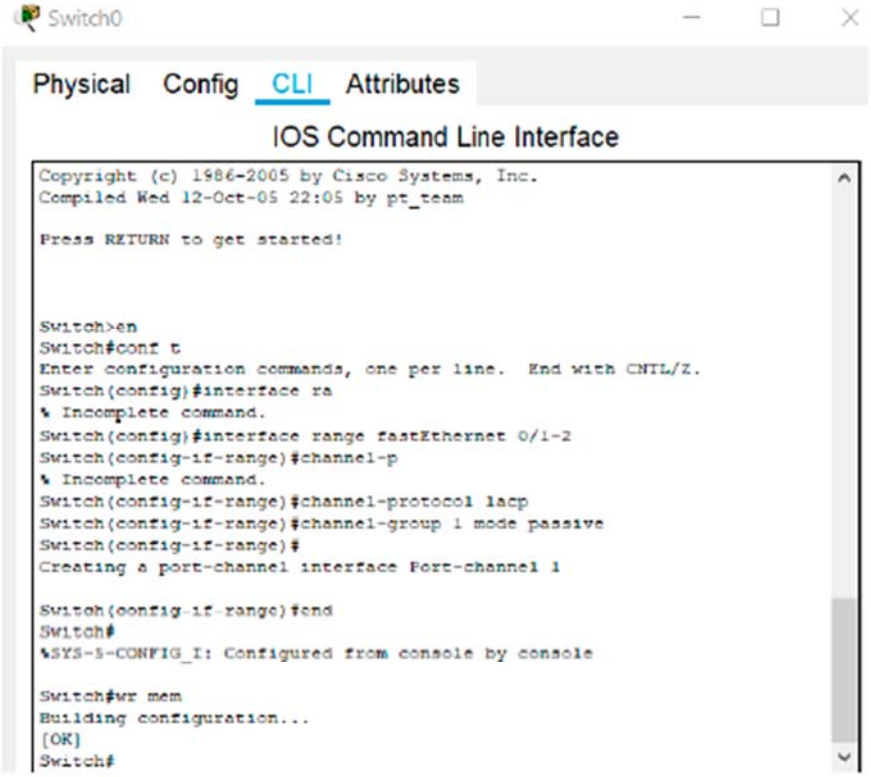


Рисунок 4 - Настройка интерфейсов fa0/1-2 на коммутаторе 2960

Аналогичные действия производим на остальных двух коммутаторах.

5. Далее соединим коммутаторы. Поскольку это устройства разного уровня, то соединяем их прямым кабелем. Соединения производим в соот-

ветствии с теми настройками, которые мы прописали на каждом коммутаторе (табл. 1).

Таблица 1. Настройка интерфейсов на коммутаторах

Коммутатор	Интерфейсы на коммутаторах 2960	Интерфейсы на коммутаторе 3560
Switch 0	FastEthernet 0/1 FastEthernet 0/2	FastEthernet 0/1 FastEthernet 0/2
Switch 1	FastEthernet 0/1 FastEthernet 0/2	FastEthernet 0/3 FastEthernet 0/4
Switch 2	FastEthernet 0/1 FastEthernet 0/2	FastEthernet 0/5 FastEthernet 0/6

Все интерфейсы загорелись зеленым цветом, что показывает, что сеть функционирует. Далее на центральном коммутаторе введем команду:

Switch# show eth

Увидим все группы портов, которые мы объединили по протоколу LACP (рис. 5).

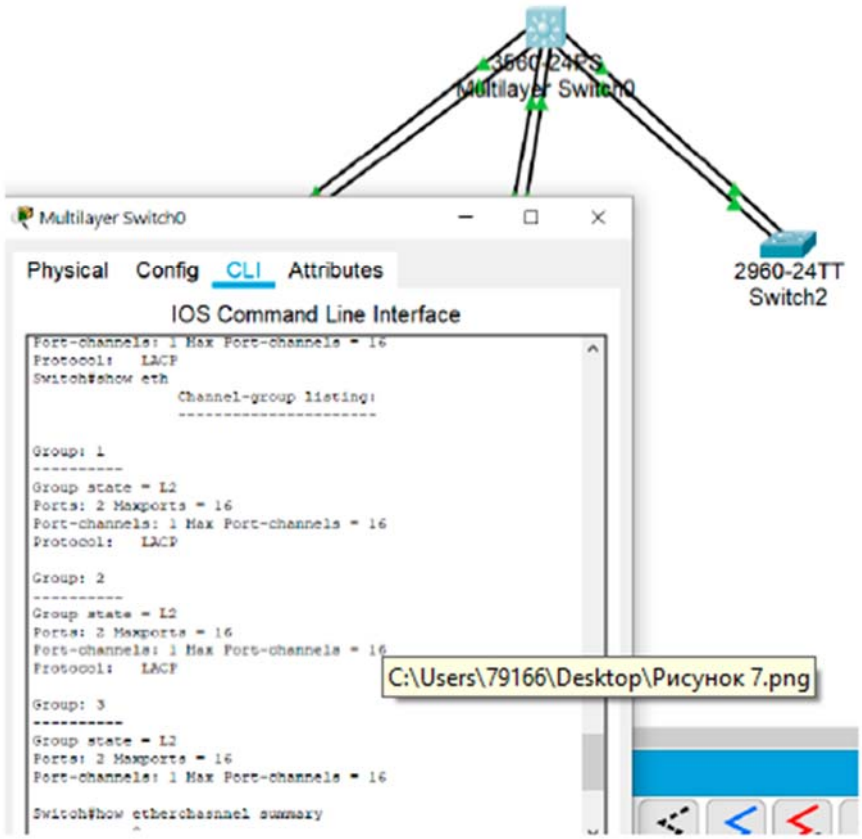


Рисунок 5 - Проверка настроенных портов в коммутаторе 3560

Контрольные вопросы

1.В чем отличие работы портов коммутатора в пассивном и активных режимах?

2.Какие характеристики портов, объединённых в агрегированные кана-лы, должны быть одинаковые?

3.Какой режим работы нужно в данной практической работе нужно выбрать для коммутатора Cisco 2960 и почему?

4. Как можно проверить отказоустойчивость интерфейса FastEthernet 0/1 на коммутаторе 2-го уровня?
5. Какие режимы работы возможны при настройке канала-группы?
6. Зачем портам присваивается активный или пассивный режимы?
7. Опишите преимущества протокола LACP.
8. Коммутаторы, каких уровней модели OSI используются в данной ра-боте? В чем их отличие?
9. Какими командами выводятся из строя, и вводится в строй интер-фейсы коммутатора?
10. На каких участках сети применяется технология агрегирования ка-налов и почему?
11. С помощью, какой команды можно посмотреть группы портов коммутатора?

Практическое задание №9. Использование коммутаторов 2-го и 3-го уровней для построения компьютерных сетей. Часть 1

25.11.2023 -1 час

Цель работы

Изучить принципы построения сетей на коммутаторах 2-го и 3-го уровней.

Задание

1.Ознакомиться с иерархической моделью компьютерной сети;
2. Ознакомиться с характеристиками коммутаторов;
3.Ответить на вопросы.

Иерархическая модель определяет подход к проектированию сетей и включает в себя три логических уровня (рис. 1):

• уровень доступа (*access layer*);
• уровень распределения/агрегации (*distribution layer*);
• уровень ядра (*core layer*).

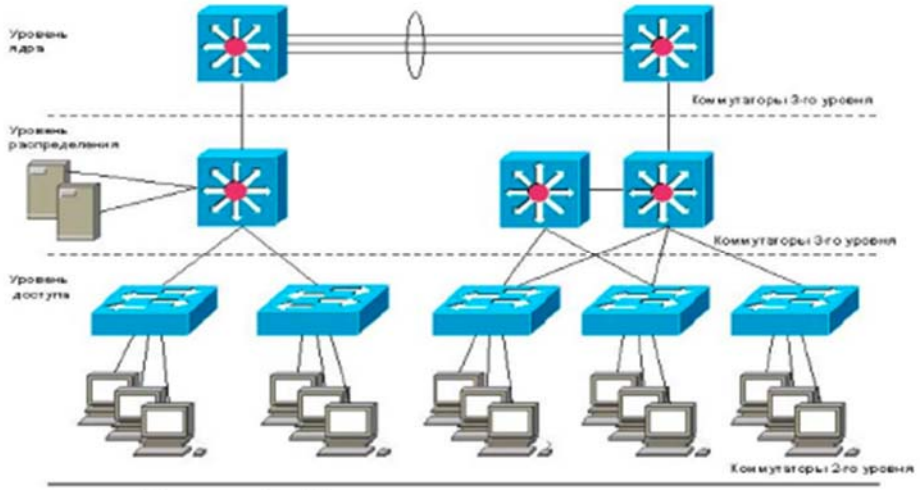


Рисунок 1 - Иерархическая модель компьютерной сети

Уровень ядра находится на самом верху иерархии и отвечает за надежную и быструю передачу больших объемов данных. Трафик, передаваемый через ядро, является общим для большинства пользователей. Сами пользовательские данные обрабатываются на уровне распределения, который, при необходимости, пересылает запросы к ядру.

Уровень распределения (агрегации) является связующим звеном между уровнями доступа и ядра. Он выполняет функции маршрутизации, обеспечения качества обслуживания, безопасности сети, агрегирование каналов, переход от одной технологии к другой (например, от FE к GE).

Уровень доступа управляет доступом пользователей (компьютеры, серверы, видеокамеры, IP-телефоны и т.д.) к ресурсам сети. Эти коммутаторы производят сегментирование сети с помощью известной нам технологии VLAN. Коммутаторы уровня доступа могут соединяться между собой только через коммутаторы уровня распределения.

Коммутаторы можно классифицировать в соответствии с уровнями модели OSI, на которых они передают, фильтруют и коммутируют кадры. Различают *коммутаторы уровня 2 (Layer 2 switch)* и *коммутаторы уровня 3 (Layer 3 switch)*.

Коммутаторы уровня 2 (L2- коммутаторы) анализируют входящие кадры, принимают решения об их дальнейшей передаче на основе MAC-адресов. Они не осуществляет анализ информации протоколов верхних уровней модели OSI. Эти коммутаторы обычно применяются на уровне доступа сети.

Коммутаторы 2-го уровня на схемах обозначаются  . Коммутацию трафика они производят на основе MAC- адресов. Они коммутируют трафик между портами и между VLAN. Соединение коммутаторов 2-го уровня между собой возможно только через коммутаторы 3-го уровня.

Коммутаторы уровня 3 (L3 - коммутаторы) осуществляют обработку трафика на основе адресов канального уровня и сетевого уровня модели OSI. Коммутаторы 3-го уровня применяются на уровнях ядра и распределения.

На схемах они обозначаются следующим образом  .

Коммутаторы второго уровня подключаются к коммутатору третьего уровня с помощью топологии «Звезда». Такая схема может применяться, например, в многоэтажном здании, где на каждом этаже стоят коммутаторы 2-го уровня, которые по агрегированным каналам соединяется далее с коммутаторами 3-го уровня.

Коммутаторы 3-го уровня поддерживают IP- маршрутизацию, т.е. могут работать с сетевыми устройствами по IP-адресам. Они не только могут разбить сеть на VLAN, но и маршрутизировать трафик между различными сегментами сети. Данные коммутаторы чаще всего используются, как коммутаторы уровня распределения и предназначены для объединения коммутаторов уровня доступа. Он применяется в локальных сетях.

Если не использовать на схеме, изображенной на рисунке 1 коммутаторы уровня распределения, то для соединения коммутаторов 2-го уровня между собой по схеме «каждый с каждым» необходимо организовать гораздо больше соединений, чем при использовании коммутаторов 3-го уровня. Коммутаторы 3 уровня можно отнести уже к разряду маршрутизаторов, но они могут использоваться для маршрутизации трафика только внутри сети. Например, такой коммутатор нельзя использовать для маршрутизации трафика в сеть Интернет. Таким образом, коммутатор 3-го уровня не может заменить маршрутизатор, который ставится на границе сети (рис. 2). У маршрутизатора есть ряд дополнительных функций, например функции межсетевого экрана, NAT (преобразование сетевых адресов), организация VPN т.д. Коммутатор третьего уровня гораздо дешевле маршрутизатора, но он превосходит по производительность маршрутизатора в десятки раз.

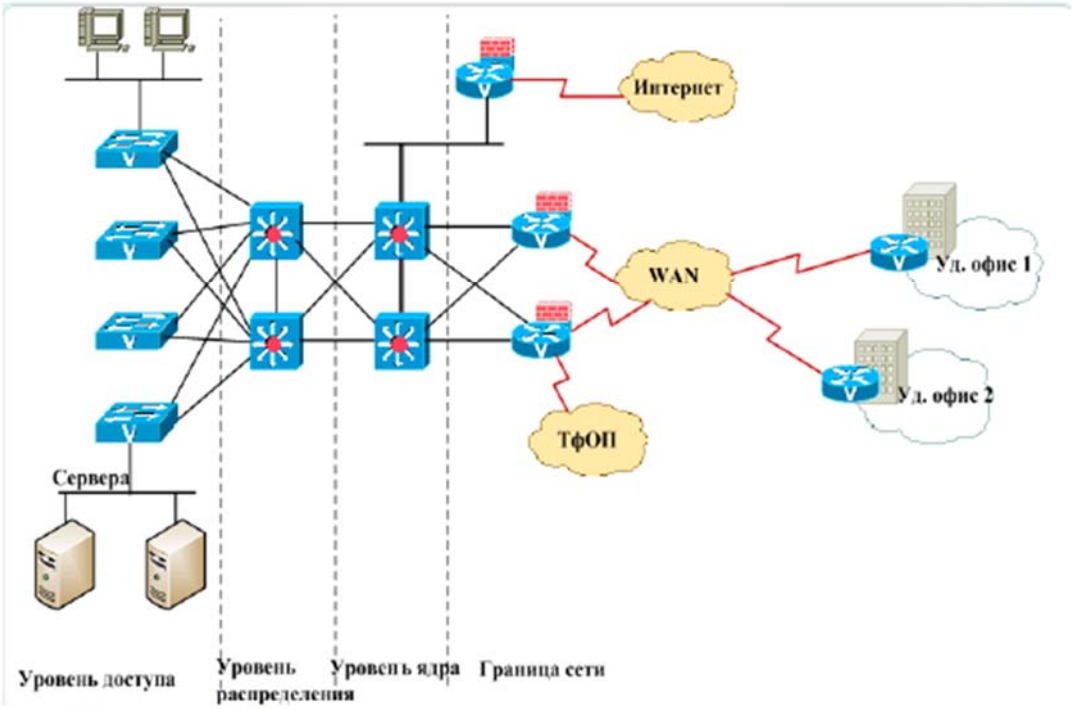


Рисунок 2 - Пример типичной структуры предприятия

Характеристики, влияющие на производительность коммутаторов

Производительность коммутатора. Основными показателями коммутатора, характеризующими его производительность, являются:

- скорость фильтрации кадров;
- скорость продвижения кадров;
- пропускная способность;
- задержка передачи кадра.
- размер буфера (буферов) кадров;
- производительность коммутирующей матрицы;
- производительность процессора или процессоров;
- размер таблицы коммутации;

Скорость фильтрации (filtering) определяет скорость, с которой коммутатор выполняет следующие этапы обработки кадров:

- прием кадра в свой буфер;
- отбрасывание кадра, в случае обнаружения в нем ошибки;
- отбрасывание кадра в соответствии с настроенными на порте фильтрами;

Скорость продвижения (forwarding) определяет скорость, с которой коммутатор выполняет следующие этапы обработки кадров:

- прием кадра в свой буфер;
- просмотр таблицы коммутации с целью нахождения порта назначения на основе MAC-адреса получателя кадра;
- передача кадра в сеть через найденный по таблице коммутации порт назначения.

Обе эти характеристики измеряются обычно *в кадрах в секунду*.

Пропускная способность коммутатора измеряется количеством пользовательских данных (обычно в мегабитах или гигабитах в секунду), переданных в единицу времени через его порты.

Задержка передачи кадра (forward delay) измеряется как время, прошедшее с момента прихода первого байта кадра на входной порт коммутатора до момента появления этого байта на его выходном порту. Задержка складывается из времени, затрачиваемого на буферизацию кадра, а также времени, затрачиваемого на обработку кадра коммутатором, а именно на просмотр таблицы коммутации, принятие решения о продвижении и получение доступа к среде выходного порта.

Для обеспечения временного хранения кадров в тех случаях, когда их невозможно немедленно передать на выходной порт, коммутаторы, в зависимости от реализованной архитектуры, оснащаются буферами на входных, выходных портах или общим буфером для всех портов. Размер буфера влияет как на задержку передачи кадра, так и на скорость потери пакетов. Поэтому чем больше объем буферной памяти, тем менее вероятны потери кадров.

Контрольные вопросы

1. Назовите функции коммутаторов 2-го уровня
2. Назовите функции коммутатора 3-го уровня
3. Какие характеристики влияют на производительность коммутатора?
4. Какие функции выполняет уровень ядра в иерархической модели сети?
5. Опишите функции уровня распределения?
6. Как определяется задержка передачи кадра коммутатора?
7. Что определяет скорость фильтрации кадров?
8. На каком уровне иерархической модели сети применяются коммутаторы 2-го уровня?
9. На каких уровнях иерархической модели сети применяются коммутаторы 3-го уровня?
10. Как измеряется задержка передачи кадра коммутатором?

Практическое задание №9. Использование коммутаторов 2-го и 3-го уровней

для построения компьютерных сетей. Часть 2

Изучить принципы работы коммутатора третьего уровня

Задание

Построить сеть, состоящую из коммутатора 3-го уровня и трех компьютеров и установить соединения между коммутаторами. Сравнить принципы работы коммутаторов 2-го и 3-го уровней.

Порядок выполнения работы

1.Открываем Cisco Packet Tracer.

2. Создать сеть, изображенную на рисунке 1. Мы хотим разбить эту сеть на 3 сегмента, чтобы наши коммутаторы могли связываться между собой.

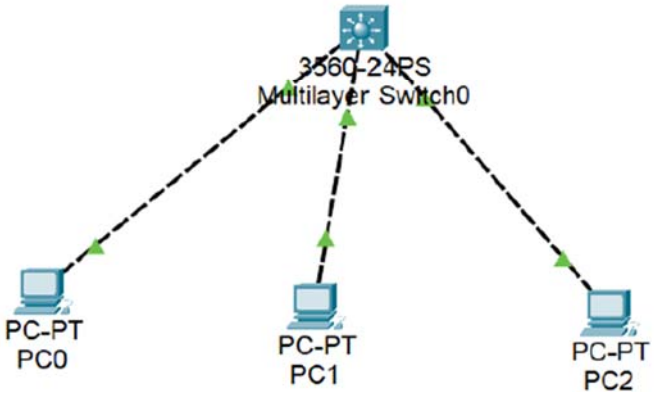


Рисунок 1- Сеть для изучения коммутаторов 3-го уровня

3.Переходим в настройки коммутатора в 3560, в CLI (рис. 2). Мы хотим разбить сеть на три VLAN (VLAN2, VLAN3, VLAN4). Для этого набираем следующие команды:

Switch >en
Switch #
Switch #conf t
Switch(config)#vlan 2
Switch(config- vlan)#name VLAN2
Switch(config-if- vlan)#exit

Switch(config)#vlan 3
Switch(config- vlan)#name VLAN3

Switch(config-if- vlan)#exit

Switch(config)#vlan 4
Switch(config- vlan)#name VLAN4
Switch(config-if- vlan)#end

```
Switch>
Switch>
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 2
Switch(config-vlan)#name VLAN2
Switch(config-vlan)#exit
Switch(config)#vlan 3
Switch(config-vlan)#name VLAN3
Switch(config-vlan)#exit
Switch(config)#vlan 4
Switch(config-vlan)#name VLAN 4
                           ^
% Invalid input detected at '^' marker.

Switch(config-vlan)#name VLAN4
Switch(config-vlan)#
Switch(config-vlan)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

Рисунок 2 - Настройка коммутатора 3560

4. Теперь определим порты, в которые подключаются пользователи, к определенному VLAN. Сначала подведем курсор к коммутатору и посмотрим состояние портов (рис. 3).

Port	Link	VLAN	IP Address	IPv6 Address
FastEthernet0/1	Up	1	<not set>	<not set>
FastEthernet0/2	Up	1	<not set>	<not set>
FastEthernet0/3	Up	1	<not set>	<not set>
FastEthernet0/4	Down	1	<not set>	<not set>
FastEthernet0/5	Down	1	<not set>	<not set>
FastEthernet0/6	Down	1	<not set>	<not set>
FastEthernet0/7	Down	1	<not set>	<not set>
FastEthernet0/8	Down	1	<not set>	<not set>
FastEthernet0/9	Down	1	<not set>	<not set>
FastEthernet0/10	Down	1	<not set>	<not set>
FastEthernet0/11	Down	1	<not set>	<not set>
FastEthernet0/12	Down	1	<not set>	<not set>
FastEthernet0/13	Down	1	<not set>	<not set>
FastEthernet0/14	Down	1	<not set>	<not set>
FastEthernet0/15	Down	1	<not set>	<not set>
FastEthernet0/16	Down	1	<not set>	<not set>
FastEthernet0/17	Down	1	<not set>	<not set>
FastEthernet0/18	Down	1	<not set>	<not set>
FastEthernet0/19	Down	1	<not set>	<not set>
FastEthernet0/20	Down	1	<not set>	<not set>
FastEthernet0/21	Down	1	<not set>	<not set>
FastEthernet0/22	Down	1	<not set>	<not set>
FastEthernet0/23	Down	1	<not set>	<not set>
FastEthernet0/24	Down	1	<not set>	<not set>
GigabitEthernet0/1	Down	1	<not set>	<not set>

Рисунок 3 - Состояние портов коммутатора

Пропишем порт FastEthernet 0/1 в VLAN2, порт FastEthernet 0/2 в VLAN3, порт FastEthernet 0/3 в VLAN4. Для этого произведем конфигурацию на коммутаторе (рис. 4). Заходим в его настройки и набираем команды:

Switch >en
Switch #
Switch #conf t
Switch(config)#
Switch(config)#interface fastEthernet0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config-if-range)#exit

Тоже самое указываем для других интерфейсов.

Switch(config)#interface fastEthernet0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 3
Switch(config-if-range)#exit

Switch(config)#interface fastEthernet0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 4
Switch(config-if-range)#end

```
Switch#
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int fa0/1
Switch(config-if)#swi
Switch(config-if)#switchport mode ac
Switch(config-if)#switchport mode access
Switch(config-if)#sw
Switch(config-if)#switchport access vl
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
Switch(config)#int fa0/2
Switch(config-if)#sw
Switch(config-if)#switchport mode access
Switch(config-if)#sw
Switch(config-if)#switchport access vlan 3
Switch(config-if)#exit
Switch(config)#int fa0/3
Switch(config-if)#sw
Switch(config-if)#switchport mode access
Switch(config-if)#sw
Switch(config-if)#switchport access vlan 4
Switch(config-if)#end
Switch#
```

Рисунок 4 - Конфигурация на коммутаторе

Смотрим состояние портов с помощью команды (рис. 5):

Switch# show run

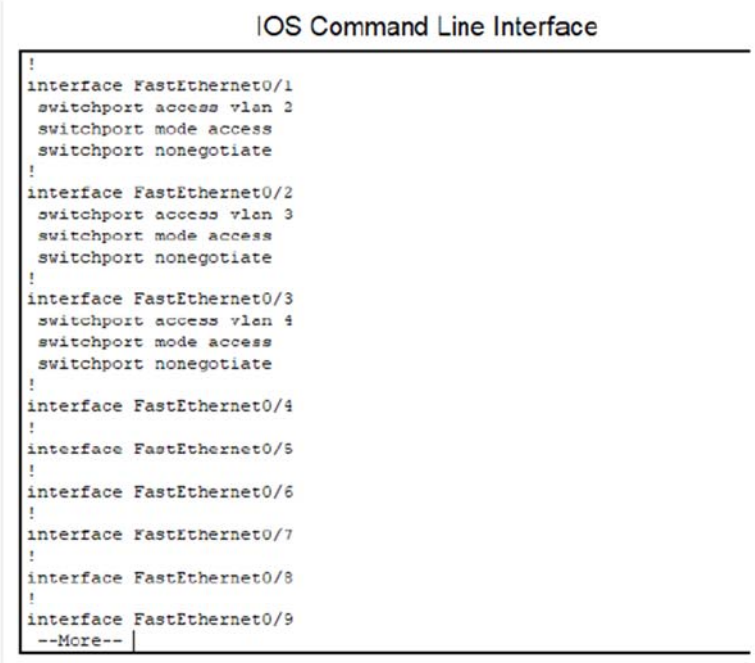


Рисунок 5 - Состояние портов коммутатора после настройки

Поскольку это коммутатор 3-го уровня, то необходимо настроить IP-адреса на созданных сегментах. Для этого в режиме глобального конфигурирования заходим в интерфейс vlan 2, vlan 3, vlan 4 и присваиваем им IP-адреса.

Switch #
Switch #conf t
Switch(config)#int vlan 2
Switch(config-if)#ip address 192.168.2.1 255.255.255.0
Switch(config-if)#exit

Switch(config)#int vlan 3
Switch(config-if)#ip address 192.168.3.1 255.255.255.0
Switch(config-if)#exit

Switch(config)#int vlan 4
Switch(config-if)#ip address 192.168.4.1 255.255.255.0
Switch(config-if)#end

С помощью команды **Switch# show run** можно увидеть IP-адреса, присвоенные виртуальным интерфейсам (рис. 6).

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int vlan 2
Switch(config-if)#ip address 192.168.2.1 255.255.255.0
Switch(config-if)#exit
Switch(config)#int vlan 3
Switch(config-if)#ip adress 192.168.3.1 255.255.255.0
                   ^
% Invalid input detected at '^' marker.

Switch(config-if)#ip address 192.168.3.1 255.255.255.0
Switch(config-if)#exit
Switch(config)#int vlan 4
Switch(config-if)#ip address 192.168.4.1 255.255.255.0
Switch(config-if)#
Switch(config-if)#end
Switch#show run
Building configuration...

Current configuration : 1610 bytes
!
version 12.2(37)SE1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
```

Рисунок 6 - Присвоение IP-адресов виртуальным интерфейсам

```
interface Vlan1
 no ip address
 shutdown
!
interface Vlan2
 mac-address 00e0.b0b4.e401
 ip address 192.168.2.1 255.255.255.0
!
interface Vlan3
 mac-address 00e0.b0b4.e402
 ip address 192.168.3.1 255.255.255.0
!
interface Vlan4
 mac-address 00e0.b0b4.e403
 ip address 192.168.4.1 255.255.255.0
!
ip classless
!
ip flow-export version 9
!
!
!
!
!
 --More-- |
```

Рисунок 7 - Проверка настройки интерфейсов

Зададим следующие IP-адреса компьютерам (табл.1).

Талица 1. IP- адреса для компьютеров

Сетевой элемент	IP-адрес	Маска	Шлюз
PC0	192.168.2.2	255.255.255.0	192.168.2.1
PC1	192.168.3.2	255.255.255.0	192.168.3.1
PC2	192.168.4.2	255.255.255.0	192.168.4.1

И проверим связь между PC0 и коммутатором. Соединение проходит.

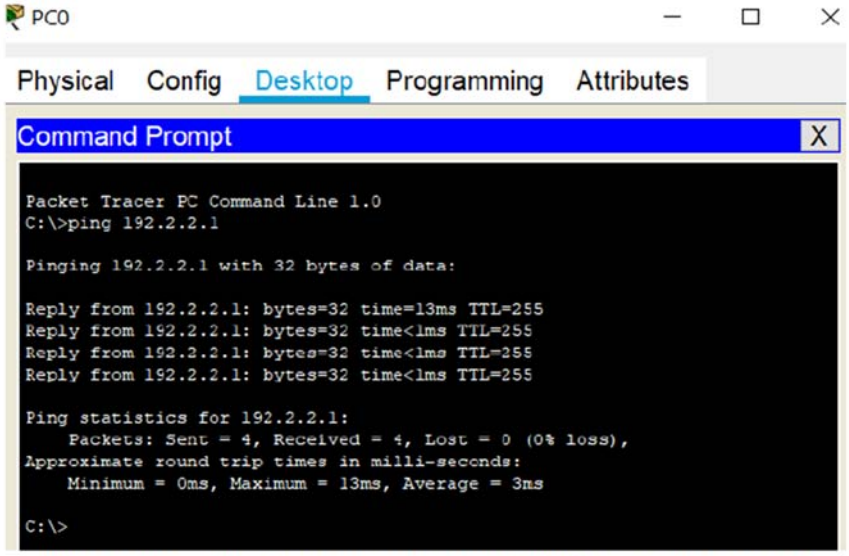


Рисунок 8 - Проверка связи между PC0 и коммутатором

Аналогично проверьте связи между коммутатором и PC1 и PC2. Связи нет. Для того, чтобы связь прошла необходимо на коммутаторе добавить следующие настройки.

Switch #

Switch #conf t

Switch(config)#ip routing

Switch(config)#end

Теперь проверим связь между коммутаторами, например, между PC1 и PC0. Проверим это с помощью команды ping. Связь проходит (рис. 9). Проверьте связь между остальными компьютерами.

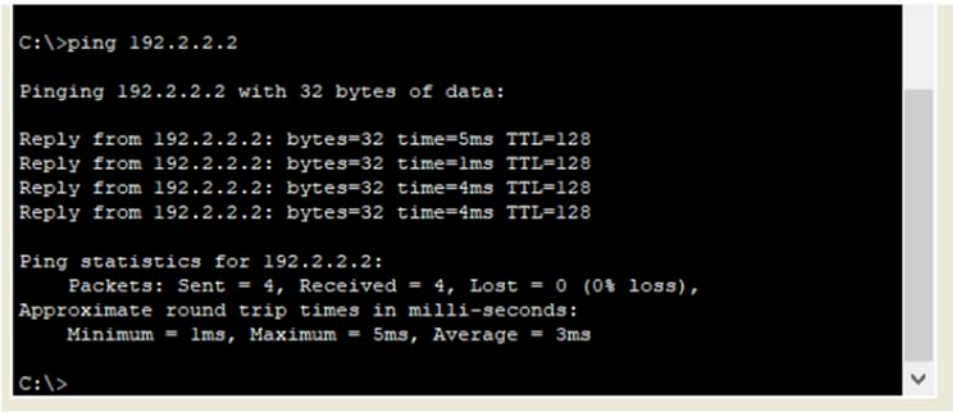


Рисунок 9 - Связь между PC1 и PC0

Контрольные вопросы

1. Опишите последовательность разбиения сети на три VLAN.
2. Почему коммутаторы третьего уровня и персональные компьютеры связаны между собой перекрестным кабелем?
3. Как прописать порт порт FastEthernet 0/1 в VLAN?
4. Как произвести настройку IP- адресов на коммутаторе 3-го уровня?
5. С помощью какой команды можно посмотреть присвоенные IP-адреса?
6. Назовите основные показатели, которые определяют производительность коммутатора.
7. Как определяется пропускная способность коммутатора?
8. Как связаны между собой коммутаторы уровня доступа в иерархической модели компьютерной сети?
9. Опишите функции коммутаторов доступа в иерархической модели компьютерной сети?
10. Назовите функции коммутаторов уровня ядра сети.

Практическое задание №10. Назначение службы DNS и протокола DHCP. Часть 1

Изучить назначение службы DNS и протокола DHCP

Задание

1.Ознакомиться с пространством доменных имен;

2. Ознакомиться с принципами работы протокола DHCP;

3.Ответить на вопросы.

Назначение службы DNS

Для человека символические имена более удобны, чем числовые адре-са. В сети Интернет используется система доменных имен, организованная следующим образом. Имеются корневые **домены**. Домен – определенная зо-на в системе доменных имен (DNS) Интернета, выделенная какой-либо стране, организации. Например, домен **ru** относится к сетям России, корне-вой домен **de** относится к сетям Германии и т.д. Есть специальные корневые домены: домен **com** (Cisco.com) зарезервирован для коммерческих компаний, домен **org** зарезервирован за некоммерческими организациями.

В стеке TCP/IP применяется доменная система имен, которая имеет иерархическую древовидную структуру, допускающая в имени наличие произвольного количества составных частей (рис. 1). Дерево имен начинается с корня, обозначаемое точкой. Затем следует старшая символьная часть имени, вторая по старшинству символьная часть имени и т.д. Младшая часть имени соответствует

конечному узлу сети.

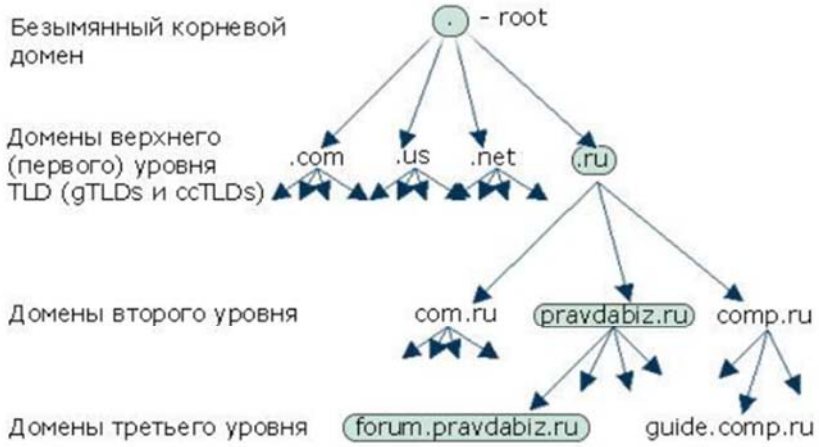


Рисунок 1 -Пространство доменных имен

Составные части доменного имени отделяются друг от друга точкой (рис. 2). Все приложения в сети Интернет используют протокол IP. Поэтому для обмена данными с поставщиком услуг Интернет надо знать IP-адрес сервера поставщика услуг. Если пользователь задает некоторое доменное имя, то его компьютер обращается к специальному серверу в сети Интернет, называемому сервером DNS. У такого сервера имеется база данных о доменных именах, и доменное имя конвертируется в IP-адрес. Запрос и ответ передается через IP-сеть в соответствии со специальным протоколом, также называемым DNS.

Рисунок 2 - Пример доменного имени

Если вы используете доменные имена, то ваш компьютер должен располагать адресом ближайшего DNS-сервера. Конечно, каждыйDNS-сервер не может располагать информацией обо всех доменных именах в мире. Предположим, ваш ближайший DNS-сервер не располагает такой информацией, тогда запрос будет передан следующему DNS-серверу и т.д.

Если ваш ближайший DNS-сервер получает ответ от удаленного DNS-сервера, он запоминает эту информацию, и в дальнейшем поиск IP-адреса происходит быстрее.

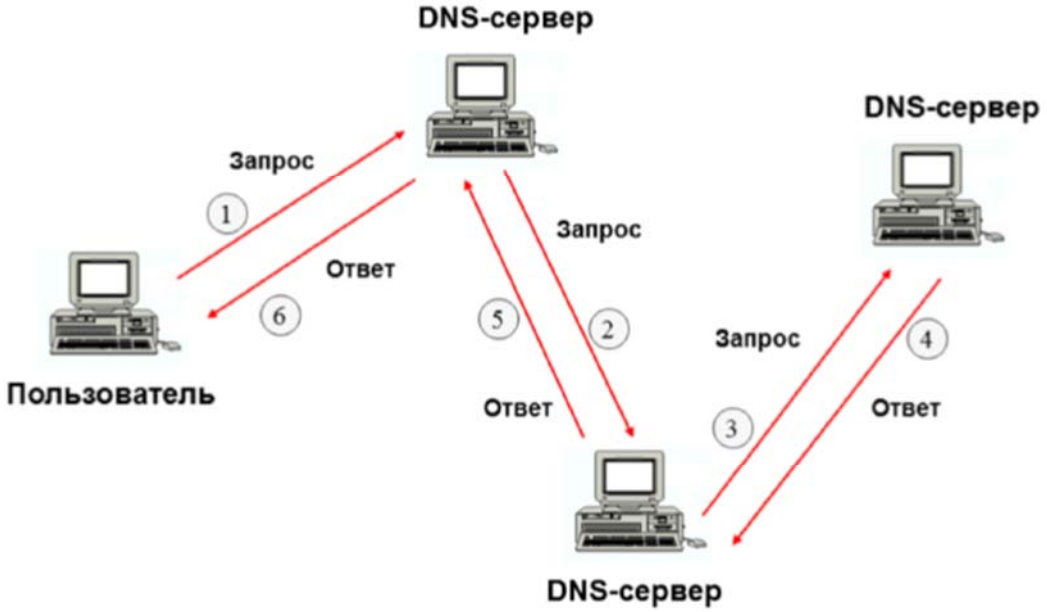


Рисунок 3 - Работа службы доменных имен

Для нормальной работы сети каждому устройству должен быть присвоен IP-адрес. Процедура присвоения адресов происходит в ходе конфигурирования компьютеров и маршрутизаторов. В предыдущих лабораторных работах мы вручную прописывали IP-адреса у каждого компьютера. Конечно, если в сети имеется несколько компьютеров, то прописать IP-адрес для каждого из них не составит большого труда. Но если сеть состоит из большого числа компьютеров, например, 50 или 100, то это становится уже более сложной задачей. А если на сети происходят какие-то изменения, то администратору сети опять придется менять IP-адреса вручную. При этом администратор должен помнить, какие IP-адреса он использовал, а какие еще свободны. При конфигурировании сети помимо IP-адресов устройству назначается маска сети, IP-адрес машрутизатора, IP-адрес DNS- сервера, доменное имя компьютера. Даже при небольшом размере сети это очень утомительная процедура для администратора.

Для автоматического процесса конфигурирования компьютеров (хостов) был придуман протокол DHCP (Dynamic Host Configuration Protocol), который позволяет автоматически настраивать IP-адреса на компьютерах пользователя. Он работает по принципу клиент-сервер. Рассмотрим более подробно работу протокола DHCP. В данном процессе участвуют две стороны. Первая сторона это DHCP – клиент. Это может быть обычный компьютер, ноутбук или смартфон, который подключается через сеть Wi-Fi, это та сторона, которая хочет получить IP-адрес. Вторая сторона это DHCP-сервер, который выдает IP-адреса. В качестве DHCP-сервера может выступать обычный маршрутизатор или специальный сервер. Рассмотрим этот процесс более подробно (рис. 4).

Рисунок 4 - Принципы работы протокола DHCP

В локальной сети одновременно может присутствовать несколько DHCP-серверов, которые должны действовать согласованно.

1.При подключении компьютера к сети он пытается найти DHCP-сервер и выполняет запрос на широковещательный адрес 255.255.255.255, рассылая пакет DHCPDISCOVER. В этом запросе он указывает свой MAC-адрес. Этот запрос обозначает, что компьютеру нужен IP-адрес и он обращается за ним к серверам DHCP. Все компьютеры локальной сети получают такой запрос, но обрабатывается он только DHCP-серверами.

2. Все DHCP-серверы отвечают на запрос сообщением DHCPOFFER, предлагая значение IP-адреса.

3.Хост выбирает один из предложенных адресов и посылает широковещательный запрос DHCPREQUEST, сообщая, что один из предложенных адресов выбран. Такой запрос содержит идентификатор сервера, предложившего выбранный IP-адрес.

4.Сервер, предложивший выбранный IP-адрес, отвечает подтверждением DHCPPARK.

5.После окончания работы хост отправляет сообщение DHCPRELEASE, освобождая выбранный IP-адрес.

В качестве сервера DHCP в компьютерных сетях могут использоваться машины, работающие под управлением Windows Server, Linux, FreeBSD или других серверных операционных систем, а также аппаратные устройства, такие как, маршрутизаторы и точки доступа. Минимальная настройка сервера DHCP заключается в определении диапазона свободных IP-адресов.

DHCP-сервер может работать в следующих режимах:

- ручное назначение статических адресов;
- автоматическое назначение статических адресов;
- автоматическое распределение динамических адресов.

В **ручном** режиме администратор помимо списка доступных адресов снабжает DHCP-сервер информацией о жестком соответствии IP-адресов физическим адресам или другим идентификаторам клиентских узлов. DHCP-сервер, пользуясь этой информацией, всегда выдаст определенному DHCP-клиенту один и тот же назначенный ему администратором IP-адрес, а также другие конфигурационные параметры.

В режиме **автоматического** назначения статических адресов DHCP-сервер самостоятельно без вмешательства администратора произвольным образом выбирает компьютеру IP-адрес из списка наличных IP-адресов. Адрес дается клиенту в постоянное пользование, т.е. между информацией, идентифицирующей клиента и его IP-адресом, как и при ручном назначении, существует постоянное соответствие. При всех последующих запросах сервер возвращает клиенту тот же IP-адрес.

При **динамическом** распределении адресов DHCP-сервер выдает адрес клиенту на ограниченное время, называемое сроком аренды. Когда компьютер, который является клиентом DHCP, удаляется из сети, назначенный ему IP-адрес автоматически освобождается. Это дает возможность использовать этот IP-адрес при подключении другого компьютера. Так, например, если сотрудник уехал в командировку со своим ноутбуком, то освободившийся IP-адрес может использовать другой сотрудник данной организации. Таким образом, общее количество IP-адресов, необходимое организации равно числу сотрудников, которые присутствуют в офисе.

При динамическом распределении адресов администратору при настройке DHCP-сервера достаточно один раз указать диапазон адресов, а каждый вновь прибывший сотрудник будет физически подключать в сеть свой компьютер, на котором запускается DHCP-клиент.

Контрольные вопросы

1. Опишите назначение службы DNS
2. Какие функции DHCP-сервера вы можете назвать?
3. Опишите ручной способ назначение статических адресов.
4. Опишите автоматическое назначение статических адресов.
5. Какие особенности автоматического распределения динамических адре-сов?
6. Пользователь выходит в сеть Интернет со своего смартфона через сеть Wi-Fi. Какой способ назначения IP-адреса будет применен в данном слу-чае?
7. Опишите сигнальный обмен по протоколу DHCP.
8. Что такое домен?
9. Напишите доменное имя вашей организации.
10. Какие устройства могут выступать в роли DHCP- сервера?

Практическое задание №10. Назначение службы DNS и протокола DHCP. Часть 2

Цель работы

Изучить принципы работы протокола DHCP.

Задание

Построить сеть, состоящую из маршрутизатора, коммутатора и трех компьютеров. В качестве DHCP сервера необходимо использовать маршру-тизатор. Прописать список IP-адресов, которые необходимо назначать устройствам в данной сети и проверить работоспособность сети.

Порядок выполнения работы

1.Открываем Cisco Packet Tracer.

2. Создать сеть, изображенную на рисунке 1.

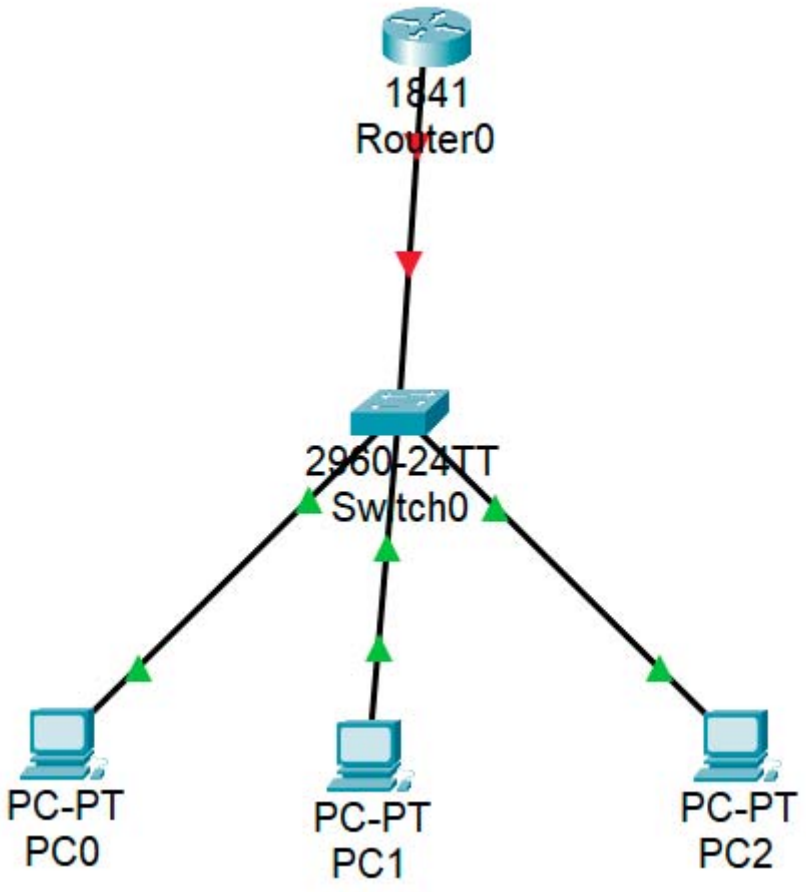


Рисунок 1 - Сеть для исследования протокола DHCP

Далее отказываемся от системной конфигурации и на вопрос « Continue with configuration dialog?» отвечаем **no**.

Настраиваем маршрутизатор с помощью следующих команд:

Router>en

Router #

Router #conf t

Router (config)#int fa0/0

Router (config-if)#no shutdown

Router (config-if)#ip address 192.168.1.1 255.255.255.0

Router **(config-if)#exit**

Теперь надо создать DHCP pool, т.е. пространство IP-адресов, которое мы будем использовать в данной сети. Дадим ему название DHCP. В данной схеме в качестве DHCP сервера выступает машрутизатор (роутер), поэтому и адреса назначаем из сети, в которой находится маршрутизатор, т.е. из сети 192.168.1.0. Каждому компьютеру нам необходимо выдать IP-адрес, а также адрес шлюза, через который маршрутизируется трафик (шлюз по умолчанию - Default gateway). В качестве шлюза по умолчанию записываем IP-адрес маршртизатора- 192.168.1.1. Также для доступа в сеть Интернет необходимо указать DNS сервер. В качестве примера зададим DNS компании Google.

Router (config)#ip dhcp pool DHCP

Router (dhcp-config)#network 192.168.1.0 255.255.255.0
Router (dhcp-config)#default-router 192.168.1.1
Router (dhcp-config)#dns-server 8.8.8.8

Router **(dhcp-config)#exit**

Предположим у нас есть сервер с IP-адресом 192.168.1.100 (на схеме не показан). Мы должны исключить его из пула адресов, чтобы этот адрес не присваивался другим устройствам сети. Серверам, которым необходим по-стоянный доступ в сеть Интернет, не рекомендуется выдавать динамические IP-адреса. Им лучше назначать статические адреса. Для исключения адреса 192.168.1.100 напишем следующую команду:

Router (config)#ip dhcp excluded-address 192.168.1.100

Также исключим IP-адрес, который есть у роутера.

Router (config)#ip dhcp excluded-address 192.168.1.1

Router (config)#exit

Router (config)#wr mem

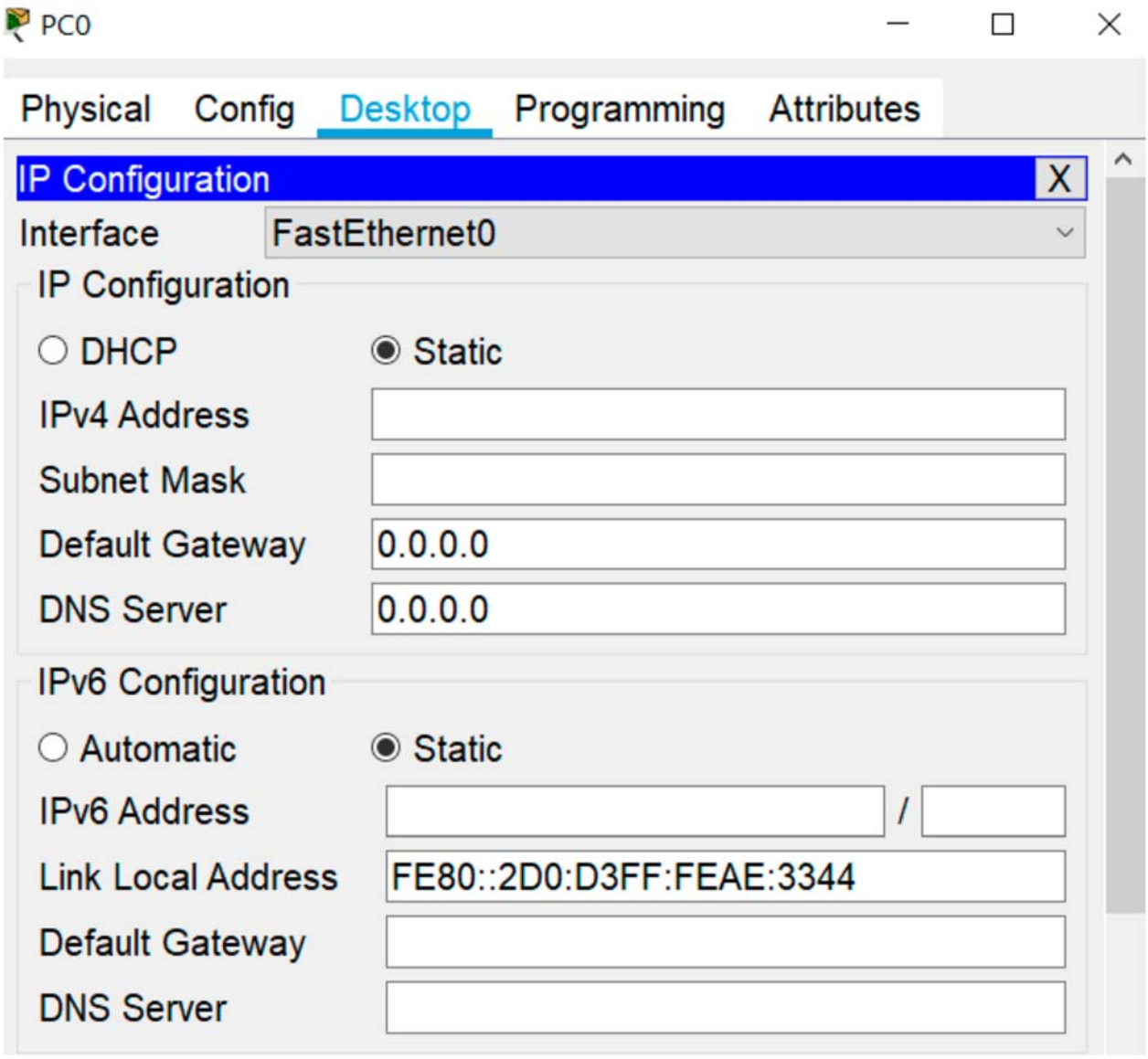


Рисунок 2 - По умолчанию стоит параметр Static

Меняем параметр Static на DHCP и компьютер PC0 автоматически получает IP-адрес, маску, адрес шлюза, а также DNS-сервер.

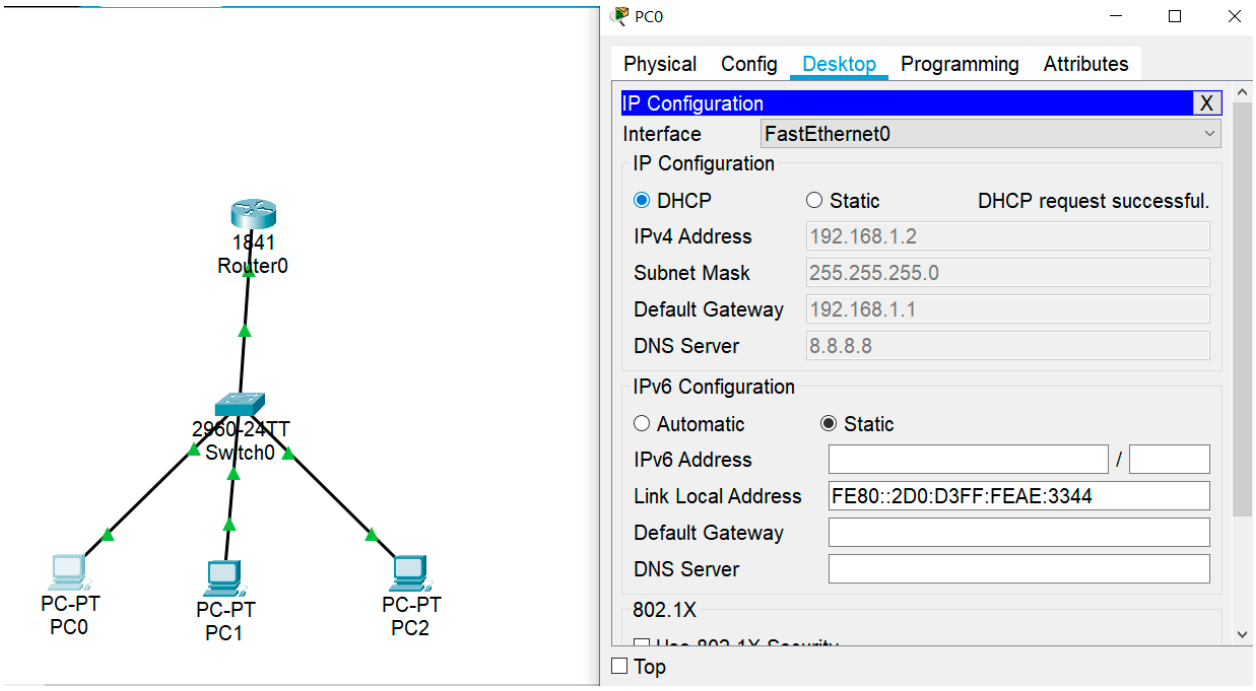


Рисунок 3 - Компьютер получил IP-адрес по протоколу DHCP

Аналогично и другие компьютеры получают IP-адреса. Компьютер PC1 получает адрес 192.168.1.3, а PC2 – 192.168.1.4.

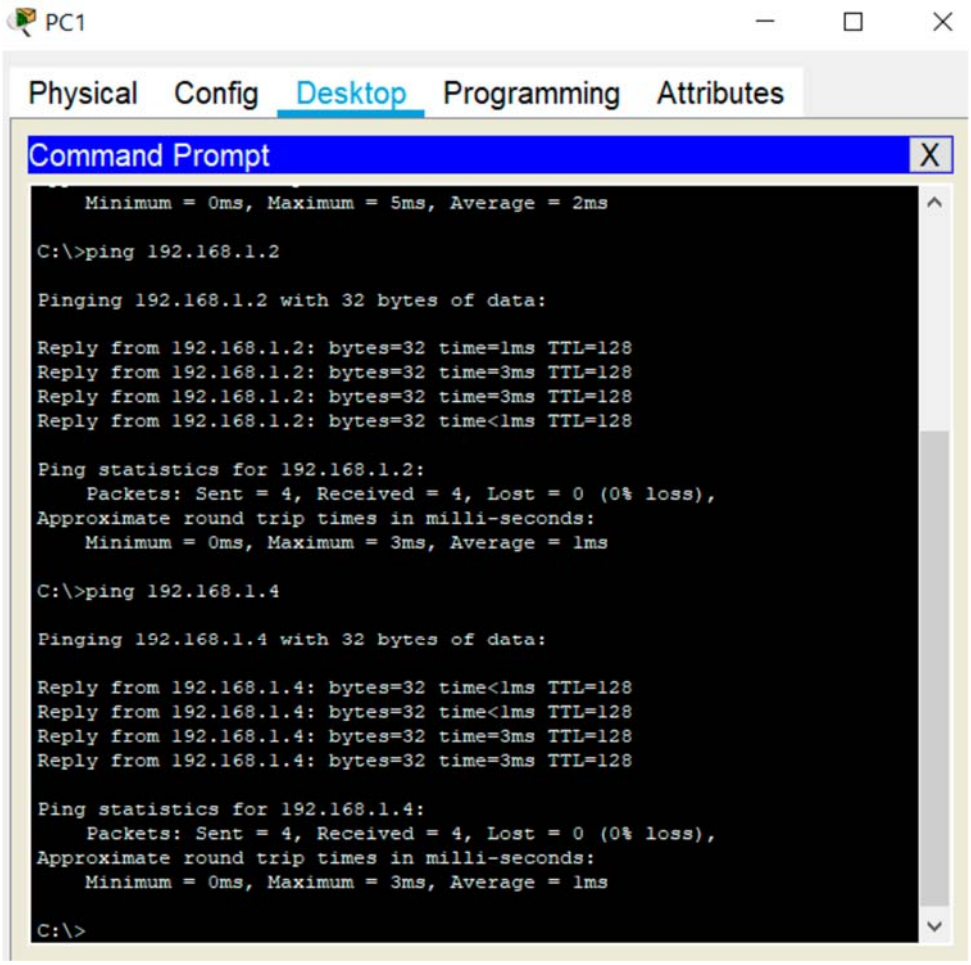


Рисунок 4 - Проверка связи между компьютерами PC0, PC1 и PC2

Проверим взаимосвязь между компьютерами. Так для PC1 проверка связи показана на рисунке 4. Проверить связность между всеми компьютера-ми.

Содержание отчета

В индивидуальном отчёте должны быть указаны цель, задание, представлены необходимые снимки экрана и пояснения к ним. Следует проанализировать полученные данные.

Практическое задание №11. Статическая и динамическая маршрутизации. Часть 1

Цель работы

Изучить принципы статической и динамической маршрутизации

Задание

1.Ознакомиться со статической маршрутизацией;

2. Ознакомиться с динамической маршрутизацией;

3.Ответить на вопросы.

Маршрутизация является функцией третьего уровня модели OSI. Под термином ‘‘маршрутизация’’подразумевают процесс определения наиболее эффективного пути от одного устройства к другому. Основным устройством, отвечающим за осуществление процесса маршрутизации, является ***маршрутизатор*.**

Маршрутизатор выполняет две ключевые функции:

-поддерживает таблицы маршрутизации и обменивается информацией об изменениях в топологии сети с другими маршрутизаторами. Эта функция реализуется с помощью одного или нескольких протоколов маршрутизации;

-когда пакеты приходят на один из интерфейсов, маршрутизатор, руководствуясь таблицей маршрутизации, должен определить, куда именно сле-дует отправить пакет.

При этом он использует одну или несколько ***метрик маршрутизации*** для того чтобы установить оптимальный путь, по которому должен следовать сетевой трафик. Метрика маршрутизации это параметр, по которому опреде-ляется наиболее предпочтительный маршрут. Для определения наилучшего межсетевого маршрута вычисляются различные метрики: полоса пропуска-ния, задержки, надежность, загрузка, стоимость и др.

Маршрутизаторы используют протоколы маршрутизации для обмена таблицами маршрутизации и совместного использования информации о доступных маршрутах.

При **статической** маршрутизации все записи в таблице имеют неизменяемый статически статус, что подразумевает бесконечный срок их жизни. Записи о маршрутах составляются и вводятся в память каждого маршрутизатора вручную администратором сети. При изменении состоянии сети администратор должен отразить эти изменения в таблице маршрутизации. Статическая маршрутизация не подходит для большинства сложных систем, так как сети включают избыточные связи, смешанные топологии и разнообраз-ные протоколы. При статической маршрутизации администратор полностью контролирует сеть, т.е. какой маршрут прописали, так и будет работать сеть. Это является ее плюсом.

При **динамической (адаптивной)** маршрутизации все изменения в конфигурации сети автоматически отражаются в таблицах маршрутизации благодаря протоколам маршрутизации. Эти протоколы собирают информацию о топологии связей в сети, что позволяет им оперативно отражать все текущие изменения. В таблицах маршрутизации обычно имеется информация об интервале времени, в течение которого данный маршрут будет оставаться действительным. Это время

называется время жизни маршрута (TTL). Если по истечении времени жизни существование маршрута не подтверждается протоколом маршрутизации, то он считается не рабочим и пакеты по нему больше не посылаются.

Достоинства динамической маршрутизации:

- автоматическое добавление маршрута;

- организация отказоустойчивости сети. Так, если сеть доступна по двум или более маршрутам, то при недоступности основного маршрута произойдет автоматическое переключение на другой маршрут.

Недостатки динамической маршрутизации:

- более высокая загрузка вычислительных ресурсов сети (память и процессор);

-требуется более высокая квалификация инженеров при поиске неисправностей;

- сеть менее предсказуема, т.е. если сеть очень сложная, то не всегда можно сказать, как пойдет тот или иной маршрут.

Сами протоколы динамической маршрутизации можно классифицировать по нескольким критериям.

По алгоритмам:

1) дистанционно-векторные протоколы (Distance-vector Routing Protocols) – RIP;

2) протоколы состояния каналов связи (Link-state Routing Protocols) - OSPF, IS-IS.

Иногда выделяют третий класс, усовершенствованные дистанционно-векторные протоколы (advanced distance-vector), для того чтобы подчеркнуть

существенные отличия протоколов от классических дистанционно-векторных, например EIGRP.

По области применения:

1) протоколы междоменной маршрутизации (EGP) - BGP ;

2) протоколы внутридоменной маршрутизации (IGP): OSPF, RIP, EIGRP, IS-IS.

IGP (Interior Gateway Protocol). IGP-протоколы используются для пе-редачи информации о маршрутах в пределах автономной системы (AS). Как правило, для упрощения, можно воспринимать автономную систему, как сеть одной компании. К современным IGP-протоколам, как правило, предъявля-ются такие требования:

1) быстрая сходимость;

2) выбор маршрутов в зависимости от физических характеристик сети (полоса пропускания, задержка);

3) поддержка масок переменной длины (VLSM);

4) возможность суммировать маршруты.

Если говорить об использовании IGP-протоколов в сетях крупных про-вайдеров, то также можно добавиться такие требования:

1) поддержка большого количества маршрутов;

2) совместимость и поддержка других технологий.

EGP (Exterior Gateway Protocol). EGP-протоколы используются для передачи информации между автономными системами (AS). На текущий мо-мент представителем этого класса является один протокол BGP. Хотя, чаще всего, BGP используется для передачи маршрутов между разными AS, он может также использоваться и внутри корпоративной сети. Особенно, когда сеть большая.

OSPF (Open Shortest Path First) — протокол динамической марш-рутизации. Он используется для передачи информации между маршрутиза-торами в пределах одной автономной системы (AS).

Протокол OSPF разбивает процедуру построения таблицы маршрути-зации на 2 этапа. К первому относится построение и поддержание базы дан-ных о состоянии связей сети, ко второму построение оптимального маршрута и генерация таблиц маршрутизации.

Построение и поддержание базы данных о состоянии связей сети

Сети связи могут быть представлены в виде графа, в которых верши-нами графа являются маршрутизаторы, а ребрами – связи между ними. Каж-дый маршрутизатор обменивается со своими соседями о текущей конфигу-рации графа связей сети.

Для контроля состояния связей между собой маршрутизаторы переда-ют каждые 10 секунд сообщения Hello. Если это сообщение не поступает от соседа, то маршрутизатор делает вывод, что состояние связи между ними из-менилось на неработоспособное и вносит соответствующие корректировки в свою базу данных. Одновременно он отсылает своим соседям объявления о состоянии связей - LSA (Link State Advertisment).

Построение оптимального маршрута и генерация таблиц маршрутизации

Задача нахождения оптимального пути на графе является достаточно сложной. Для ее решения используется алгоритм Дейкстры. Каждый марш-рутизатор в соответствии с этим алгоритмом ищет оптимальные маршруты от своих интерфейсов до всех известных ему сетей. В каждом найденном маршруте запоминается только один шаг – до следующего маршрутизатора. Эти данные и попадают в таблицу маршрутизации. При изменении состояния связей в сети, каждый маршрутизатор заново ищет оптимальные маршруты и корректирует свою

таблицу маршрутизации. Если в сети появляется новый маршрутизатор, он объявляет о себе сообщением Hello.

Вычислительная сложность алгоритма Дейкстры предъявляет высокие требования к мощности процессоров маршрутизаторов. Каждые 30 минут маршрутизаторы обмениваются всеми записями баз данных, т.е. синхрони-зируют их для более надежной работы сети.

Контрольные вопросы

1. К какому уровню модели OSI относится марщрутизация?

2. Какие функции выполняет маршрутизатор?

3. Что такое метрика маршрутизации?

4. Опишите цель таблицы маршрутизации?

5. Что представляет собой статическая маршрутизация?

6. Что представляет собой динамическая маршрутизация?

7. Назовите достоинства и недостатки статической маршрутизации?

8. Назовите достоинства и недостатки динамической маршрутизации?

9. Как можно классифицировать протоколы динамической маршрутизации?

10. Приведите примеры протоколов динамической маршрутизации.

Практическое задание №11. Изучение процесса работы протокола динамической маршрутизации OSPF с использованием Cisco Packet Tracer.

Часть 2

Цель работы

Изучить и практически освоить процесс настройки протокола динамической маршрутизации OSPF с использованием сетевого симулятора Cisco Packet Tracer. Научиться настраивать протокол OSPF на маршрутизаторах, проверять доступность различных узлов сети.

Задание

1. Ознакомиться с основными понятиями динамической маршрутизации и протокола OSPF в частности.

2. Запустить Cisco Packet Tracer.

3. Собрать необходимую топологию сети, запустить и настроить виртуальное оборудование.

4. Согласно пунктам выполнения практической работы, сделать необходимые снимки экрана. Изучить полученную информацию и оформить ее в соответствии с требованиями раздела «Содержание отчета».

5. Ответить на вопросыю

Порядок выполнения работы

1.Предварительная настройка сетевого оборудования

Соберите сетевую топологию согласно рисунку 1. Топология содержит 3 ПК и 3 маршрутизатора (Cisco 2911), на которых необходимо настроить динамическую маршрутизацию с использованием OSPF.

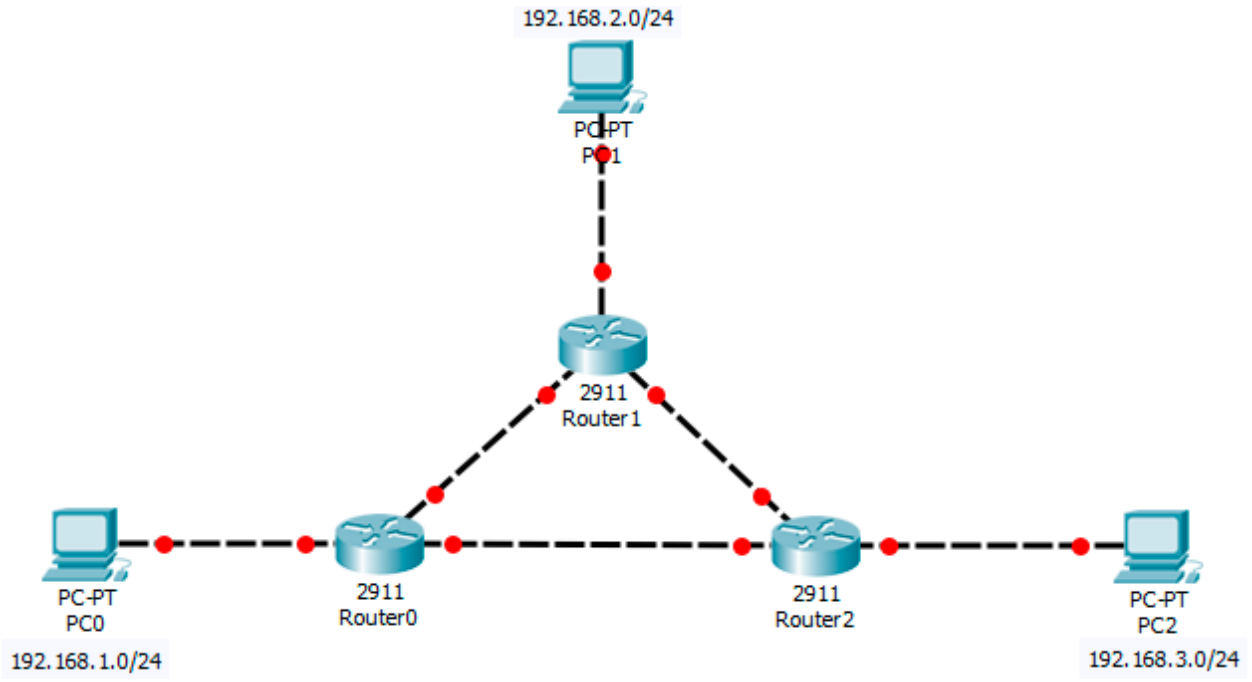


Рисунок 1 - Топология сети

Каждому компьютеру присвойте IP-адрес: PC0 – 192.168.1.2/24 (шлюз по умолчанию 192.168.1.1); PC1 – 192.168.2.2/24 (шлюз по умолчанию 192.168.2.1); PC2 – 192.168.3.2/24 (шлюз по умолчанию 192.168.3.1). Для того чтобы назначить сетевые адреса компьютерам, один раз нажмите левой кнопкой мыши на устройстве и перейдите в закладку Desktop, а затем нажмите на IP Configurations. Введите IP-адрес, маску подсети и шлюз по умолчанию в соответствующие поля, как это показано на рисунке 2 для PC0. Повторите для других компьютеров.

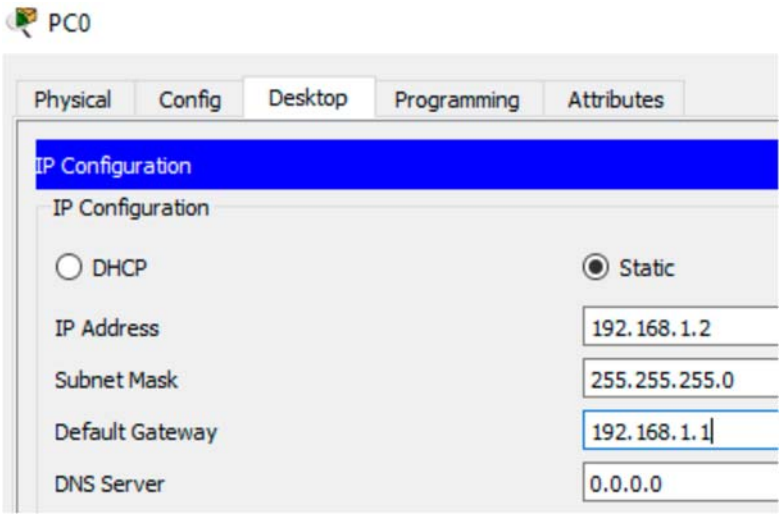


Рисунок 2 - Конфигурация для PC0

Необходимо удостовериться в правильности введенных настроек. Для этого один раз нажмите левой кнопкой мыши на устройстве и перейдите в закладку Desktop, а затем нажмите на Command Prompt. Введите команду:

C:\>ipconfig

Сделайте снимок экрана. Повторите для других PC.

Настройте все маршрутизаторы согласно таблице 1.

Таблица 1. Сетевые адреса маршрутизаторов

Маршрутизатор	Интерфейс	IP-адрес	Маска подсети
Router0	Gig0/0	10.10.10.1	30 бит – 255.255.255.252
	Gig0/1	10.10.11.1	30 бит – 255.255.255.252
	Gig0/2	192.168.1.1	24 бита – 255.255.255.0
Router1	Gig0/0	10.10.10.2	30 бит – 255.255.255.252
	Gig0/1	10.10.12.1	30 бит – 255.255.255.252
	Gig0/2	192.168.2.1	24 бита – 255.255.255.0
Router2	Gig0/0	10.10.12.2	30 бит – 255.255.255.252
	Gig0/1	10.10.11.2	30 бит – 255.255.255.252
	Gig0/2	192.168.3.1	24 бита – 255.255.255.0

Настройте маршрутизатор Router0, для этого один раз нажмите по устройству и перейдите во вкладку CLI, на задаваемый вопрос введите **no**, затем вводите следующие команды (для завершения команды пользуйтесь клавишей **Tab**):

Router>enable

Router#configure terminal

Router(config)#interface gigabitEthernet 0/0

Router(config-if)#ip address 10.10.10.1 255.255.255.252

Router(config-if)#no shutdown

Router(config-if)#exit

Router(config)#interface gigabitEthernet 0/1

Router(config-if)#ip address 10.10.11.1 255.255.255.252

Router(config-if)#no shutdown

Router(config-if)#exit

Router(config)#interface gigabitEthernet 0/2

Router(config-if)#ip address 192.168.1.1 255.255.255.0

Router(config-if)#no shutdown

Router(config-if)#exit

Router(config)#exit

Router#wr mem

Повторите настройки для маршрутизаторов Router1 и Router2 с адреса-ми, взятыми из таблицы. Проверьте доступность шлюзов с каждого ПК. Для этого один раз нажмите левой кнопкой мыши на устройстве и перейдите в закладку Desktop, а затем нажмите на Command Prompt (рисунок 3) и введите команду ping**.**

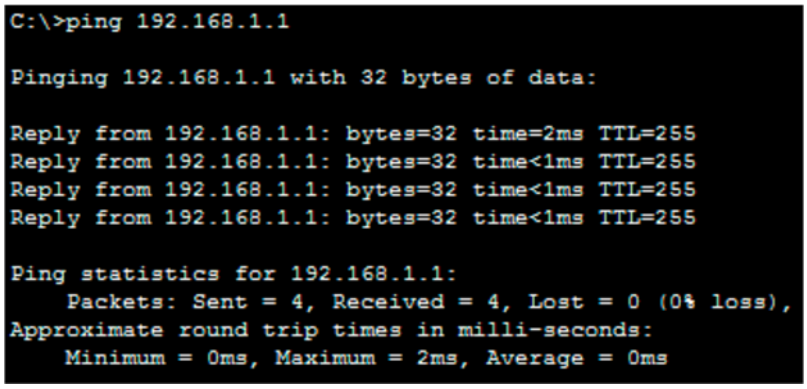


Рисунок 3 - Проверка связности для компьютера PC0

2.Настройка OSPF протокола

Прежде чем настроить протокол динамической маршрутизации, следу-ет настроить адрес на loopback-интерфейсе. Это необходимо для корректной работы протокола OSPF. Loopback-интерфейс – логический интерфейс, не привязанный к физическим. Аналогичный адрес есть на любом из компьюте-ров.

Настраиваем loopback-интерфейс на Router0:

Router>enable

Router#configure terminal

Router(config)#interface loopback 0

Router(config-if)#ip address 192.168.100.1 255.255.255.255 (192.168.100.0/32 – сеть для всех loopback-интерфейсов. Маска 32 бита подразумевает всего один IP-адрес)

Router(config-if)#no shutdown

Router(config-if)#exit

Приступаем непосредственно к настройке OSPF, для этого входим в режим конфигурирования роутера, выбираем протокол ospf и задаем номер процесса 1:

Router(config)#router ospf 1

Указываем все сети, которые подключены к нашему маршрутизатору:

Router(config-router)#network 192.168.1.0 0.0.0.255 area 0 (0.0.0.255 – обратная маска (смотрите таблицу), все маршрутизаторы должны быть в одной области **area 0**)

Router(config-router)#network 10.10.10.0 0.0.0.3 area 0

Router(config-router)#network 10.10.11.0 0.0.0.3 area 0

Router(config-router)#end

Router#wr mem

Как только мы ввели эти команды OSPF автоматически включается на всех интерфейсах, которые соответствуют данном у диапазону адресов.

Router#show running-config (после введения команды используйте клавиши «Пробел» или «Enter» для просмотра настроек) найдите в выведенных настройках строчки с назначенными портам адресами и занесите снимок экрана в отчет (рисунок 4.).

```
interface Loopback0
 ip address 192.168.100.1 255.255.255.255
!
interface GigabitEthernet0/0
 ip address 10.10.10.1 255.255.255.252
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 10.10.11.1 255.255.255.252
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 network 192.168.1.0 0.0.0.255 area 0
 network 10.10.10.0 0.0.0.3 area 0
 network 10.10.11.0 0.0.0.3 area 0
```

Рисунок 4 - Настройки портов и OSPF на маршрутизаторе Router0

Для маршрутизаторов Router1 и Router2 повторить настройки, при этом для них адреса loopback-интерфейсов 192.168.100.2 и 192.168.100.3 соответ-ственно, area

0 для Router1 и Router2. Соседние сети можно посмот реть в настройках каждого роутера. После настройки OSPF на маршрутизаторе Router1 появится сообщение:

01:10:34: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.100.1 on GigabitEthernet0/0 from LOADING to FULL, Loading Done

Оно означает, что был найден «сосед». Занесите снимок экрана в отчет. Повторите для маршрутизатора Router2.

На маршрутизаторе Router2 введите:

Router#show ip ospf neighbor

Видно, что маршрутизатор нашел двух «соседей» (рисунок 5):

```
Neighbor ID     Pri   State           Dead Time   Address
Interface
192.168.100.2     1   FULL/DR         00:00:31    10.10.12.1
GigabitEthernet0/0
192.168.100.1     1   FULL/DR         00:00:31    10.10.11.1
GigabitEthernet0/1
```

Рисунок 5 - Вывод информации о «соседях» маршрутизатора Router2

Для получения информации из таблицы маршрутизации введите команду:

Router#show ip route

Записи, рядом с которыми есть символ «O», означают, что маршрут создан с использованием протокола динамической маршрутизации OSPF (рисунок 6).

```
     10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
O       10.10.10.0/30 [110/2] via 10.10.12.1, 00:08:35,
GigabitEthernet0/0
                      [110/2] via 10.10.11.1, 00:08:35,
GigabitEthernet0/1
C       10.10.11.0/30 is directly connected, GigabitEthernet0/1
L       10.10.11.2/32 is directly connected, GigabitEthernet0/1
C       10.10.12.0/30 is directly connected, GigabitEthernet0/0
L       10.10.12.2/32 is directly connected, GigabitEthernet0/0
O    192.168.1.0/24 [110/2] via 10.10.11.1, 00:08:35,
GigabitEthernet0/1
O    192.168.2.0/24 [110/2] via 10.10.12.1, 00:08:35,
GigabitEthernet0/0
     192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, GigabitEthernet0/2
L       192.168.3.1/32 is directly connected, GigabitEthernet0/2
     192.168.100.0/32 is subnetted, 1 subnets
C       192.168.100.3/32 is directly connected, Loopback0
```

Рисунок 6 - Информация из таблицы маршрутизации

Буква «O» обозначает, что данный маршрут прописался с использованием протокола OSPF. На рисунке видно, что с роутера R2 сеть 192.168.1.0/24 доступна через адрес 10.10.11.1, а этот адрес находится на роутере R0. А сеть 192.168.2.0

доступна через адрес 10.10.12.1, а это адрес интерфейса роутера R1. Повторите вывод информации о «соседях» и данных из таблицы маршрутизации для Router0 и Router1. Проверьте доступность PC0 с маршрутизатора Router2:

Router# ping 192.168.1.2

Router#traceroute 192.168.1.2

Занесите снимок экрана в отчет (рисунок 7) и повторите для PC1:

```
Router# ping 192.168.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1
ms

Router#tr
Router#traceroute 192.168.1.2
Type escape sequence to abort.
Tracing the route to 192.168.1.2

  1   10.10.11.1      1 msec    0 msec    0 msec
  2   192.168.1.2     0 msec    0 msec    0 msec
```

Рисунок 7 - Проверка с Router2 маршрута до компьютера PC0

Сохраните схему сети для выполнения следующей работы.

Контрольные вопросы

1. Опишите принципы работы протокола OSPF.

2. Какой алгоритм для нахождения оптимального пути применяется в протоколе OSPF?

3. Для чего используется алгоритм Дейкстры в протоколе OSPF?

4. Как корректируется таблица маршрутизации при применения протокола OSPF?

5. Опишите последовательность настройки маршрутизаторов в данной лабораторной работе.

6. Опишите последовательность настройки OSPF – протокола.

7. Опишите принципы работы протокола маршрутизации IGP.

8. Что такое метрика маршрутизации? Для чего она используется?

9. Приведите достоинства и недостатки статической маршрутизации.

10. Опишите достоинства и недостатки динамической маршрутизации.

Практическое задание №11. Изучение отказоустойчивости протокола динамической маршрутизации OSPF Tracer. Часть 3

Цель работы

Проверять отказоустойчивость сети, для которой был настроен прото-кол OSPF.

Задание

1. Для выполнения работы необходимо открыть схему сети из работы №11 Часть 2.

2. Проверить отказоустойчивость сети и сделать необходимые снимки экрана. Изучить полученную информацию и оформить ее в соответствии с требованиями раздела «Содержание отчета».

3. Ответить на контрольные вопросы.

Откроем схему, которую вы построили в предыдущей практической работе (рис.1).

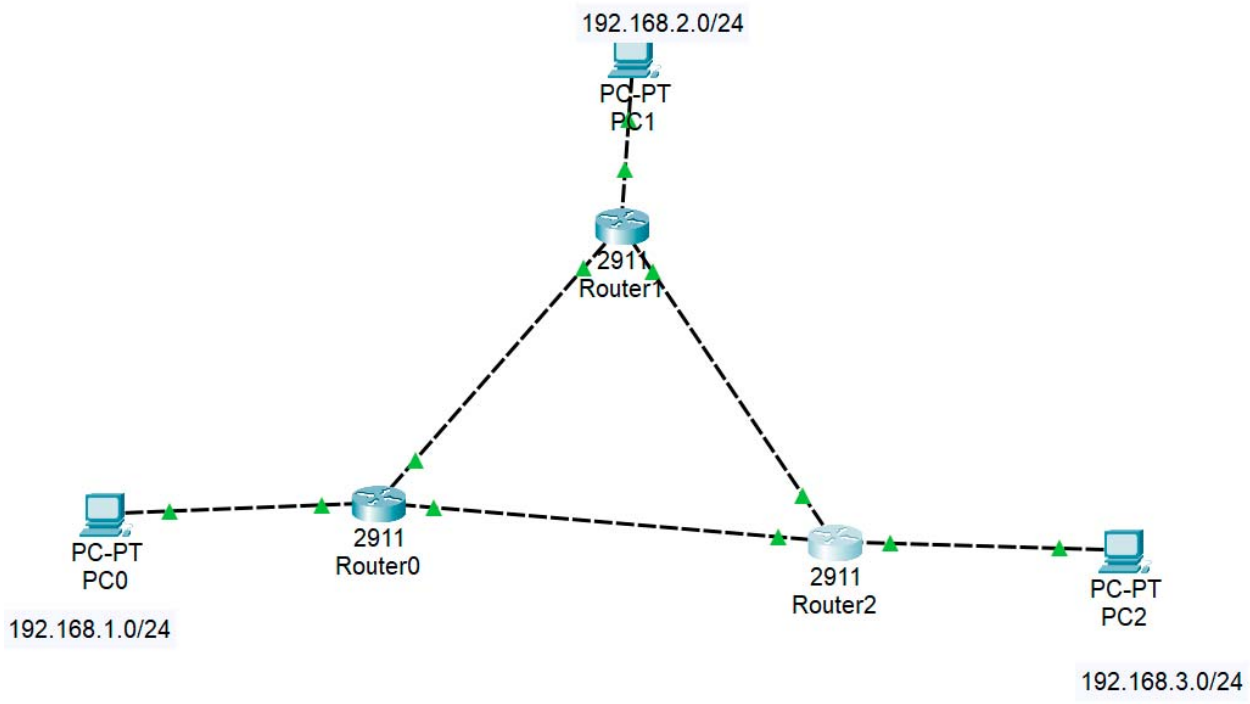


Рисунок 1 - Схема исследуемой сети

Как было показано в предыдущей работе, что с роутера R2 сеть 192.168.1.0/24 доступна через канал, который соединяет роутеры R2 и R0, а сеть 192.168.2.0 доступна через роутер R1. Попробуем вывести из строя ка-нал между роутерами R2 и R0. Для этого нужно выйти в настройки роутера R2 и набрать следующие команды:

Router>enable

Router#configure terminal

Router(config)#interface gigabitEthernet 0/1

Router(config-if)#shutdown

После этого звено между роутерами R2 и R0 вышло из рабочего состояния (рис. 2).

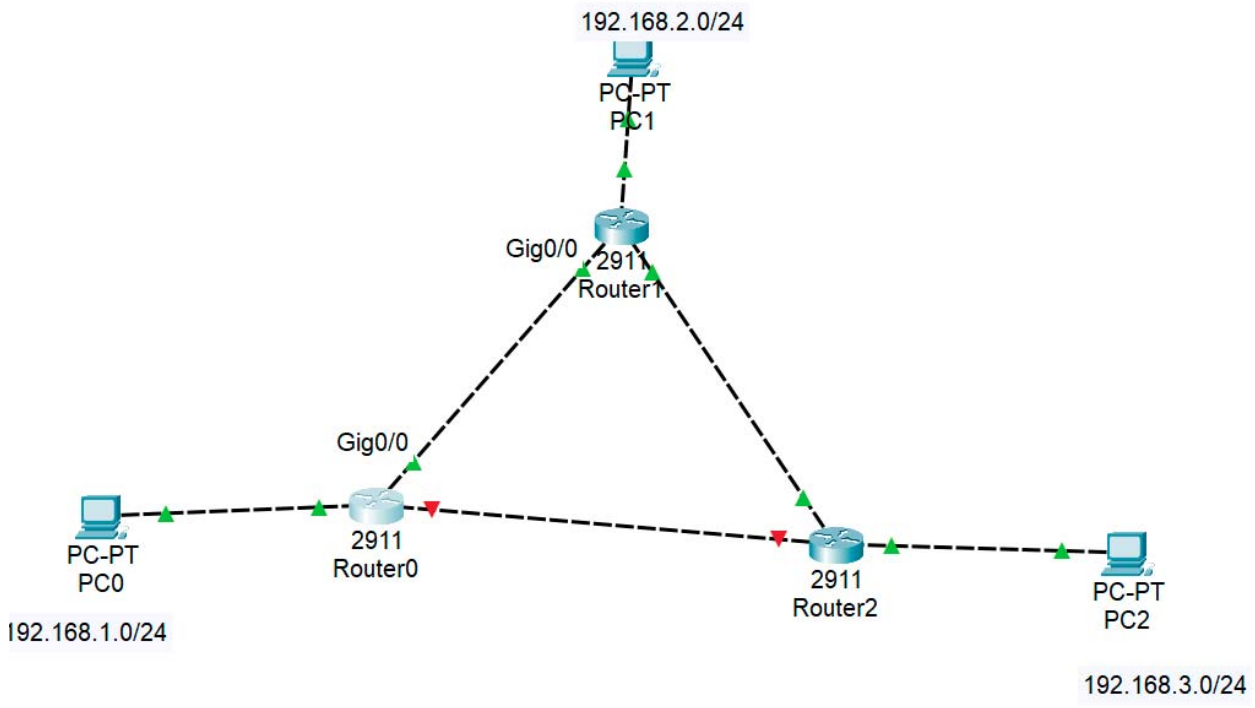


Рисунок 2 - Звено между R2 и R0 находится в нерабочем состоянии

Теперь проверим связь между компьютерами PC2 и PC0, для этого с PC2 пошлем команду ping на PC0. Проверим, установится ли связь и сколько пакетов при этом потеряется. При тестировании необходимо определить 1000 запросов ping.

ping 192.168.1.2 -n 1000

На PC2 определить, сколько было потеряно пакетов (рисунок 3).

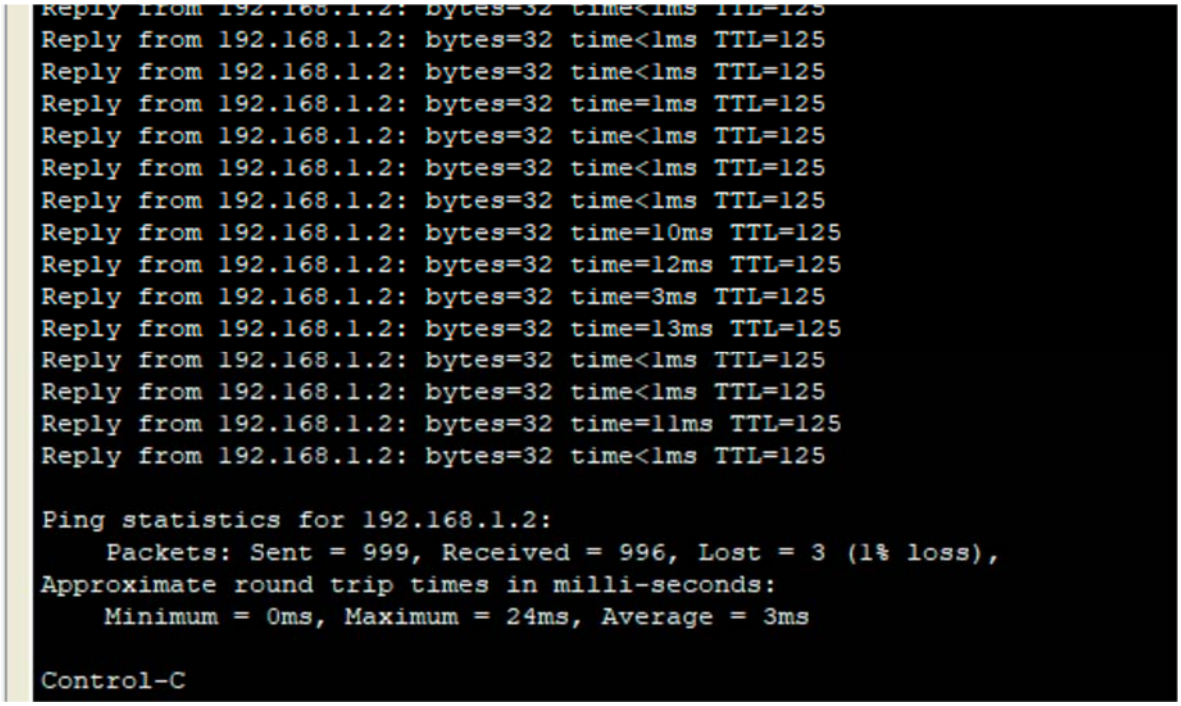


Рисунок 3 - Отправка ping-пакетов с PC2

Для того, чтобы остановить процесс передачи пакетов необходимо нажать комбинацию клавиш Ctrl+C. В данном случае было потеряно 3 из 999 пакетов. Обычно на реальном оборудовании можно произвести настройки, чтобы пакеты не терялись.

Для получения информации из таблицы маршрутизации на Router2 введите команду:

Router#show ip route

На рисунке 4 видно, что сеть 192.168.1.0 доступна теперь через адрес 10.10.12.1, т.е. через маршрутизатор Router1, так же как и сеть 192.168.2.0 (рисунок 4.).

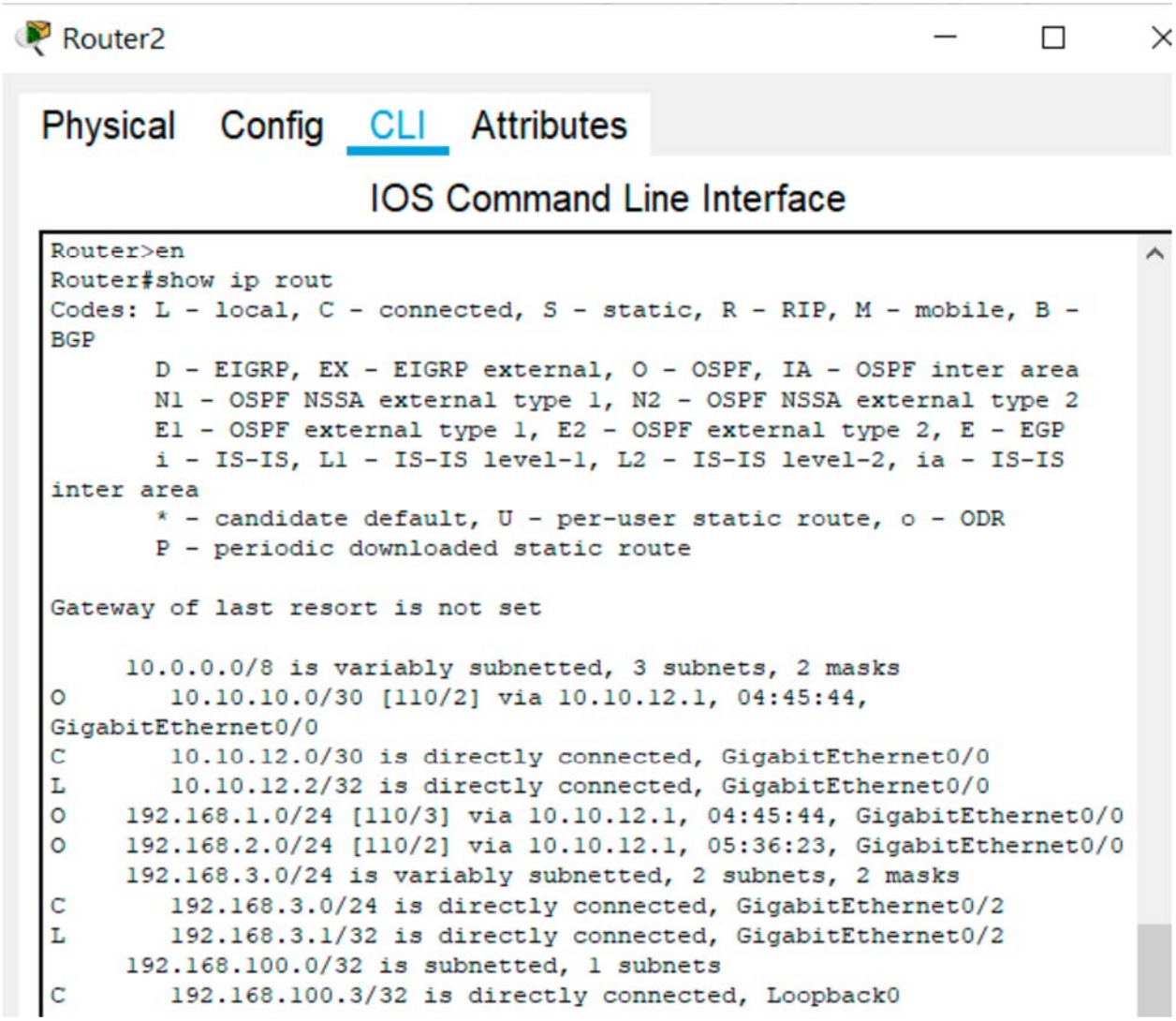


Рисунок 4 - Изменения в таблице маршрутизации

Исследуйте маршрут до 192.168.1.2, убедитесь, что он идет через 10.10.12.1 (рисунок 5). Для этого на PC2 введите команду:

tracert 192.168.1.2

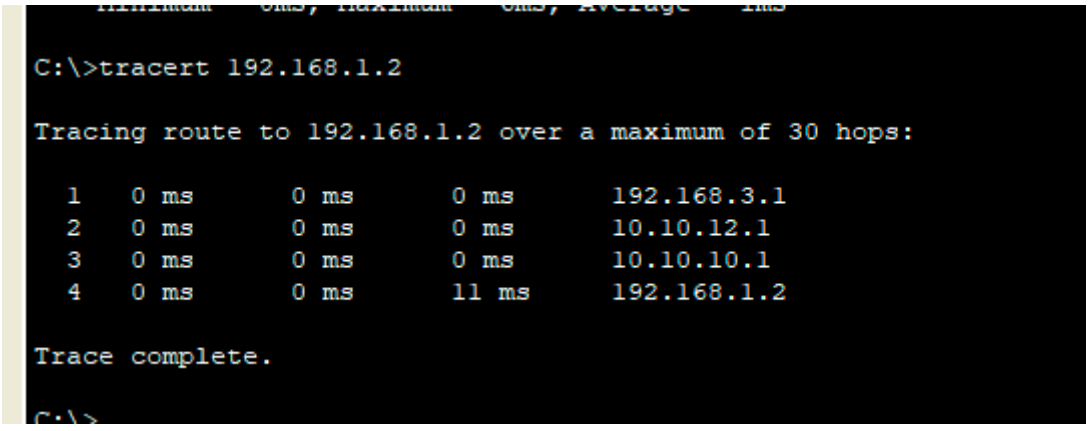


Рисунок 5 - Новый маршрут между PC2 до PC0

Содержание отчета

В индивидуальном отчёте должны быть указаны цель, задание, представлены необходимые снимки экрана и пояснения к ним. Следует проанализировать полученные данные и дать ответы на контрольные вопросы.

Контрольные вопросы

1. Что такое маршрутизация? Зачем она нужна и какие функции выполняет?

2. Какие виды маршрутизации бывают? В чем их различие?

3. Что такое таблица маршрутизации?

4. Опишите цель таблицы маршрутизации?

5. Что такое протокол OSPF? На каком математическом алгоритме он основан? Каковы его основные особенности?

6. Объясните принцип работы протокола маршрутизации OSPF по восстановлению связности сети исходя из полученных результатов.

7. Проведите оценку количества потерянных пакетов и время, потребовавши-еся на восстановление маршрутов исходя из ваших результатов.

8. Какую информацию выводит команда **show ip route**?

9. Как определить, что при настройке OSPF, был обнаружен соседний маршрутизатор?

10. Как изменится маршрут после обрыва связи между соседними маршрутизаторами?

Практическое задание №12. Бесклассовая адресация IPv4

Цель работы

Изучить принципы бесклассовой адресации IPv4

Задание

1.Ознакомиться причинами отказа от классовой маршрутизации;

2. Ознакомиться с принципами разбиения сети на подсети при помощи технологии VLSM;

3.Ответить на вопросы.

С точки зрения эффективности использования адресного пространства классовая модель адресации оказалась нерациональной. Например, если у нас есть диапазон адресов класса B, то в такой сети может быть максимально **Цель работы**

Изучить принципы бесклассовой адресации IPv4

Задание

1.Ознакомиться причинами отказа от классовой маршрутизации;

2. Ознакомиться с принципами разбиения сети на подсети при помощи технологии VLSM;

3.Ответить на вопросы.

С точки зрения эффективности использования адресного пространства классовая модель адресации оказалась нерациональной. Например, если у нас есть диапазон адресов класса B, то в такой сети может быть максимально 65535 устройств. А в существующей сети имеется, например, 2000 компью-теров. Таким образом,

оставшиеся 63535 адресов не будут использоваться. В случае классовой адресации сеть можно разбить на подсети одинакового размера.

Постепенно с ростом сети Интернет произошел отказ от классовой схемы адресации, и была принята бесклассовая модель IPv4-адресации, в которой отсутствует привязка к классу сети и маске подсети по умолчанию. Бесклассовая адресация использует маски сети переменной длины (Variable Length Subnet Mask – VLSM) и технологию межклассовой междоменной маршрутизации (Classless Inter Domain Routing - CIDR). Термин «маска пе-ременной длины обозначает, что сеть может быть разбита на подсети с раз-личными масками подсети. IP-адрес записывается при этом следующим об-разом - IP-адрес/длина префикса. Число после символа «/» означает количе-ство единичных разрядов в маске подсети. Например, сетевой адрес 192.168.1.7 с маской подсети 255.155.255.248 также может быть записан сле-дующим образом 192.168.1.7/29. Число 29 обозначает, что в маске подсети 29 единичных бит.

Допустим, что организации выделена сеть класса С 192.168.1.0/24 (рис.1). Требуется разделить ее на 6 подсетей. В подсетях 1,2,3,4 должно быть 10 узлов, в 5-й подсети – 50, в 6-й подсети -100. Теоретически для сети 192.168.1.0/24 допустимое количество узлов равно 254, а разбить такую сеть на подсети с требуемым количеством узлов без использования технологии VLSM невозможно.

Сначала нужно разделить сеть 192.168.1.0/24 на две подсети. Для этого из четвертого октета необходимо занять 1 бит доя идентификатора подсети, т.е. для идентификации узлов остается 7 бит. В итоге получилось 2 подсети 192.168.1.0/25 и 192.168.1.128/25. В каждой сети может быть 2_7-2=126 узлов. Первую сеть оставим для 6 подсети, а вторую разделим еще на 2 подсети. Для этого возьмем один бит из сети оставшихся, отведенных под идентификатор узла, Таким образом, получается 2 подсети 192.168.1.128/26 и 192.168.1.192/26, в каждой из которых допустимое количество узлов равно 2_6-2=62. Первую подсеть оставляем для пятой подсети, в которой должно быть 50 узлов, а из второй сформируем еще 4 подсети. Для этого займем еще 2 бита из оставшихся 6 бит, отведенных под идентификатор узла. В

результате получим 4 подсети с 2_4-2=14 узлами в каждой, что позволит создать требуемое количество узлов, необходимое для подсетей 1,2,3,4.

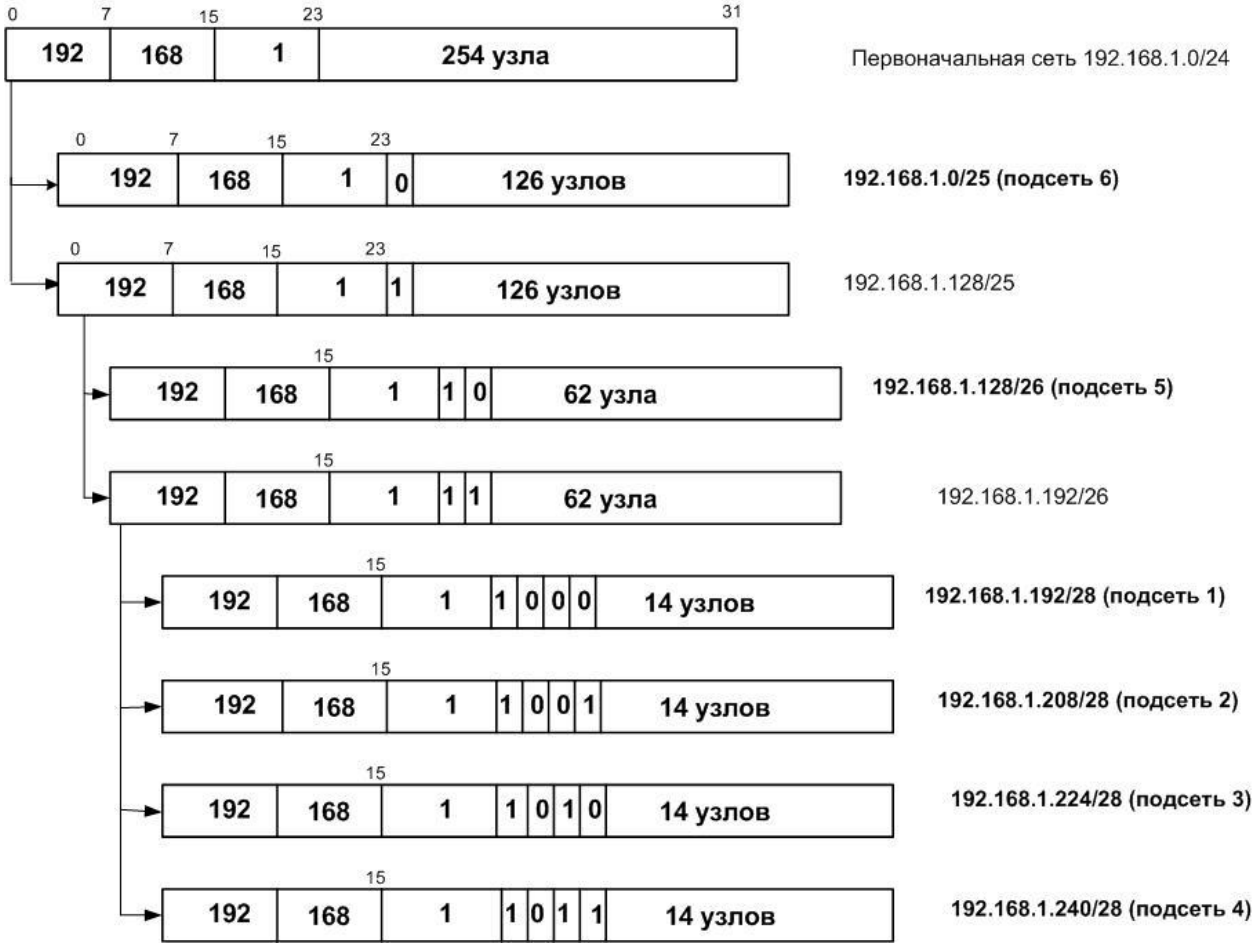


Рисунок 1 - Пример разбиения сети 192.168.1.0/24 на подсети при помощи технологии VLSM

В таблице 1 приведены примеры масок подсети, а также количество уз-лов и IP-адресов при бесклассовой адресации. Из таблицы видно, что чем длиннее маска сети, тем меньшее количество узлов может находиться в дан-ной сети.

Маска подсети должна сообщать сетевому устройству, занимающемуся обработкой конкретного пакета, какая часть IP-адреса в нем определяет адрес сети, а какая часть – адрес сетевого интерфейса в этой сети. Маршрутизатор выполняет логическое перемножение IP-адреса на маску подсети для того, чтобы получить адрес сети, в которую следует отправить данный пакет.

Таблица 1. Бесклассовая IP-адресация

№№	Маска подсети	Количество узлов	Количество IP-адресов	Обратная маска
1	255.255.255.255 /32	1	1	0.0.0.0
2	255.255.255.254 /31	2	2	0.0.0.1
3	255.255.255.252 /30	2	4	0.0.0.3
4	255.255.255.248 /29	6	8	0.0.0.7
5	255.255.255.240 /28	14	16	0.0.0.15
6	255.255.255.224 /27	30	32	0.0.0.31
7	255.255.255.192 /26	62	64	0.0.0.63
8	255.255.255.128 /25	126	128	0.0.0.127
9	255.255.255.0 /24	254	256	0.0.0.255
10	255.255.254.0 /23	510	512	0.0.1.255
11	255.255.252.0 /22	1022	1024	0.0.3.255
12	255.255.248.0 /21	2046	2048	0.0.7.255
13	255.255.240.0 /20	4094	4096	0.0.15.255
14	255.255.224.0 /19	8190	8192	0.0.31.255
15	255.255.192.0 /18	16 382	16 384	0.0.63.255
16	255.255.128.0 /17	32 766	32 768	0.0.127.255
17	255.255.0.0 /16	65 534	65 536	0.0.255.255
18	255.254.0.0 /15	131 070	131 072	0.1.255.255
19	255.252.0.0 /14	262 142	262 144	0.3.255.255
20	255.248.0.0 /13	524 286	524 288	0.7.255.255
21	255.240.0.0 /12	1 048 574	1 048 576	0.15.255.255
22	255.224.0.0 /11	2 097 150	2 097 152	0.31.255.255
23	255.192.0.0 /10	4 194 302	4 194 304	0.63.255.255
24	255.128.0.0 /9	8 388 606	8 388 608	0.127.255.255
25	255.0.0.0 /8	16 777 214	16 777 216	0.255.255.255
26	254.0.0.0 /7	33 554 430	33 554 432	1.255.255.255
27	252.0.0.0 /6	67 108 862	67 108 864	3.255.255.255
28	248.0.0.0 /5	134 217 726	134 217 728	7.255.255.255
29	240.0.0.0 /4	268 435 454	268 435 456	15.255.255.255
30	224.0.0.0 /3	536 870 910	536 870 912	31.255.255.255
31	192.0.0.0 /2	1 073 741 822	1 073 741 824	63.255.255.255
32	128.0.0.0 /1	2 147 483 646	2 147 483 648	127.255.255.255
33	0.0.0.0 /0	4 294 967 294	4 294 967 296	255.255.255.255

Пусть задан IP-адрес 192.190.15.45. Это сеть класса С с маской 24 бита. Произведем побитовое логическое умножение IP-адреса и маски подсети в двоичной форме:

IP- адрес 11000000 10101000 00001111 10010001

Маска 11111111 11111111 11111111 00000000

Адрес сети 11000000 10101000 00001111 00000000

Адрес хоста 00000000 00000000 00000000 10010001

Широковещательный адрес в конкретной сети образуется из адреса се-ти, путем заполнения последних нулевых бит единицами. Следовательно широковещательный адрес для сети 192.190.15.45 будет

Широковещ. адрес 11000000 10101000 00001111 11111111

(192.190.15.255).

Контрольные вопросы

1. Может ли пакет с IP-адресом 172.24.10.1 маршрутизироваться в Ip-сети?

2. Можно ли назначить узлу в локальной сети IP-адрес 192.190.1.31/27?

3. Для адреса 10.2.2.1 укажите класс сети, номер сети и номер узла.

4. Для сети 128.63.2.100 укажите класс сети, номер сети и номер узла.

5. Может ли существовать такой IP-адрес 256.241.201.10?

6. Как маршрутизатор узнает адрес сети для отправки пакета?

7. Укажите недостатки классовой маршрутизации.

8. Какие преимущества имеет бесклассовая адресация?

9. Как происходит деление сети на подсети при масках переменной длины?

10. Как записывается адрес? Приведите примеры.

Практическое задание №13. Применение технологии NAT.

Цель работы

Изучить принципы бесклассовой адресации IPv4

Задание

1.Ознакомиться с принципами применения технологии NAT на сети;

2. Ознакомиться с глобальными и частными IP- адресами;

3.Ответить на вопросы.

В сети Интернет идентификация устройства осуществляется уникальным адресом IPv4, который не должен повторяться в глобальной сети. Такие адреса называются ***глобальные*** (белыми) IP-адресами. Данные адреса марш-рутизируются в сети Интернет, т.е. они доступны из любой точки мира. Не существует двух устройств с одинаковыми IP-адресами, которые были бы подключены к открытой сети. Получают такие адреса у Интернет-провайдеров.

Из-за быстрого роста сети Интернет количество свободных IP-адресов уменьшается. В протоколе IPv4 всего порядка 4,3 млрд. IP-адресов.

Поскольку число публичных адресов ограничено, поэтому в каждом из классов IPv4- сетей определили так называемое ***частные*** (серые) IP-адреса, которые предназначены для использования в локальных компьютерных сетях и не маршрутизируются в сеть Интернет. Данные адреса могут повторяться.

Для локальных сетей, не подключенных к Интернету, можно использовать любые возможные адреса, уникальные в пределах данной сети. Гло-бальные адреса находятся в пределах от 10.0.0.1 до 223.255.255.254 за исключением частных IPv4.

Адресное пространство частных IPv4 состоит из трех блоков:

1) 10.0.0.0- 10.255.255.255 (класс A);

2) 172.16.0.0- 172.31.255.255 (класс B);

3) 192.168.0.0- 192.168.255.255 (класс C).

Но при этом встает вопрос: как обеспечить доступ компьютеров с част-ными IP-адресами в сеть Интернет? Ведь частные адреса не маршрутизиру-ются в сети Интернет. Для решения этой проблемы требуется использовать технологию NAT.

NAT (от англ. Network Address Translation — «преобразование сетевых адресов») — это механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов. (Другими словами, пакет, проходя через маршрутизатор, может поменять свой адрес источника и/или назначения).

NAT выполняет три важных функции.

1. Позволяет экономить IP-адреса (только в случае использования NAT в режиме PAT - Port Address Translation), транслируя несколько внутренних частных IP-адресов в один внешний глобальный IP-адрес (или в несколько, но меньшим количеством, чем внутренних). По такому принципу построено большинство сетей в мире: на небольшой район домашней сети местного провайдера или на офис выделяется 1 глобальный (внешний) IP-адрес, за которым работают и получают доступ интерфейсы с частными (внутренними) IP-адресами.

2. Позволяет предотвратить или ограничить обращение снаружи к внутренним хостам, оставляя возможность обращения изнутри наружу. При инициации соединения изнутри сети создаётся трансляция. Ответные пакеты, поступающие снаружи, соответствуют созданной трансляции и поэтому пропускаются. Если для пакетов, поступающих снаружи, соответствующей трансляции не существует, они не пропускаются.

3. Позволяет скрыть определённые внутренние сервисы внутренних хостов/серверов. По сути, выполняется та же указанная выше трансляция на определённый порт, но возможно подменить внутренний порт официально зарегистрированной службы (например, 80-й порт TCP (HTTP-сервер) на внешний 54055-й). Это необходимо для повышения безопасности и сокрытия «непубличных» ресурсов.

Применение NAT позволяет скрыть адреса узлов своей сети, чтобы не дать возможности злоумышленникам составить представление о структуре и масштабах корпоративной сети, а также о структуре и интенсивности исхо-дящего и входящего трафика.

Традиционная технология NAT подразделяется на технологии *базовой трансляции сетевых адресов* (Basic Network Address Translation, Basic NAT) и *трансляции сетевых адресов и портов* (Network Address Port Translation, NAPT). В технологии Basic NAT для отображения используются только IP-адреса, а в технологии NAPT – еще так называемые транспортные идентифи-каторы, в качестве которых чаще всего выступают порты TCP и UDP.

Базовая трансляция сетевых адресов

Если количество локальных узлов, которым необходимо обеспечить выход во внешнюю сеть меньше или равно имеющемуся количеству глобальных адресов, то для каждого частного адреса гарантировано однозначное отображение на глобальный адрес. В такой ситуации целью трансляции является не столько решение проблемы недостатка адресов, сколько обеспечение безопасности.

Частные адреса узлов могут отображаться на глобальные адреса статически. Соответствие внутренних адресов внешним адресам задается табли-цей, поддерживаемой маршрутизатором или файерволом, на котором уста-новлено программное обеспечение NAT. Файервол - это система, которая предотвращает

несанкционированный доступ к сети, он блокирует любой се-тевой трафик, который является подозрительным.

Рассмотрим небольшой пример (рис. 1). Пусть узел A сети 1 (адрес 10.0.1.4) посылает пакет в сеть 2 узлу D (адрес 10.0.2.3). В таблице NAT на роутерах R1 и R2 имеется информация, указанная на рисунке 1.

Когда узел A посылает узлу пакет узлу D, то он помещает в заголовок пакета в качестве адреса глобальный адрес узла D - 185.130.15.1 . Пакет направляется к маршрутизатору R1, которому известен маршрут к сети B. Перед отправкой пакета модуль NAT, работающий на данном мапшрутизато-ре, используя свою таблицу отображения, заменяет в поле адреса источника частный адрес 10.0.1.4 соответствующим ему глобальным адресом 183.230.25.2.

Когда пакет после путешествия во внешней сети, поступает на R2, на котором также находится NAT, глобальный адрес назначения 185.130.15.1 преобразуется в частный IP-адрес – 10.0.2.1. Пакеты, передаваемые в обрат-ном направлении проходят аналогичную процедуру трансляции адресов.

Таблица NAT- отображения сети A

Частные адреса	Глобальные адреса
10.0.1.4	183.230.25.2
10.0.1.5	183.230.25.3
10.0.1.7	183.230.25.4

Таблица NAT- отображения сети B

Частные адреса	Глобальные адреса
10.0.2.1	185.130.15.1
10.0.2.3	185.130.15.2
10.0.2.9	185.130.15.3

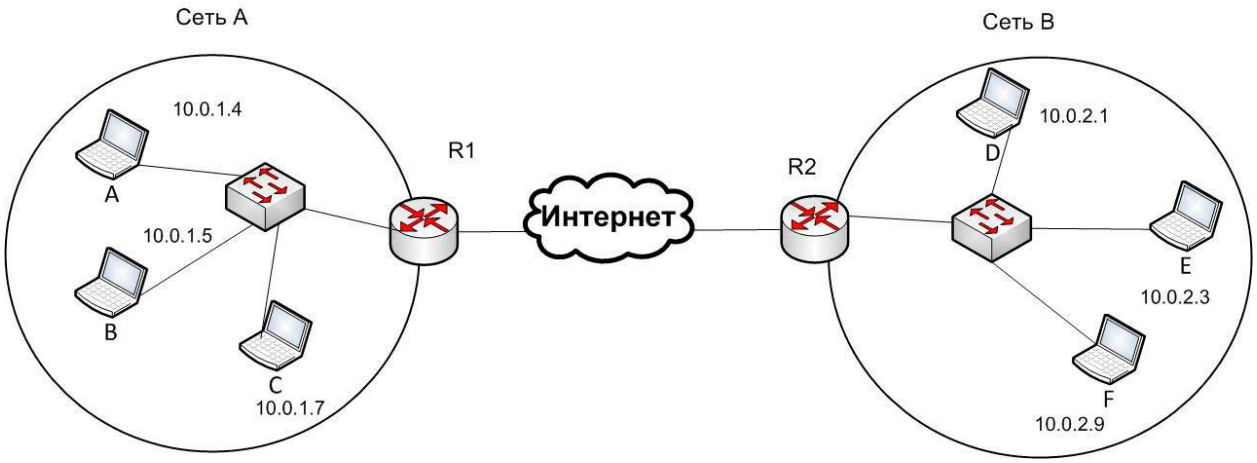


Рисунок 1 - Базовая трансляция сетевых адресов

Трансляция сетевых адресов и портов

Пусть организация имеет локальную IP-сеть, а внешнему интерфейсу пограничного маршрутизатора назначается только один глобальный IP-адрес. Остальным узлам сети назначены частные адреса. Технология NATP позволяет всем узлам сети одновременно взаимодействовать с внешними се-тями, используя единственный глобальный IP -адрес. При этом пакеты из внешних сетей должны каким-то образом находить определенный узел-отправитель в локальной сети, поскольку в поле адреса источника помещает-ся один и тот же адрес – внешнего интерфейса маршрутизатора.

Для однозначной идентификации узла – отправителя используется номер порта протоколов UDP или TCP. Но из внутренней сети может исходить несколько запросов с совпадающими номерами портов отправителя. Решение состоит в том, что при прохождении пакета из внутренней во внешнюю сеть, каждой паре портов (внутренний частный адрес, номер порта TCP или UDP отправителя) ставится в соответствие пара (глобальный адрес внешнего интерфейса, назначенный номер порта TCP или UDP). Назначенный порт выбирается произвольно, но он должен быть уникальным. Соответствие фиксируется в таблице NAT-отображения (рис. 2).

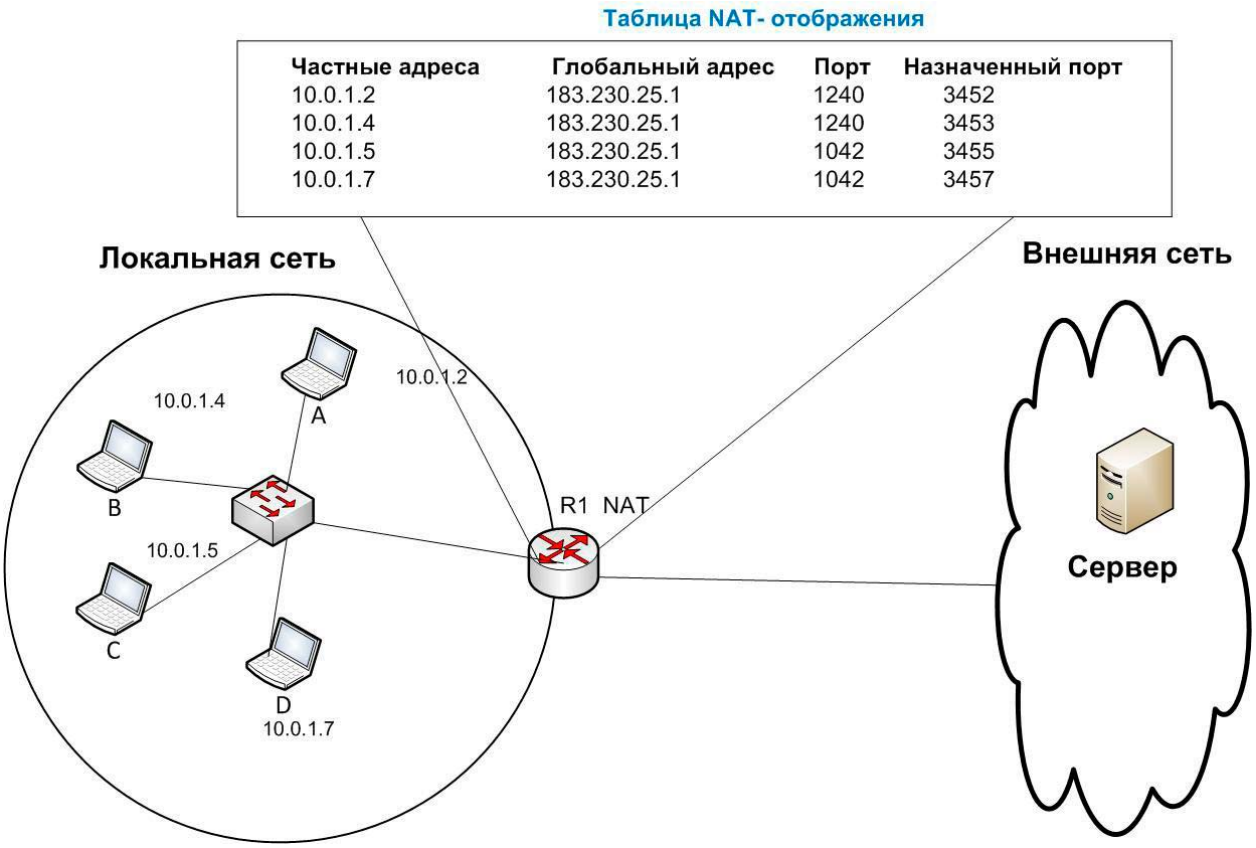


Рисунок 2 - Трансляция сетевых адресов и портов для исходящих сеан-сов TCP и UDP

На рисунке 2 приведен пример, когда в локальной сети используются частные адреса из блока 10.0.0.0. Внешнему интерфейсу маршрутизатора назначен IP-адрес 183.230.25.1.

Контрольные вопросы

1. Поясните, в чем разница между глобальными и частными адресами.

2. Из каких блоков состоит адресное пространство частных IPv4?

3. Что представляет собой технология NAT?

4. Какие функции выполняет технология NAT?

5. Какие технологии NAT вы знаете?

6. Что подразумевает базовая трансляция сетевых адресов?

7. Опишите назначение файервола.

8. Что подразумевает трансляция сетевых адресов и портов?

9. Что представляет собой таблица NAT – отображения в Basic NAT ?

10. Что представляет собой таблица NAT – отображения в NATP?

Практическое задание №14. Изучение технологии NAT

Цель работы

Изучить и практически освоить процесс настройки технологии NAT с использованием стандартных и расширенных списков доступа (access-list) для организации взаимосвязи подразделений компании и обеспечения доступа в Интернет.

Задание

1. Ознакомиться основными функциями технологии NAT.

2. Запустить Cisco Packet Tracer.

3. Собрать необходимую топологию сети, запустить и настроить вирту-альное оборудование.

4. Согласно пунктам выполнения практической работы, сделать необходимые снимки экрана. Изучить полученную информацию и оформить ее в соответствии с требованиями раздела Содержание отчета.

5. Ответить на контрольные вопросы.

Порядок выполнения работы

Предварительная настройка сетевого оборудования

Соберите сетевую топологию согласно рисунку 1

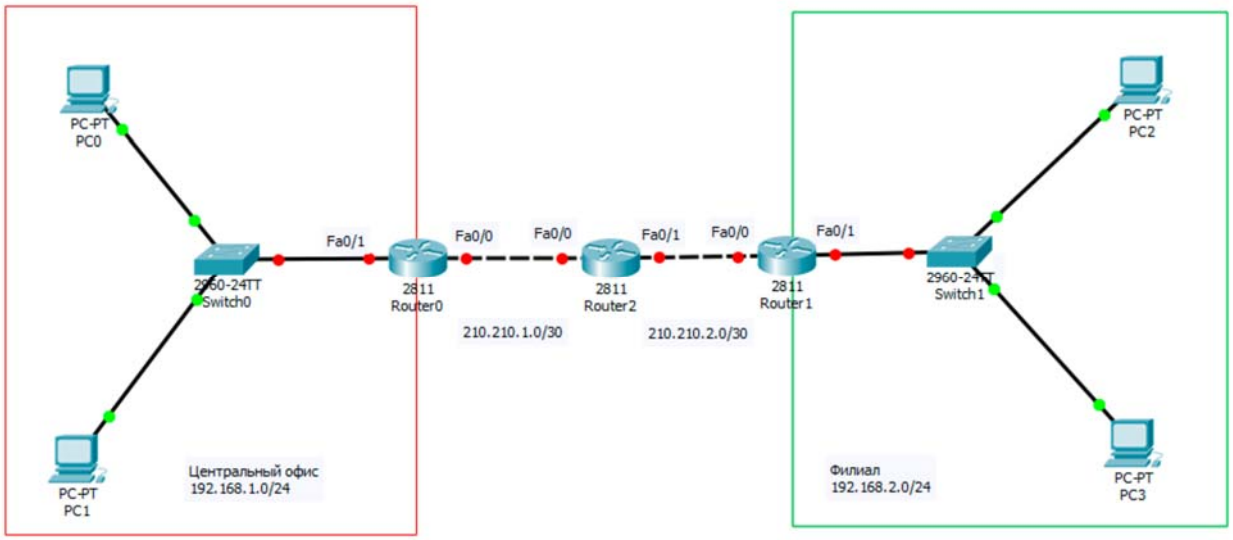


Рисунок 1 - Топология сети

Топология сети состоит из сетевого оборудования центрального офиса: 2 персональных компьютера, коммутатор (Cisco 2960), пограничный маршрутизатор (Cisco 2811), используемый для выхода в Интернет и связи с фили алом, В филиале 2 находится 2 персональных компьютера, коммутатор (Cisco 2960) и пограничный маршрутизатор (Cisco 2811), используемый для вы-хода в Интернет и связи с центральным офисом. Также имеется маршрутизатор (Cisco 2811) Интернет провайдера, который симулирует сеть Интернет. Сетевые адреса всех устройств указаны в таблице 1.

Таблица 1

Сетевые адреса устройств

Сетевой элемент	Интерфейс	IP-адрес	Маска подсети
PC0	FastEthernet 0	192.168.1.2 (шлюз по умолчанию 192.168.1.1)	255.255.255.0 (24 бита)
PC1	FastEthernet 0	192.168.1.3 (шлюз по умолчанию 192.168.1.1)	255.255.255.0 (24 бита)
PC2	FastEthernet 0	192.168.2.2 (шлюз по умолчанию 192.168.2.1)	255.255.255.0 (24 бита)
PC3	FastEthernet 0	192.168.2.3 (шлюз по умолчанию 192.168.2.1)	255.255.255.0 (24 бита)
Router0 (центральный офис)	FastEthernet 0/0	210.210.1.2	255.255.255.252 (30 бит)
	FastEthernet 0/1	192.168.1.1	255.255.255.0 (24 бита)
Router1 (филиал)	FastEthernet 0/0	210.210.2.2	255.255.255.252 (30 бит)
	FastEthernet 0/1	192.168.2.1	255.255.255.0 (24 бита)
Router2 (Интернет провайдер)	FastEthernet 0/0	210.210.1.1	255.255.255.252 (30 бит)
	FastEthernet 0/1	210.210.2.1	255.255.255.252 (30 бит)

Каждому компьютеру присвойте IP-адрес. Для того чтобы назначить сетевые адреса компьютерам, один раз нажмите левой кнопкой мыши на устройстве и перейдите в закладку Desktop, а затем нажмите на IP Configura-tions. Введите IP-адрес, маску подсети и шлюз по умолчанию в соответству-ющие поля, как это показано на рисунке 2 для PC0. Повторите для других компьютеров.

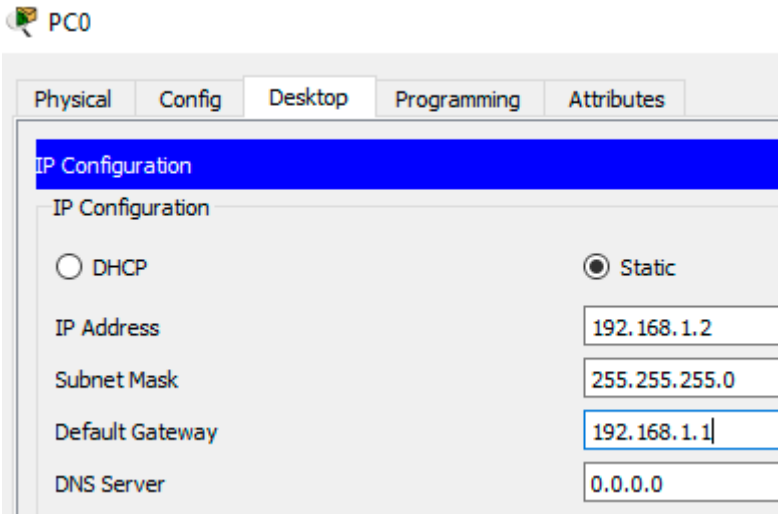


Рисунок 2 - Конфигурация PC0

Необходимо удостовериться в правильности введенных настроек. Для этого один раз нажмите левой кнопкой мыши на устройстве и перейдите в закладку Desktop, а затем нажмите на Command Prompt. Введите команду:

C:\>ipconfig

Сделайте снимок экрана. Повторите для других PC.

Настройте маршрутизатор центрального офиса Router0, для этого один раз нажмите по устройству и перейдите во вкладку CLI, на задаваемый вопрос введите **no**, затем вводите следующие команды (для завершения команды нажмите клавишу **Tab**):

Router>enable

Router#configure terminal

Router(config)#interface fastEthernet 0/0

Router(config-if)#ip address 210.210.1.2 255.255.255.252

Router(config-if)#no shutdown

Router(config-if)#exit

Router(config)#interface fastEthernet 0/1

Router(config-if)#ip address 192.168.1.1 255.255.255.0

Router(config-if)#no shutdown

Router(config-if)#exit

Назначьте маршрут по умолчанию для организации сетевой связности с филиалом и выхода в Интернет:

Router(config)#ip route 0.0.0.0 0.0.0.0 210.210.1.1

Router(config)#end

Router#wr mem

Router#show running-config (после введения команды используйте клавиши «Пробел» или «Enter» для просмотра настроек) найдите в выведенных настройках строчки с назначенными портам адресами и занесите снимок экрана в отчет (рисунок 3).

```
interface FastEthernet0/0
 ip address 210.210.1.2 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 210.210.1.1
```

Рисунок 3 - Вывод информации по проведенным настройкам Router0

Повторите настройки для маршрутизатора филиала, взяв необходимую информацию из таблицы 1.

Настройте маршрутизатор Интернет провайдера (используются гло-бальные IP-адреса):

Router>enable

Router#configure terminal

Router(config)#interface fastEthernet 0/0

Router(config-if)#ip address 210.210.1.1 255.255.255.252

Router(config-if)#no shutdown

Router(config-if)#exit

Router(config)#interface fastEthernet 0/1

Router(config-if)#ip address 210.210.2.1 255.255.255.252

Router(config-if)#no shutdown

Router(config-if)#end

Настройка NAT

На Router0 и Router1 настройте NAT для доступа в Интернет (внутри корпоративной сети используются частные IP-адреса, которые не маршрути-зируются в сети Интернет). Для настройки Router0 введите следующие ко-манды:

Router>enable

Router#configure terminal

Router(config)#interface fastEthernet 0/0

Router(config-if)#ip nat outside

Router(config-if)#exit

Router(config)#interface fastEthernet 0/1

Router(config-if)#ip nat inside

Router(config-if)#exit

Создайте и настройте access-list (определяем трафик, который будем выпускать в Интернет):

Router(config)#ip access-list standard FOR-NAT

Router(config-std-nacl)#permit 192.168.1.0 0.0.0.255 (указываем сети)

Router(config-std-nacl)#exit

Router(config)#ip nat inside source list FOR-NAT interface fastEthernet 0/0 overload

Router(config)#end

Router#wr mem

Router#show running-config найдите в выведенных настройках строчки с созданным и настроенным access-list и занесите снимок экрана в отчет.

Проверьте доступность интерфейсов Router2 с PC0, т.е. возможность выхода в сеть Интернет с ПК центрального офиса. Для этого один раз нажмите левой кнопкой мыши на устройстве (PC0) и перейдите в закладку Desktop, а затем нажмите на Command Prompt (рисунок 4) и введите команду:

C:\>ping 210.210.1.1

Занесите снимок экрана в отчет.

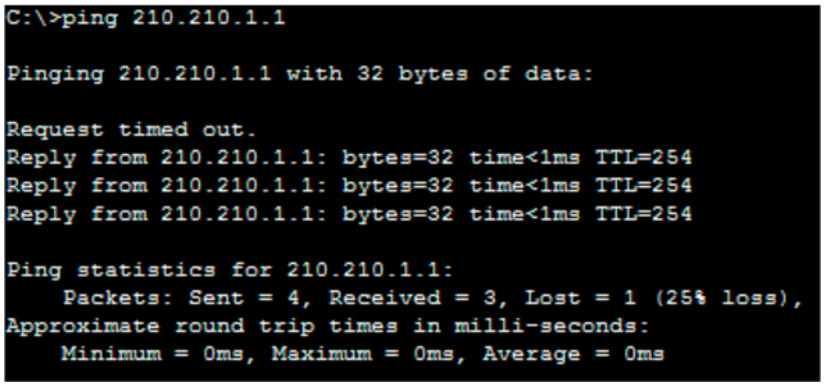


Рисунок 4 - Проверка доступности Интернета из центрального офиса

Маршрутизатор Интернет провайдера доступен, следовательно, NAT настроен верно.

Повторите настройки NAT для маршрутизатора филиала с необходи-мым изменением IP-адресов, а также проверьте связность PC2 с Router2 (IP-адрес 210.210.2.1) и занесите снимок экрана в отчет.

Содержание отчета

В индивидуальном отчёте должны быть указаны цель, задание, краткое описание лабораторного стенда, представлены необходимые снимки экрана и пояснения к ним. Следует проанализировать полученные данные и дать от-веты на контрольные вопросы.

Контрольные вопросы

1. Опишите порядок выполнения практической работы

2. Как производится настройка маршрутизатора центрального офиса?

3. Как производится настройка маршрутизатора провайдера?

4. Как производится настройка NAT для роутеров?

5. Что обозначает команда Router>enable при настройке маршрутизатора?

6. Что обозначает команда Router(config)#ip route при настройке маршрути-затора?

7. Как вы определили в процессе выполнения данной практической работы, что NAT настроен правильно?

8. Как вывести информацию по проведенным настройкам Router0?

9. Приведите примеры частных IP- адресов?

10. Опишите преимущества технологии NAT.

Практическое задание №15. Работа в физическом пространстве

Симулятор, как следует из названия, осуществляет только имита-цию 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 телекоммуника-ционный шкаф.

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

Города (Cities). Этот слой включает здания и телекоммуникацион-ные шкафы. По умолчанию город называется «Домашний город» **(Home City)**. Домашний город может быть передвинут и размещен в любом ме-сте 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 стан-дартное название «Главный телекоммуникационный шкаф» **(Main Wiring Closet)** и не имеет никаких других подразделений.

Физическое перемещение устройства

Все устройства, задействованные в логическом пространстве, раз-мещаются в главном телекоммуникационном шкафе. В этом разделе мы изучим как перемещать их.

1) Создайте схему сети в логическом рабочем пространстве, состоя-щую 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 рас-стоянию. Соедините компьютеры между собой и присвойте им IP-адреса из одной подсети.

2) Переключитесь на физический вид и нажмите кнопку «Новый го-род» **(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 со-здайте новый телекоммуникационный шкаф.

3) Используя кнопку «Навигация» **(Navigation)**, перейдите к глав-ному телекоммуникационному шкафу **Home City→ Corporate Office→ Main Wiring Closet.** В нем находятся оба ПК, которые мы разместили на логическом рабочем пространстве (рисунок 1).

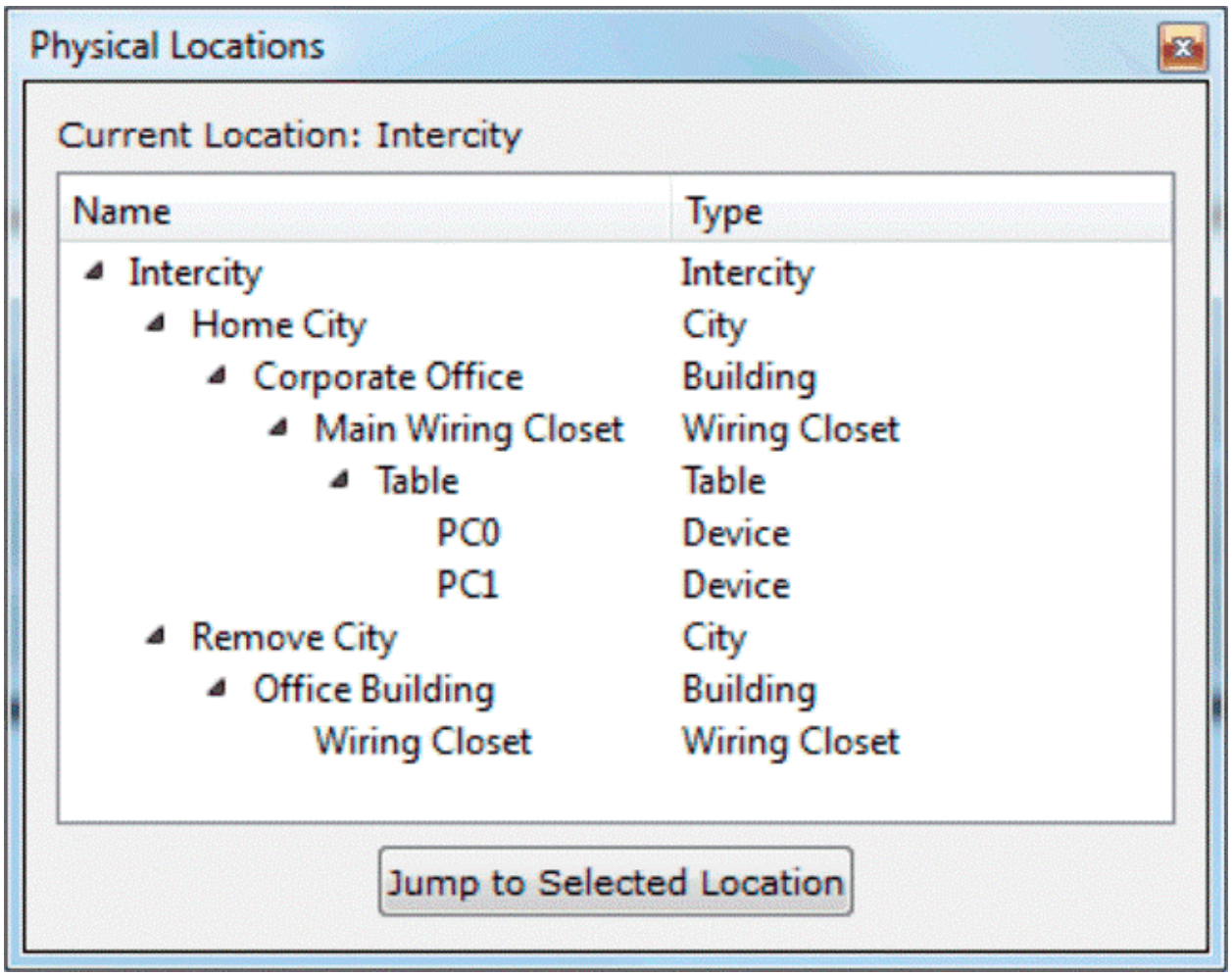


Рисунок 1 – Перемещение между объектами физического рабочего пространства

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

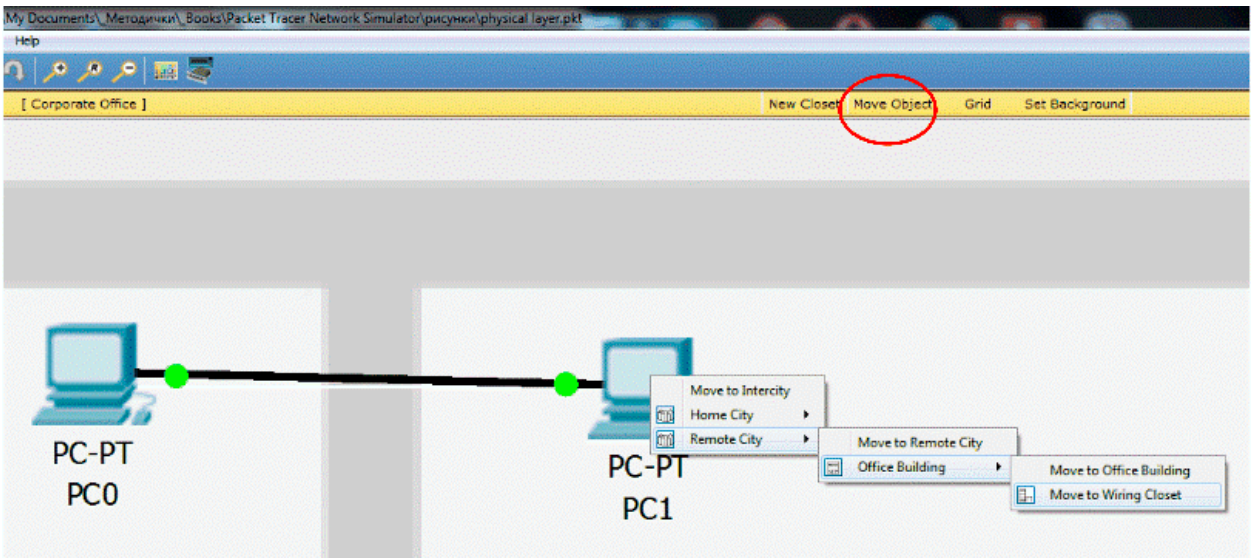


Рисунок 2 – Перемещение объектов на физическом плане

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 пере-мещены на любой уровень: междугородный, городской, здание и теле-коммуникационный шкаф. При этом их изображения буду находится 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 вос-требована для размещения беспроводных устройств.

Измерение длины кабельной линии

Измерение длины кабеля производится размещением указателя мыши над кабелем (рисунок 3).

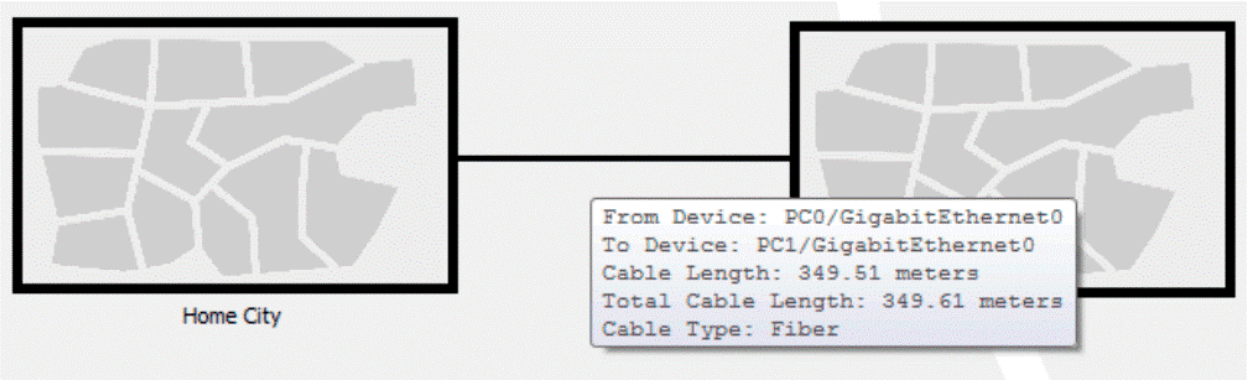


Рисунок 3 – Измерение длины кабельной линии

Стандартный медный кабель можно использовать для подключе-ния устройств, размещенных на расстоянии не более 100 м. Давайте убе-димся в этом.

1) Создайте такую, же как и прежде, схему сети из двух компьюте-ров, 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 расстоя-ние между устройствами. Если дистанция меньше 100 м, отодвиньте устройства подальше друг от друга, пока дистанциями между ними не превысит 100 м.

4) Вернитесь на логический план и вы обнаружите выключенное со-стояние портов с обоих сторон (красный цвет индикатора), т. к. соедине-ние между устройствами нарушено из-за превышения максимального расстояния между устройствами для данного типа кабеля (Примечание: в некоторых версиях Packet Tracer может потребоваться сброс по пита-нию **(**кнопка **Power Cycle Devices** в нижней

части программы**)**).

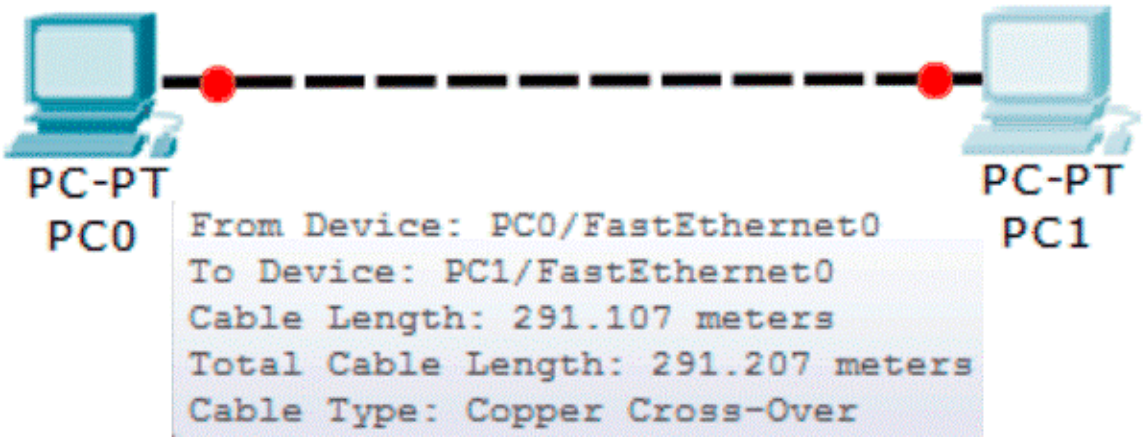


Рисунок 4 – Превышение максимальной длины кабеля

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

6) Перейдите на физический план в главный телекоммуникацион-ный 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 повтори-телей, т. к. витая пара по-прежнему имеет ограничение максимального расстояния 100 м).

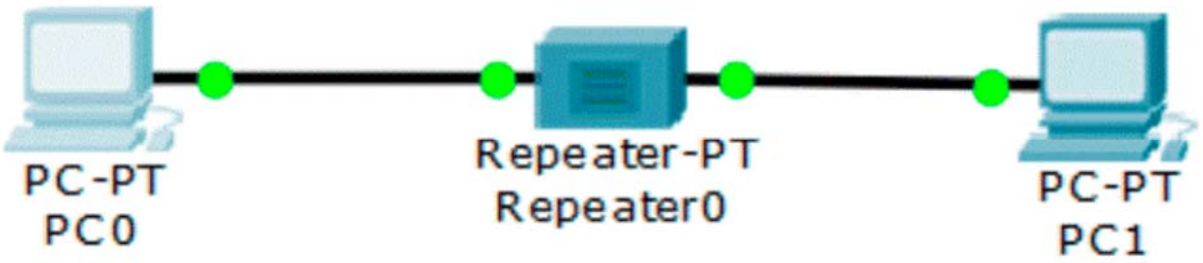


Рисунок 5 – Подключение повторителя

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. Физи-ческое рабочее пространство Packet Tracer имеет возможность, которая разрешает использовать цветовую расцветку кабелей.

Для цветового кодирования кабеля кликните на проводе в физиче-ском рабочем пространстве, выберите пункт меню «Цвет кабеля» **(Color Cable)** и подберите цвет в диалогом окне «Выбор света» **(Select Color)**. Результат представлен на рисунке 46 (Примечание: для получения ана-логичного вида может потребоваться перемещение устройства на уро-вень корпоративного офиса).

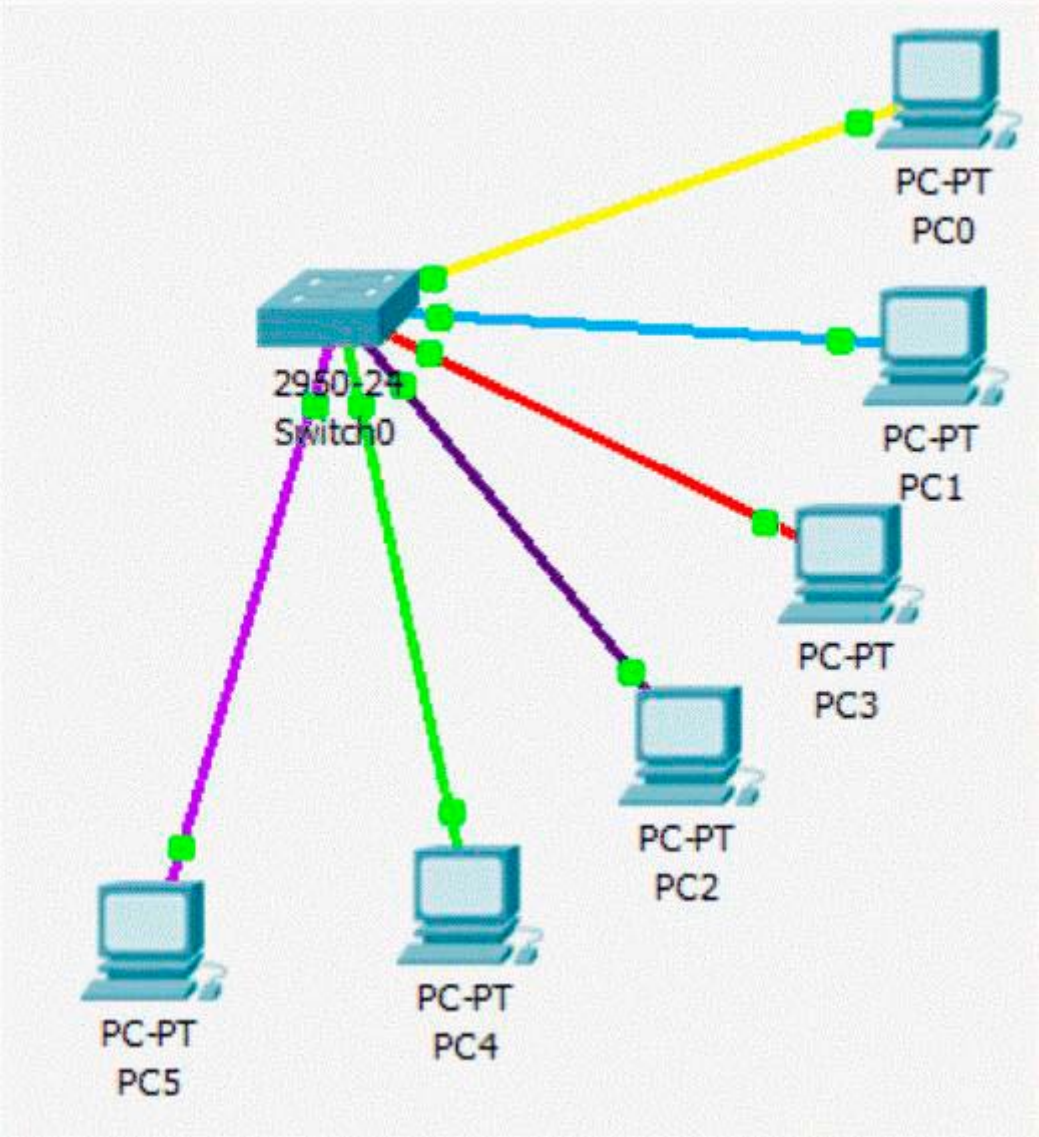


Рисунок 6 – Цветовая расцветка кабеля

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 ко-личество точек перегиба (рисунок 47)

В дополнение точки перегиба позволяют объединить несколько ка-белей 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. Появивше еся контекстное меню позволяет извлечь из группы одну точку или раз-группировать все сразу. При разгруппировке удаляется только объеди-нение точек в группу, сами точки перегиба остаются без изменений.

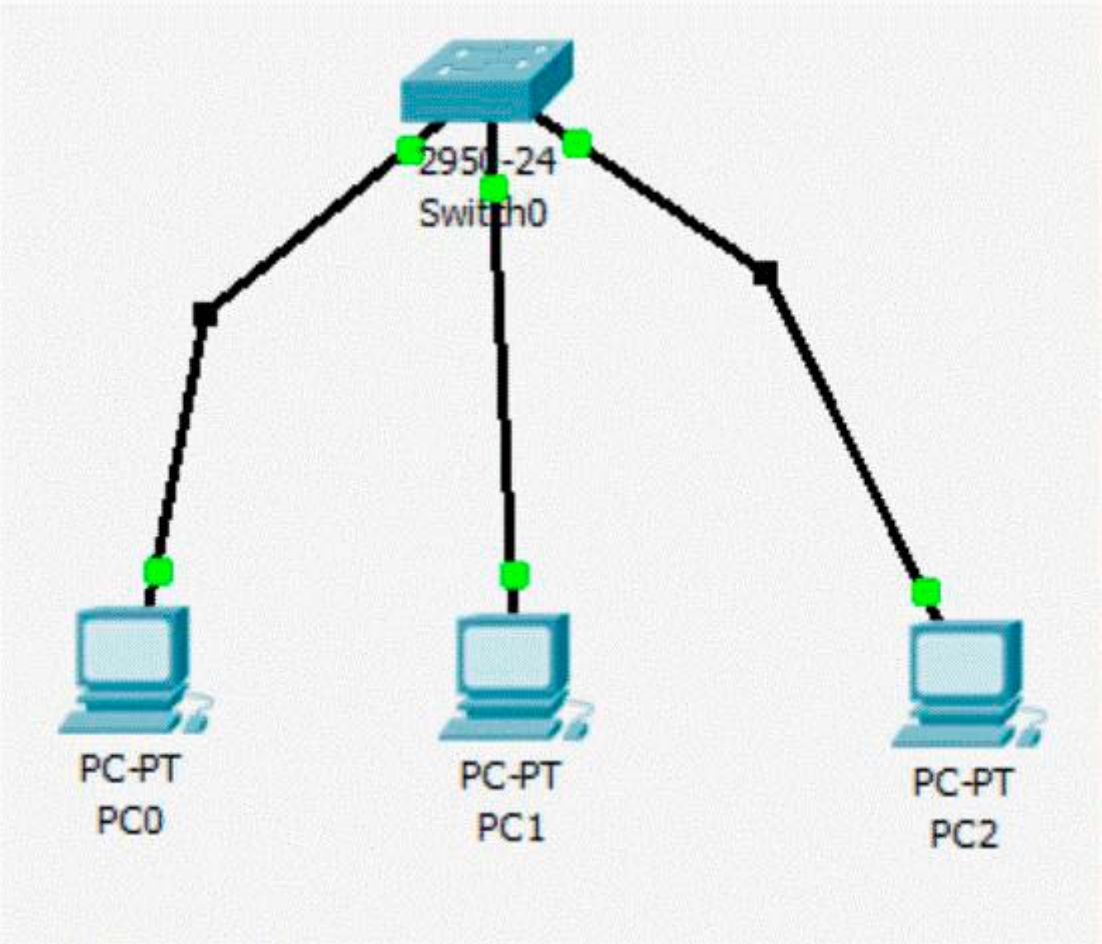


Рисунок 7 – Создание точек перегиба

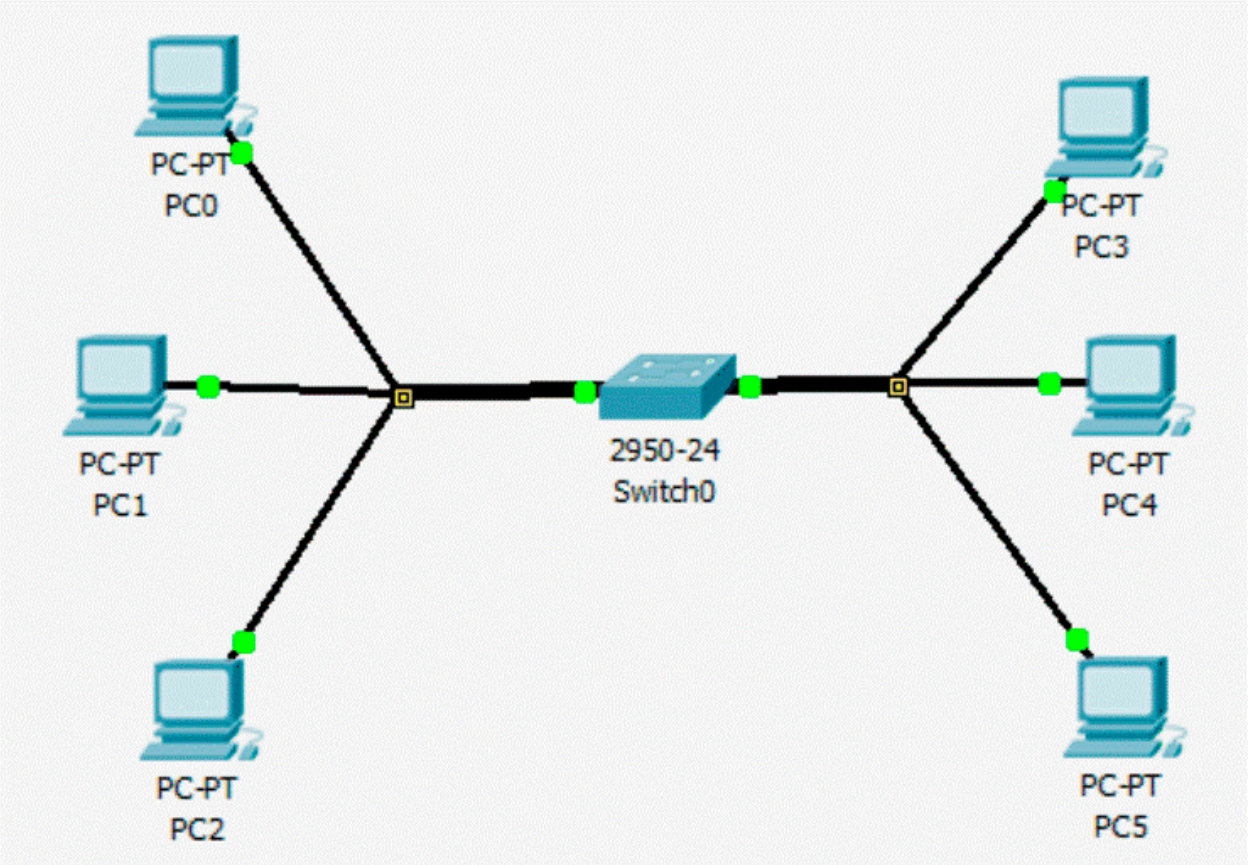


Рисунок 8 – Группировка точек перегиба

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 9).

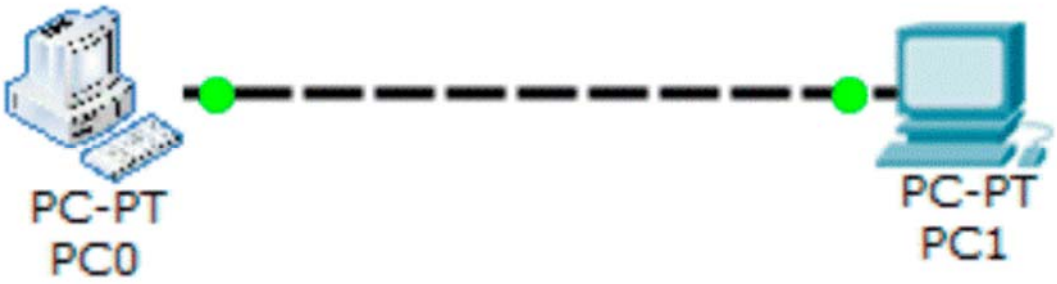


Рисунок 9 – Изменение стандартного изображения

Изменения изображения на физическом уровне становится види-мым только при перемещении устройств за пределы телекоммуникаци-онного шкафа.

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

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

Вывод

В этой главе мы изучили физическое рабочее пространство, что по-может вам задействовать множество новых возможностей при исполь-зовании беспроводных устройства. Кастомизация изображений и фона не только не только улучшает эстетику, но также помогает провести дифференциацию между устройствами, принадлежащими к разным ор-ганизациям. В следующей главе, мы сфокусируемся больше на межсете-вом взаимодействие Cisco-устройств, объяснив принципы IP-

маршрути-зации, работу статической маршрутизации и динамических протоколов. Режим имитации здесь очень пригодится для того, чтобы увидеть, как все это работает.

Задание

1 Настроить два офиса на уровне физического пространства (Практическая работа 11. Часть 2. Практическая работа 14)

2 Отчет с снимками экрана

Практическое задание №16. Сетевые службы

Цель работы

Изучить и практически освоить процесс настройки технологии DHCP и DNS.

Задание

1. Ознакомиться основными функциями технологии DHCP, DNS .

2. Запустить Cisco Packet Tracer.

3. Собрать необходимую топологию сети, запустить и настроить вирту-альное оборудование.

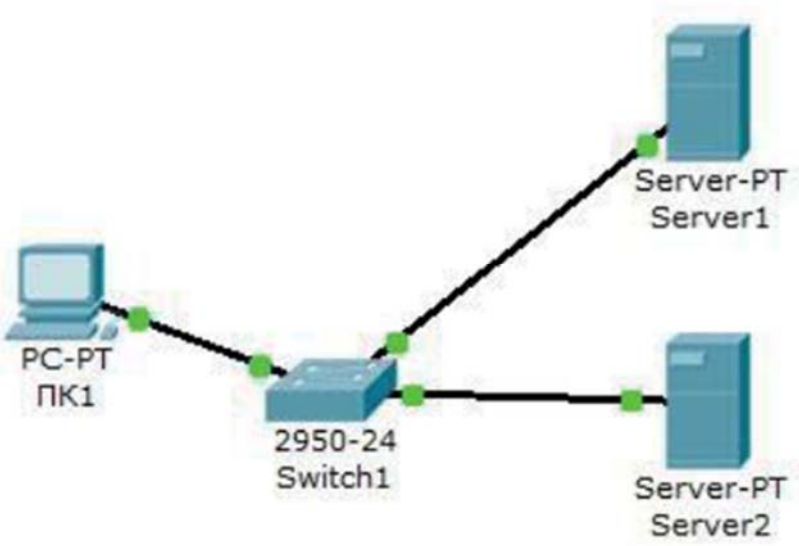
4. Согласно пунктам выполнения лабораторной работы, сделать необходимые снимки экрана. Изучить полученную информацию и оформить ее в соответствии с требованиями раздела Содержание отчета.

5. Ответить на контрольные вопросы.

Порядок выполнения работы

Эмулятор Cisco Packet Tracer позволяет проводить настройку таких сетевых сервисов, как: HTTP, DHCP, TFTP, DNS, NTP, EMAIL, FTP в составе серверасети. Рассмотрим настойку некоторых из них.

Создайте следующую схему сети, представленную на рис. 1:



Задача:

Настроить сеть следующим образом:

1 - Server1 – DNS и Web сервер;

2 - Server2 – DHCP сервер;

3 - Компьютер ПК1 получает параметры протокола TCP/IP с DHCP сервера и открывает сайт www.rambler.ru на Server1.

Этап 1.

Задайте параметры протокола TCP/IP на ПК1 и серверах.

Войдите в конфигурацию ПК1 и установите настройку IP через DHCP сервер рис..2.

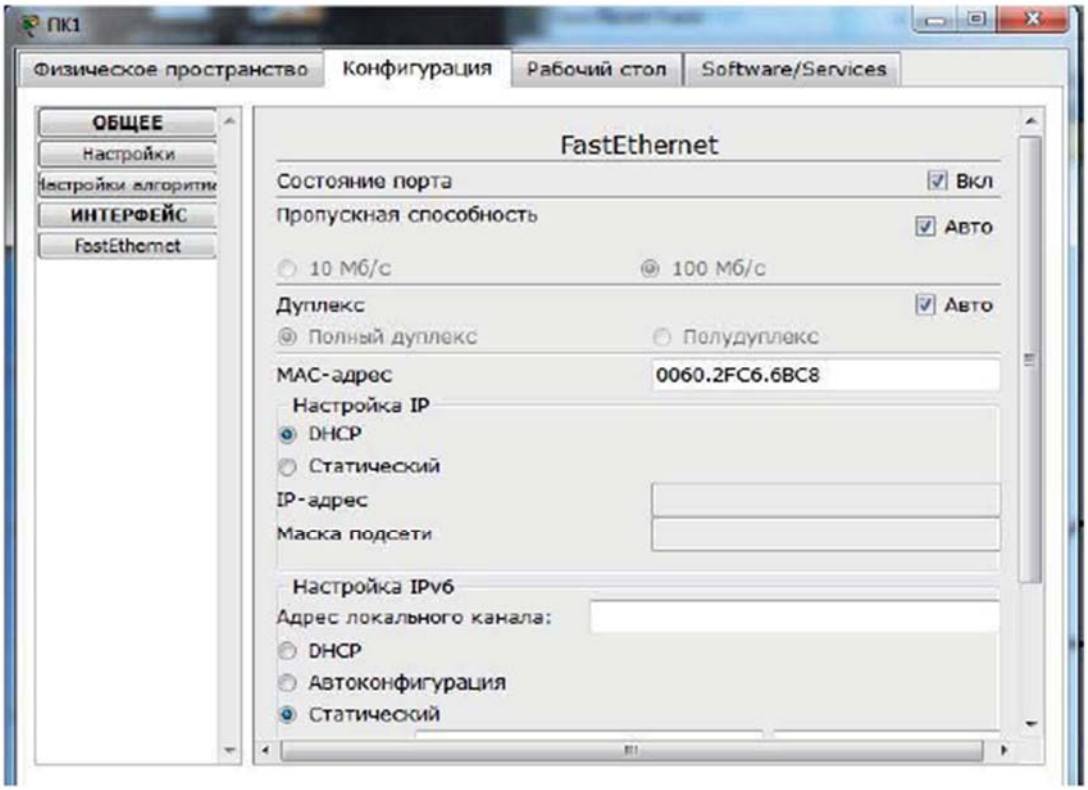


Рис. 2. Настройка IP на ПК1.

Задайте в конфигурации серверов следующие настройки IP:

Server1: IP адрес – 10.0.0.1, маска подсети – 255.0.0.0

Server2: IP адрес – 10.0.0.2, маска подсети – 255.0.0.0

Этап 2. Настройте службу DNS на Server1.

Для этого в в конфигурации Server1 войдите на вкладку DNS и задайте две ресурсные записи в прямой зоне DNS:

1 – в ресурсной записи типа A свяжите доменное имя компьютера с его IP адресом рис.3 и нажмите кнопку ДОБАВИТЬ:

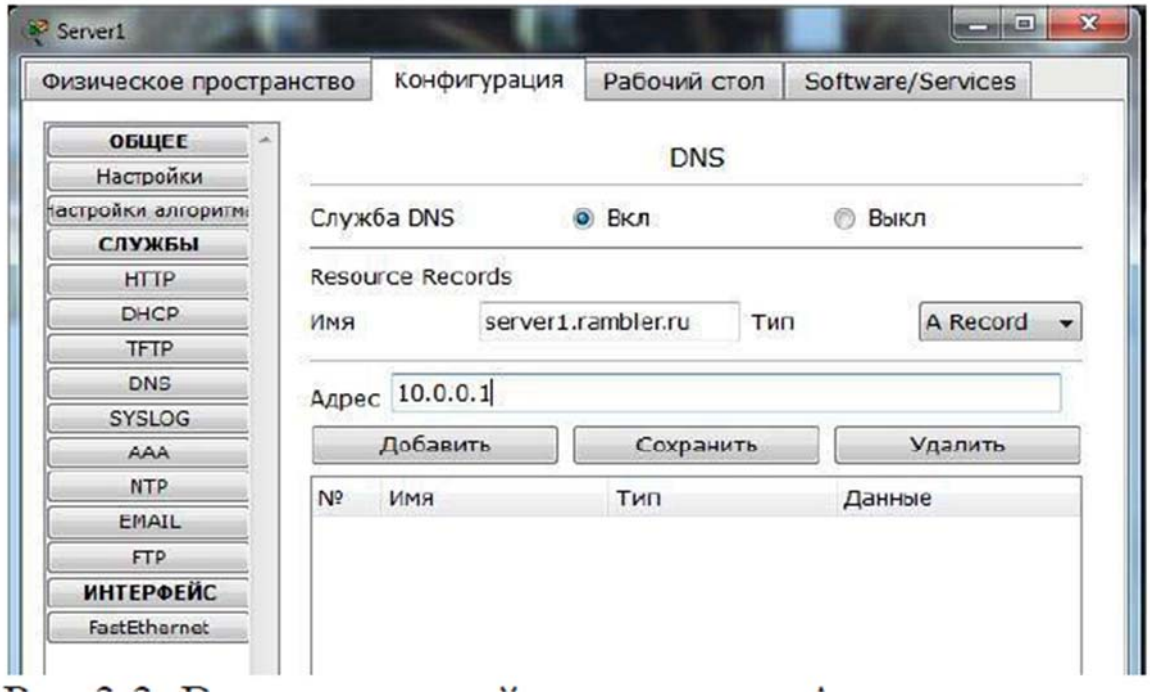
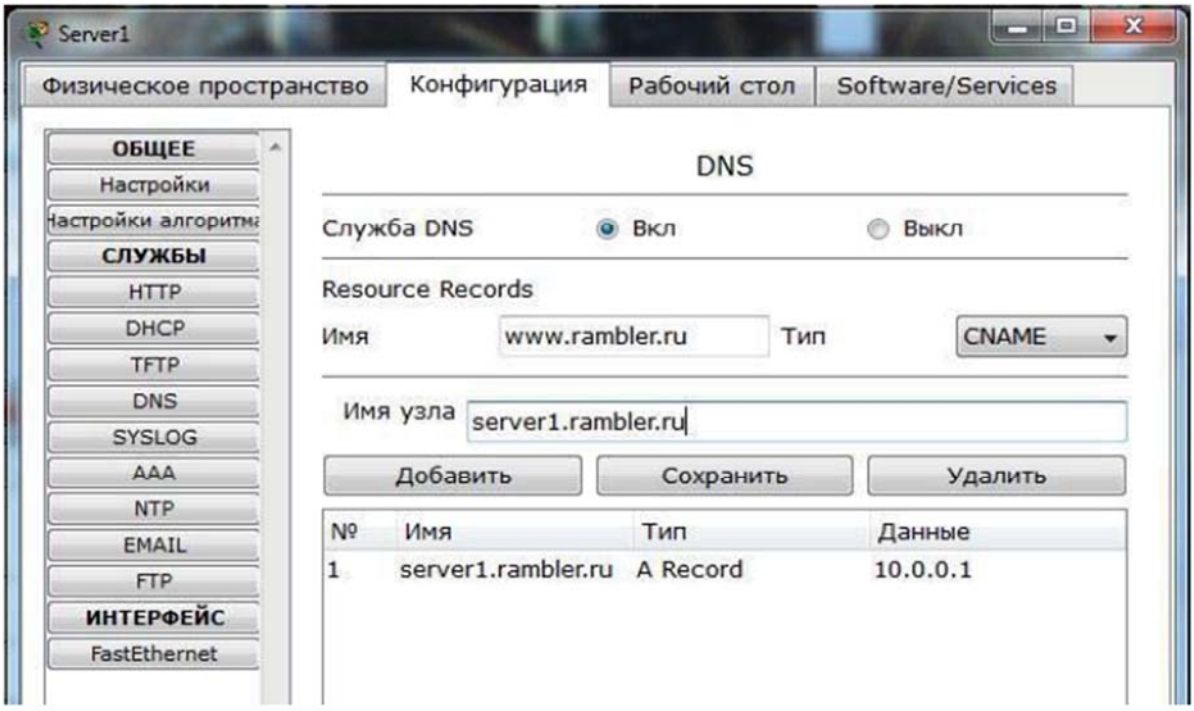


Рис.3. Ввод ресурсной записи типа A (исправить на www.rambler.ru).

2 – в ресурсной записи типа CNAME свяжите псевдоним сайта с компьютером (рис.4):



(исправить на www.rambler.ru)

Рис.4. Ввод ресурсной записи типа CNAME.

В конфигурации Server1 войдите на вкладку HTTP и задайте стартовую страницу сайта WWW.RAMBLER.RU (рис.5):

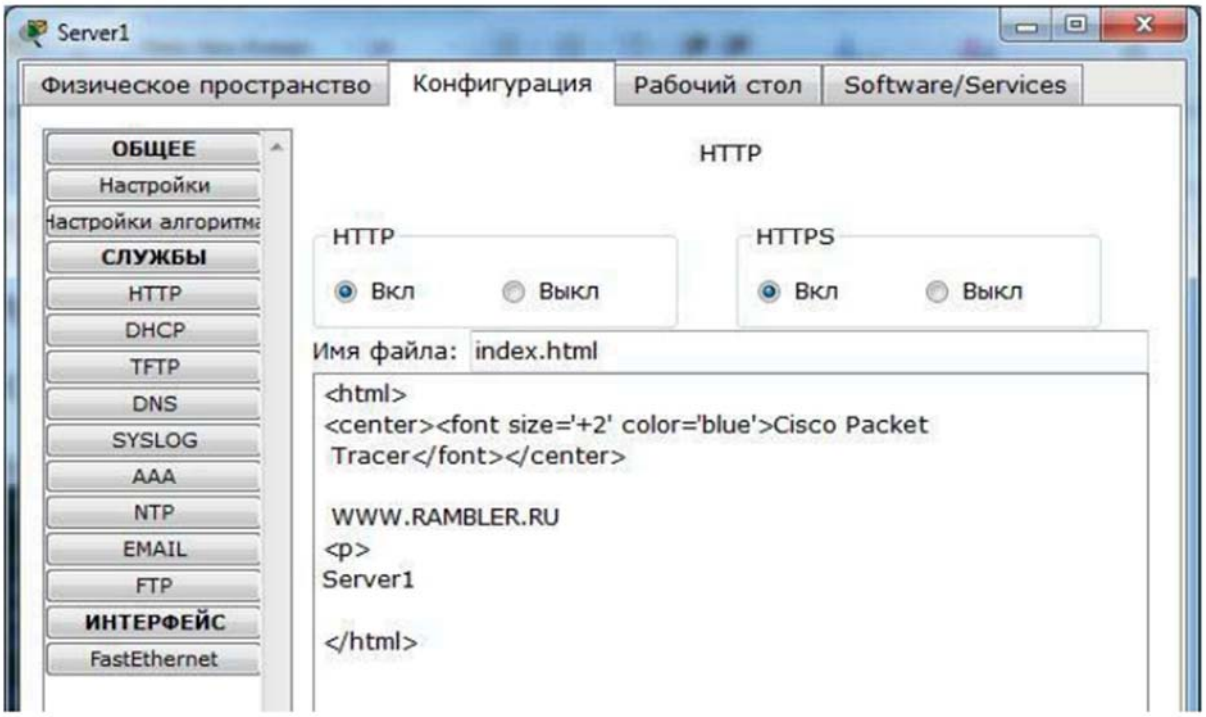


Рис.5. Стартовая страница сайта.

Включите командную строку на Server1 и проверьте работу службы DNS. Для проверки прямой зоны DNS сервера введите команду

SERVER>**nslookup** **www.rambler.ru**

Если все правильно, то вы получите отклик, представленный на рис.6, с указанием полного доменного имени DNS сервера в сети и его IP адрес.

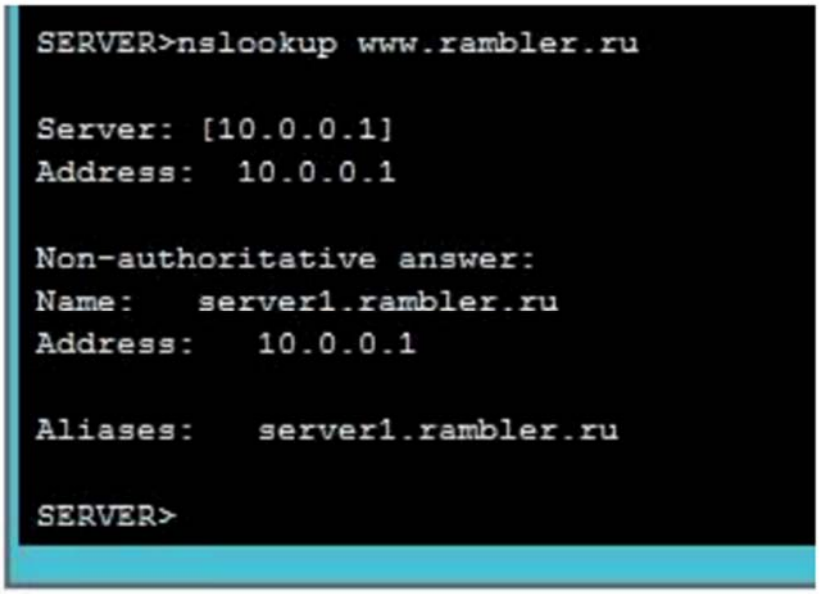


Рис .6. Проверка прямой зоны DNS.

Этап 3. Настройте DHCP службу на Server2.

Для этого войдите в конфигурацию Server2 и на вкладке DHCP настройте службу (рис.7):

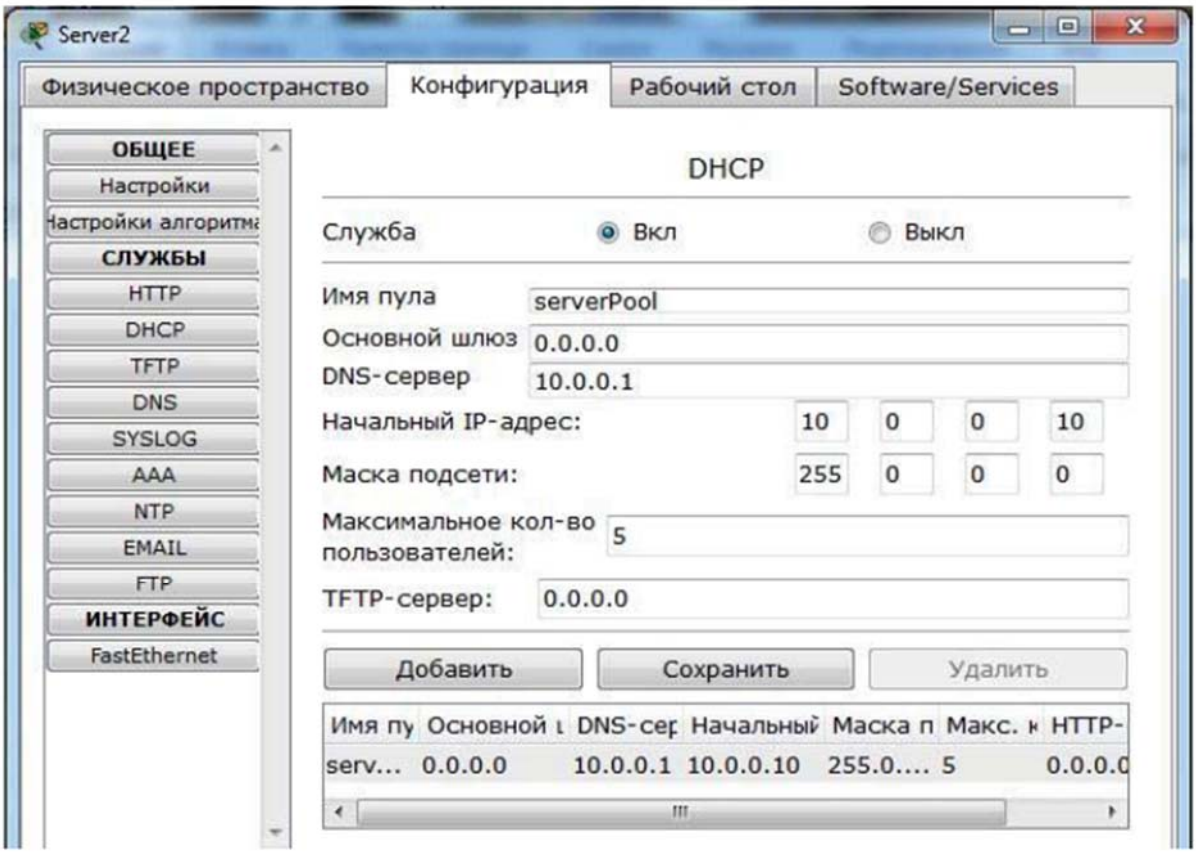


Рис. 7. Настройка DHCP сервера.

Этап 3. Проверка работы клиента.

Войдите в конфигурации хоста ПК1 на рабочий стол и в командной строке сконфигурируйте протокол TCP/IP.

Командой

PC>**ipconfig /release**

сбросьте старые параметры IP адреса, а командой:

PC>**ipconfig /renew**

получите новые параметры с DHCP сервера (рис.8):

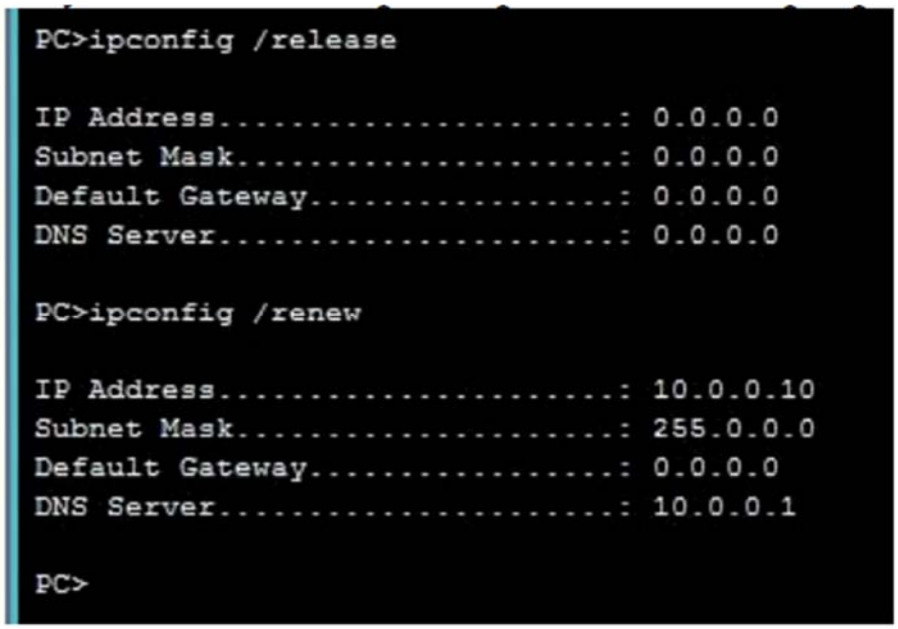


Рис.8. Конфигурация протокол TCP/IP клиента.

Откройте сайт WWW.RAMBLER.RU в браузере на клиенте (рис.9):

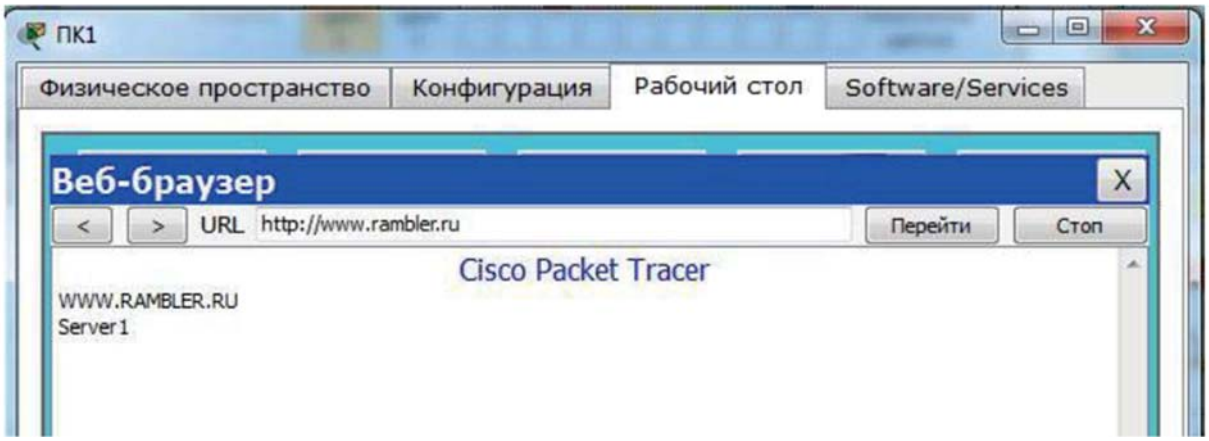


Рис.9. Проверка работы клиента.

Контрольные вопросы.

1. Что такое рекурсивный запрос DNS и какова схема его работы?

2. Укажите назначение типов ресурсных записей в прямой и обратной зонах DNS.

3. Как на DNS сервере настраивается пересылка пакетов на другие DNS сервера?

4. Опишите работу службы DHCP.

5. Как настраивается клиент DHCP?

6. Укажите местоположения папки с контентом Web узла и FTP сервера.

7. Как определяется состав обратных зон DNS сервера в корпоративной сети.

8. Продемонстрируйте настройку служба DNS в Cisco Paket Tracer?

9. Продемонстрируйте настройку служба DHCP в Cisco Paket Tracer?

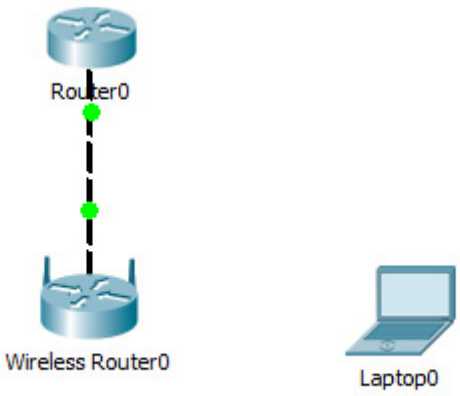
10. Продемонстрируйте настройку служба FTP в Cisco Paket Tracer?

11. Продемонстрируйте настройку WEB сервер в Cisco Paket Tracer?

Практическое задание №17. Знакомство со стандартами wi-fi. Изучение способов использования wi-fi (маршрутизация и точка доступа);

Создание модели

Создать модель локальной сети, состоящей из обычного домашнего wi-fi роутера и маршрутизатора, который имитирует провайдера Интернета. Использовать интерфейс Fast Ethernet. Добавим ещё пользовательское устройство, например ноутбук. Установим модуль wi-fi (WPC300N) в ноутбук.



Настройка модели

1)Настройки маршрутизатора провайдера **Router0** (жирным выделено то, что необходимо ввести с клавиатуры:

Router>**en**

Router#

Router#**conf t**

Enter configuration commands, one per line. End with CNTL/Z.

Router (config)**#int fa0/0**

Router (config-if)**#ip address 210.210.0.1 255.255.255.252**

Router (config-if)**#no shutdown**

Router (config-if)#

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Router (config-if)**#end**

Router#

%SYS-5-CONFIG_I: Configured from console by console

Router#**wr** **mem**

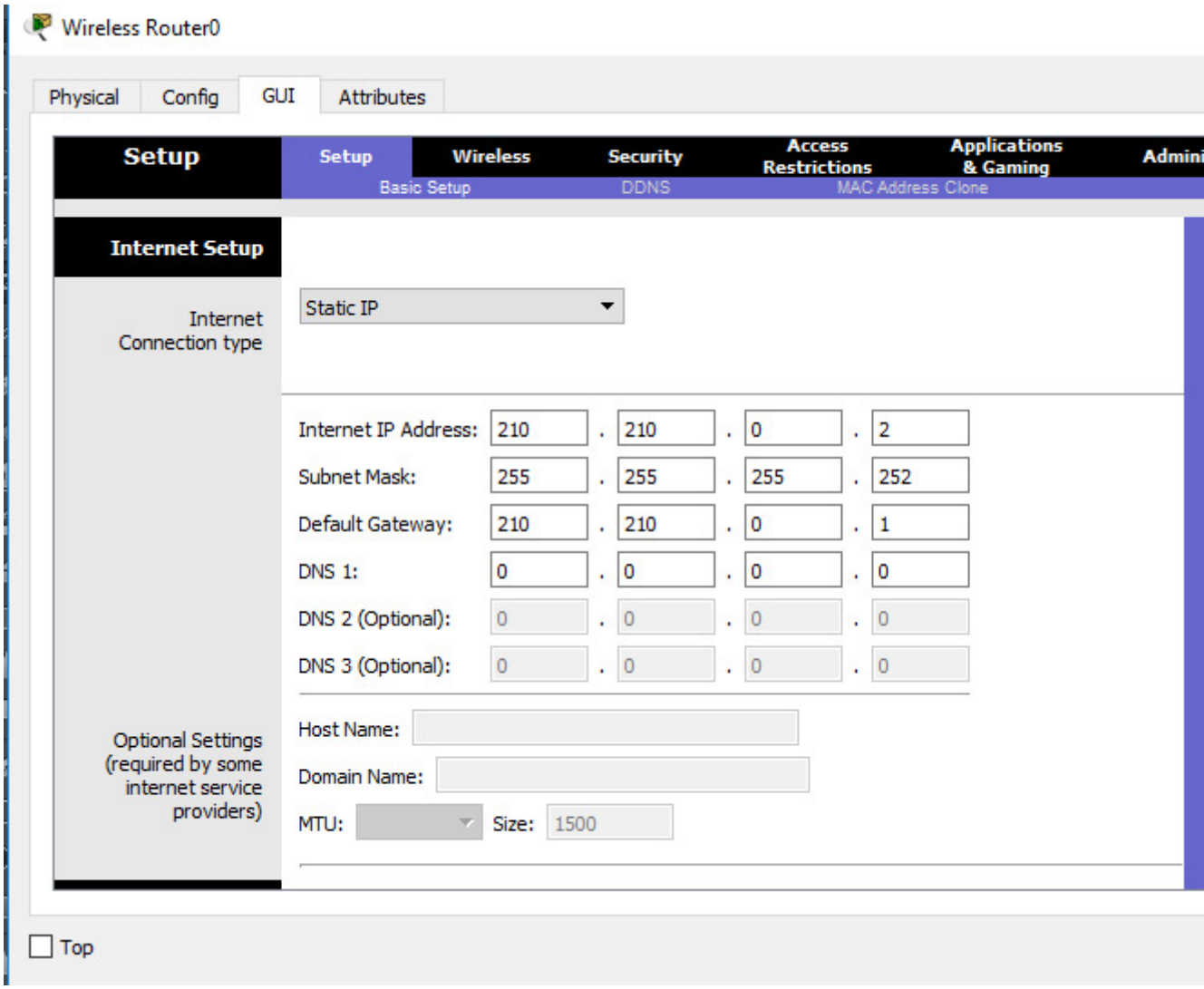
Building configuration…

[OK]

2)Настройки домашнего wi-fi маршрутизатора **Wireless Router0**

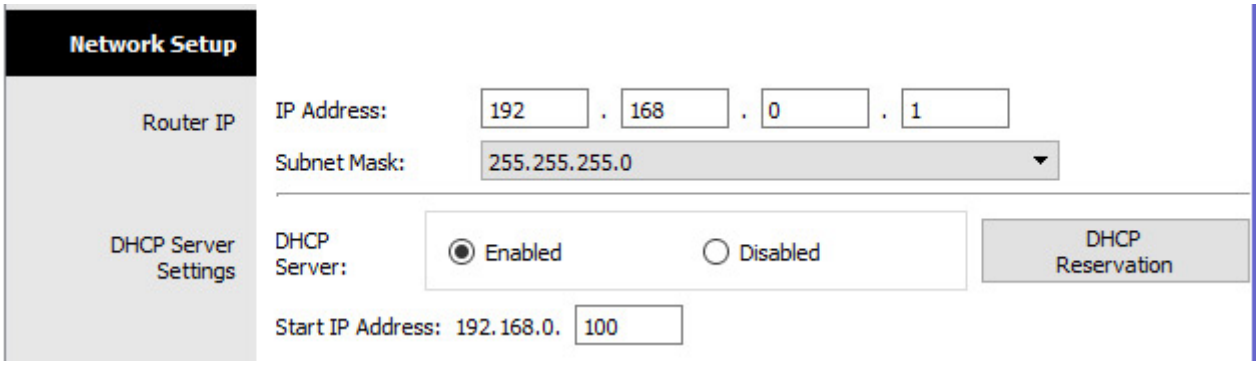
выполняется с помощью веб интерфейса.

Настройка внешнего интерфейса во вкладке Setup показана на рисунке.

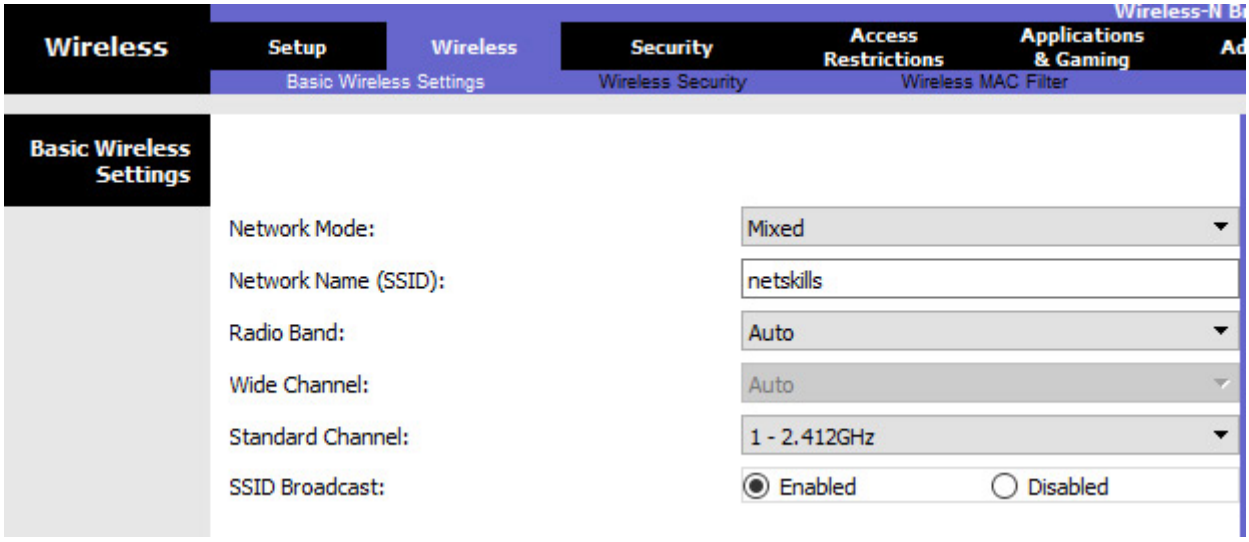


Настройка локальной сети (Network Setup)

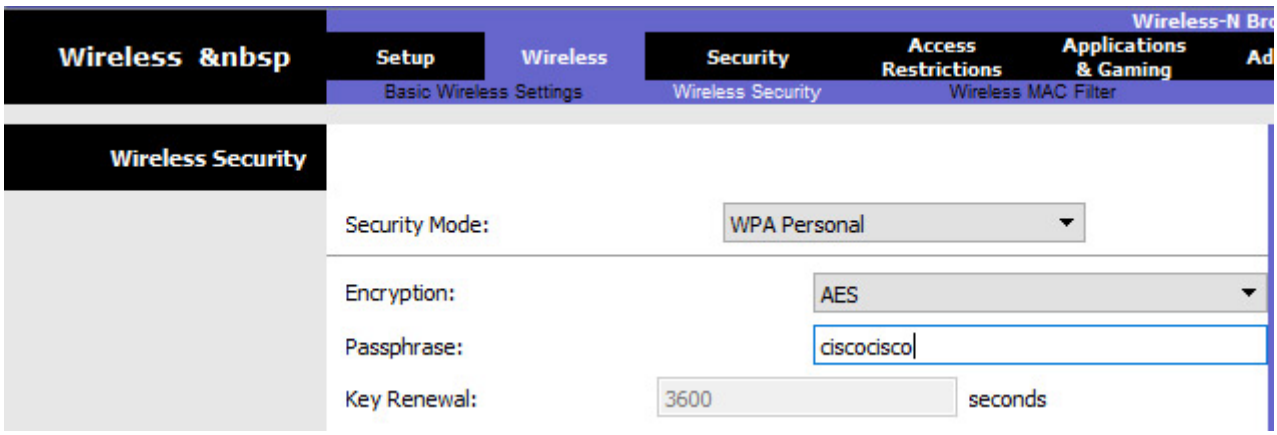
Выбираем по умолчанию ip-адрес 192.168.0.1, маска 24-битная 255.255.255.0, разрешён DHCP-сервер, начало раздачи с адреса 192.168.0.100 и всё. После чего незабываем сохранить настройки, нажать на кнопку внизу формы Save Settings.



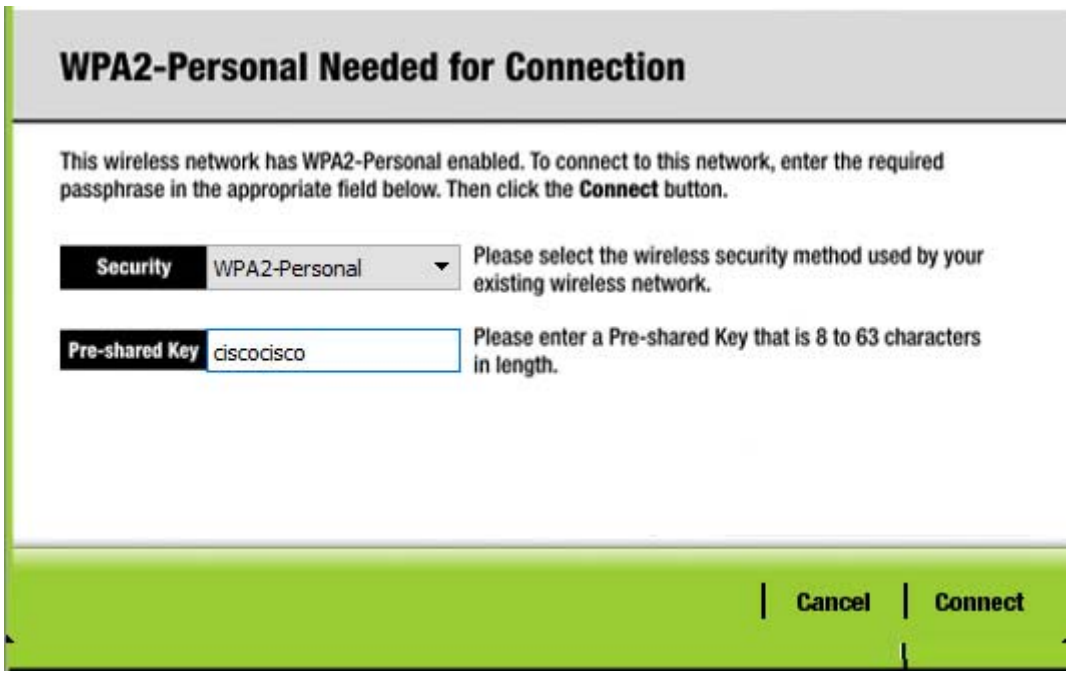
Настройки во вкладке Wireless, т.е. wi-fi. Выбираем основные настройки вайфая: режим (mode), мы выбираем смешанный (mixed); идентификатор сети (SSID) — netskills; ширина канала (Radio Band) — auto; частоту — 1-2.412HGz; видимость сети (SSID Broadcast) — видимая (enable). Сохраняем настройки.



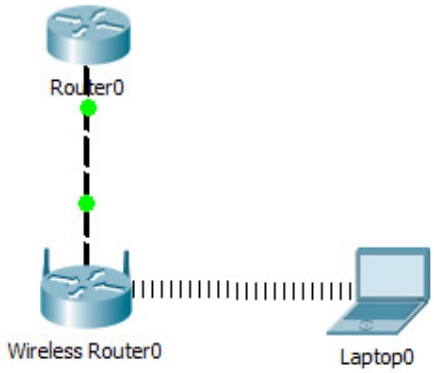
Переходим ко вкладке Wireless Security. Выбираем режим шифрования WPA2 Personal, алгоритм шифрования AES, ключевое слово для выбранного режима шифрования не менее 8 символов. Сохраняем.



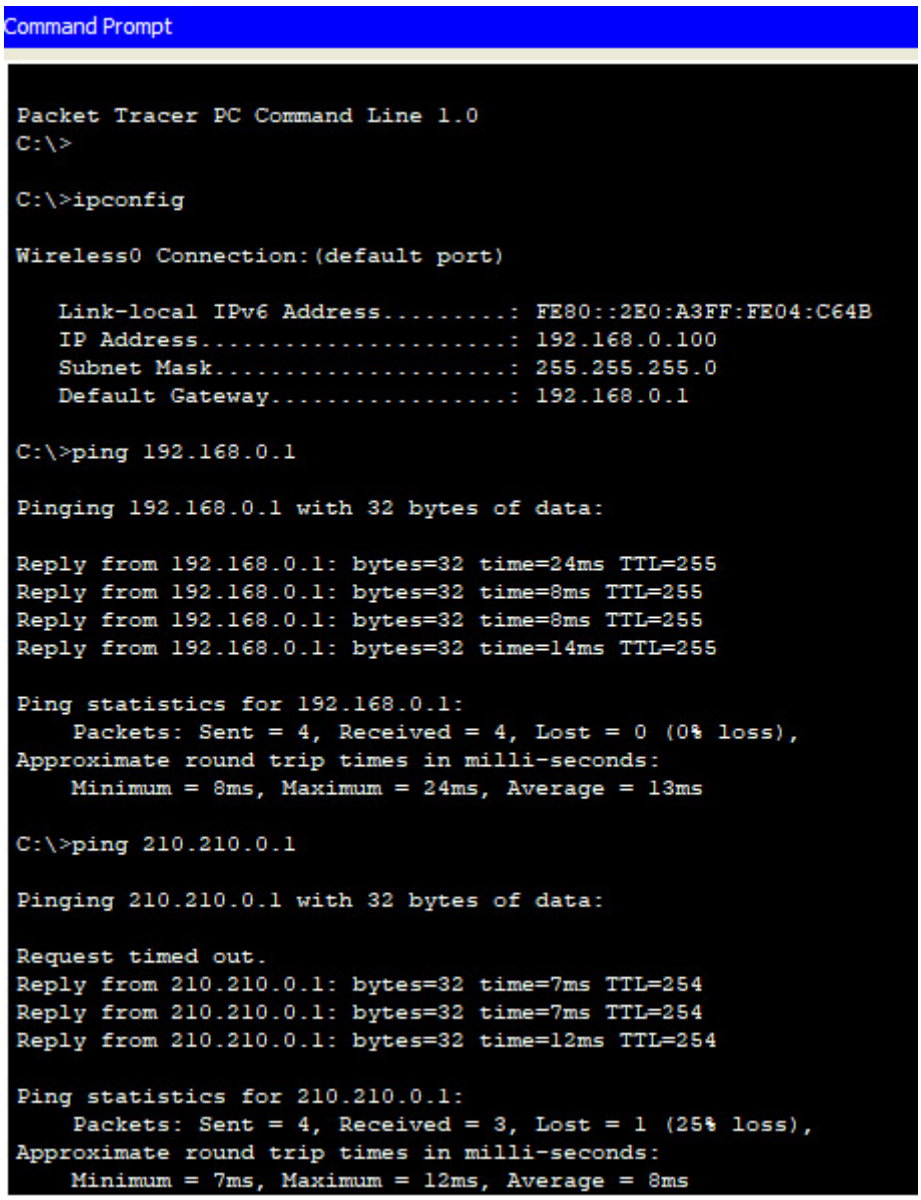
3)Настройка wi-fi адаптера на ноутбуке. Вкладка Desktop->PC Wireless->Connect. Смотрим доступные нам сети. Нажимаем кнопку Connect для подключения к сети netskills.



Если настройки произведены верно, то появиться пунктирная линия между wi-fi маршрутизатором и ноутбуком как на рисунке.



Введём на ноутбуке в командной строке команду **ipconfig**, чтобы проверить правильность настроек. Из рисунка видно, что DHCP- сервер присвоил правильный ip **192.168.0.100** Пропингуем шлюз (wi-fi маршрутизатор) и пропингуем адрес интернет провайдера. На рисунке видно, что в обоих случаях пинг идёт.



При этом NAT мы не использовали, так как практически на всех wi-fi маршрутизаторах NAT используется по умолчанию.

Список используемой литературы

1. Cisco ICND 1. Руководство для студента. Изд. Cisco, 2022
2. Аксенов А. Н. «Проектирование и анализ вычислительных сетей в программном продукте Cisco Packet Tracer.». М.: Бука, 2021.
3. Амато В. Ос новы организации сетей Cisco. Том 1. - С.-П.: Вильямс, 2002.
4. Амато В. Основы организации сетей Cisco. Том 2. - С.-П.: Вильямс, 2002.
5. Боллапрагада В., Мёрфи К., Уайт Р. Структура операционной системы Cisco IOS. С.-П.: Вилямс, 2022.
6. Бони Д. Руководство по Cisco IOS. - С.-П.: Питер, Русская Редакция, 2018.
7. Димарцио Д. Ф. Маршрутизаторы CISCO. Пособие для самостоятельного изучения. - С.-П.: Символ-Плюс, 2003.
8. Знакомство с Cisco Packet Tracer // https://litl- admin.ru/cisco/znakomstvo-s-cisco-packet-tracer.html.
9. Иванов С.Ю. Маршрутизаторы Cisco. Пособие для самостоятельного изучения. - М.: Символ-Плюс, 2013.
10. Кеннеди К., Гамильтон К. Принципы коммутации в локальных сетях Cisco. - М.: Вильямс, 2023.
11. Командная строка управления устройствами CLI. Виртуальные локальные сети VLAN //https://www.intuit.ru/studies/ courses/3 549/791 /lecture/29219.
12. Леинванд А., Пински Б. Конфигурирование маршрутизаторов Cisco. - С.-П.: Вильямс, 2022.

Лист регистрации изменений и дополнений ФОС по профессиональному модулю
ПМ 01 Выполнение работ по проектированию сетевой инфраструктуры

№ изме-нения	Номера листов		Основания для внесения изменений	Дата	№ протокола педсовета	Дата введения изменений	Подпись	Расшифровка подписи
	Замененных	Новых						