Санкт-Петербургское государственное бюджетное
профессиональное образовательное учреждение
«Академия управления городской средой, градостроительства и печати»

ПРИНЯТО

на заседании педагогического совета
Протокол № 2
«26» 12 2023 г.

УТВЕРЖДАЮ

Директор СПб ГБПОУ «АУГСГиП»
_____ А.М. Кривоносов
«___» _____ 2023 г.

КОМПЛЕКТ КОНТРОЛЬНО-ОЦЕНОЧНЫХ СРЕДСТВ

по текущему контролю успеваемости
и промежуточной аттестации
по профессиональному модулю
ПМ.01 НАСТРОЙКА СЕТЕВОЙ ИНФРАСТРУКТУРЫ

по специальности
09.02.06 Сетевое и системное администрирование

Квалификация
Системный администратор

Форма обучения
очная

Санкт-Петербург
2023 год

Комплект контрольно-оценочных средств по профессиональному модулю ПМ.01 Настройка сетевой инфраструктуры разработан на основе Федерального государственного образовательного стандарта по специальности 09.02.06 Сетевое и системное администрирование, утвержденного приказом Министерства Просвещения РФ от 10 июля 2023 г. № 519.

СОГЛАСОВАНО
ООО «ДЖИ-ТИ ИНВЕСТ»
Генеральный директор
_____ П.С. Тюганов
«26» 12 2023 г.

Комплект контрольно-оценочных средств по профессиональному модулю рассмотрен на заседании методического совета СПб ГБПОУ «АУГСГиП»

Протокол № 2 от «29» 11 2023 г.

Комплект контрольно-оценочных средств по профессиональному модулю рассмотрен на заседании цикловой комиссии общетехнических дисциплин и компьютерных технологий

Протокол № 4 от «21» 11 2023 г.

Председатель цикловой комиссии: Караченцева М.С. _____

СОДЕРЖАНИЕ

1. Паспорт комплекта оценочных средств

Результатом освоения профессионального модуля является готовность обучающегося к выполнению вида профессиональной деятельности «Выполнение работ по проектированию сетевой инфраструктуры» и составляющих его профессиональных компетенций, а также общих компетенций, формирующихся в процессе освоения ППССЗ в целом.

Комплект контрольно-оценочных средств позволяет оценивать:

1. Освоение профессиональных компетенций (ПК), соответствующих виду профессиональной деятельности, и общих компетенций (ОК):

№ ПК и ОК	Содержание компетенции
ПК 1.1.	Документировать состояния инфокоммуникационных систем и их составляющих в процессе наладки и эксплуатации
ПК 1.2.	Поддерживать работоспособность аппаратно-программных средств устройств инфокоммуникационных систем.
ПК 1.3.	Устранять неисправности в работе инфокоммуникационных систем.
ПК 1.4.	Проводить приемо-сдаточные испытания компьютерных сетей и сетевого оборудования различного уровня и оценку качества сетевой топологии в рамках своей ответственности.
ПК 1.5.	Осуществлять резервное копирование и восстановление конфигурации сетевого оборудования информационно-коммуникационных систем.
ПК 1.6	Осуществлять инвентаризацию технических средств сетевой инфраструктуры, контроль оборудования после проведенного ремонта.
ПК 1.7.	Осуществлять регламентное обслуживание и замену расходных материалов периферийного, сетевого и серверного оборудования инфокоммуникационных систем.
ОК 1.	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам;
ОК 2.	Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности;
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях;
ОК 4.	Эффективно взаимодействовать и работать в коллективе и команде;
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста;
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведе-

№ ПК и ОК	Содержание компетенции
	ния;
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях;
ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности;
ОК 9.	Пользоваться профессиональной документацией на государственном и иностранном языках.

2. Приобретение в ходе освоения профессионального модуля практического опыта:

Освоение практического опыта

Иметь практический опыт	Виды работ на учебной и/ или производственной практике и требования к их выполнению
– проектировании архитектуры локальной сети в соответствии с поставленной задачей; – установки и настройкие сетевых протоколов и сетевого оборудования в соответствии с конкретной задачей; – выбора технологии, инструментальных средств при организации процесса исследования объектов сетевой инфраструктуры; – обеспечения безопасного хранения и передачи информации в локальной сети; – использования специального программного обеспечения для моделирования, проектирования и тестирования компьютерных сетей.	Учебная практика 1. Проектирование сетевой инфраструктуры. 2. Администрирование сети 3. Настройка сетевых сервисов 4. Анализ использования и функционирования программно-технических средств компьютерных сетей 5. Инвентаризация технических средств сетевой инфраструктуры, осуществление контроля поступившего из ремонта оборудования 6. Проведение профилактических работ на объектах сетевой инфраструктуры и рабочих станциях. 7. Замена расходных материалов и мелкий ремонт периферийного оборудования, определение устаревшего оборудования и программных средств сетевой инфраструктуры Производственная практика 1. Общая характеристика организации. 2. Определение инструментальных средств и средств вычислительной техники для организации процесса работы организации 3. Защита информации в локальной сети организации с применением программно-аппаратных средств 4. Подбор оборудования (серверов, систем-

Иметь практический опыт	Виды работ на учебной и/ или производственной практике и требования к их выполнению
– проектировании архитекту-	Учебная практика
	ных блоков рабочих станций, сетевого оборудования программного обеспечения и т.д.) 5. Защита данных от несанкционированного доступа и уничтожения, в.т.ч. с использованием антивирусного программного обеспечения. 6. Удаление временных и ненужных файлов 7. Дефрагментация жестких дисков 8. Проведение диагностики аппаратного обеспечения и сетевого оборудования 9. Создание диска аварийного восстановления 10. Обеспылевание аппаратного обеспечения 11. Обучение пользователей по вопросам профилактики сбоев в работе оборудования 12. Выявление сбоев в работе оборудования 13. Восстановление работоспособности оборудования 14. Выявление устаревшего оборудования.

3. Освоение умений и усвоение знаний:

№	Освоенные умения, усвоенные знания
З1	общие принципы построения сетей, сетевых топологий, многослойной модели OSI, требований к компьютерным сетям;
З2	архитектуру протоколов, стандартизации сетей, этапов проектирования сетевой инфраструктуры;
З3	базовые протоколы и технологии локальных сетей;
З4	принципы построения высокоскоростных локальных сетей;
З5	стандарты кабелей, основные виды коммуникационных устройств, терминов, понятий, стандартов и типовых элементов структурированной кабельной системы;
У1	проектировать локальную сеть, выбирать сетевые топологии;
У2	использовать многофункциональные приборы мониторинга, программно-аппаратные средства технического контроля локальной сети;

Формой аттестации по профессиональному модулю является. Итогом экзамена является однозначное решение: «вид профессиональной деятельности освоен/не освоен».

2. Система контроля и оценки освоения программы ПМ.01 Выполнение работ по проектированию сетевой инфраструктуры

2.1. Формы промежуточной аттестации по ППССЗ при освоении профессионального модуля

Элементы модуля, профессиональный модуль	Формы промежуточной аттестации
МДК.01.01 «Компьютерные сети»	Комплексный экзамен
МДК.01.02 «Организация, принципы построения и функционирования компьютерных сетей»	Дифференцированный зачет
МДК 01.03 «Безопасность компьютерных сетей»	Комплексный экзамен
УП.01	Дифференцированный зачет
ПП.01	Дифференцированный зачет
ПМ.01	**Экзамен**

2.2. Организация контроля и оценки освоения программы ПМ

Итоговый контроль освоения вида профессиональной деятельности Выполнение работ по проектированию сетевой инфраструктуры осуществляется на экзамене. Условием допуска к экзамену является положительная аттестация по МДК, учебной практике и производственной практике.

Экзамен проводится в виде выполнения практического экзаменационного задания.

Условием положительной аттестации (вид профессиональной деятельности освоен) на экзамене квалификационном является положительная оценка освоения всех профессиональных компетенций по всем контролируемым показателям. При отрицательном заключении хотя бы по одной из профессиональных компетенций принимается решение «вид профессиональной деятельности не освоен».

Промежуточный контроль освоения профессионального модуля осуществляется при проведении экзаменов по МДК, дифференцированного зачета по учебной практике и зачета по производственной практике. Предметом оценки освоения МДК являются умения и знания. Экзамен по МДК проводится по заранее подготовленным и утвержденным экзаменационным вопросам. Условием положительной аттестации является получение обучающимся на экзамене оценки «удовлетворительно», «хорошо», «отлично».

Предметом оценки по учебной и производственной практике является освоение общих и профессиональных компетенций, умений. Контроль и оценка по учебной и (или) производственной практике проводится на основе Аттестационного листа обучающегося с места прохождения практики.

Текущий контроль по МДК осуществляется в форме выполнения практических проверочных заданий, устных зачетов.

3. Комплект материалов для освоения умений и усвоения знаний, оценки сформированности общих и профессиональных компетенций по виду профессиональной деятельности

3.1. Задания для оценки освоения теоретического курса профессионального модуля

3.1.1. Оценка освоения теоретического курса профессионального модуля по МДК.01.01

Дидактические единицы	Проверяемые ОК, ПК, У, З	Формы контроля (наименование контрольной точки)	
		Текущая аттестация	Промежуточная аттестация
Тема 1.1. Основы сетей передачи данных	У1, З1 ОК1-ОК12 ПК 1.1	Практическая работа № 1. Опрессовка кабеля и розеток. Обжим перекрестного кабеля.	Устные ответы на экзамене
Тема 1.2. Системы связи с подвижными объектами	У1, З1 ОК1-ОК12 ПК 1.1	Устный зачет по теме 1.2.	
Тема 1.3. Статическая маршрутизация.	У2, З1, ОК1-ОК12 ПК 1.2	Практическое занятие №4. Настройка адресации и маршрутизации.	
Тема 1.4. Универсальный идентификатор ресурсов (URI) и его назначение	З2, ОК1-ОК12 ПК 1.2	Устный зачет по теме 1.4.	
Тема 1.5. Глобальные компьютерные сети	У6, З2, ОК1-ОК12 ПК 1.2	Практическое занятие №19. Настройка протокола DHCP	
Тема 1.6. Сетевые информационные службы	У5, З3, ОК1-ОК12 ПК 1.2	Практическое занятие №24. Настройка маршрутизации сети в Cisco PT	
Тема 1.7. Безопасность компьютерных сетей	У7, З3, ОК1-ОК12 ПК 1.3	Практическая работа № 30. Обеспечение безопасности локальной сети	

Дидактические единицы	Проверяемые ОК, ПК, У, З	Формы контроля (наименование контрольной точки)	
		Текущая аттестация	Промежуточная аттестация
Тема 1.8. Настройка сети в ОС Windows	У5, З3, ОК1-ОК12 ПК 1.2	Практическое занятие №34. Создание виртуальной частной сети	
Тема 1.9 Настройка сети в ОС Linux	У5, З3, ОК1-ОК12 ПК 1.2	Практическое занятие №35. Настройка сетевых параметров через графический интерфейс	
Тема 1.11. Настройка сети в Router ОС	У5, З3, ОК1-ОК12 ПК 1.2	Практическое занятие №42. Построение сети с использованием Microkik	
Тема 1.13. Построение сети с выделенным сервером	У5, З3, ОК1-ОК12 ПК 1.2	Практическое занятие №50. Использование CMS для создания веб-ресурсов	

Практическая работа № 2 «Установка контроллера домена. Использование Windows PowerShell для администрирования AD DS»

Инструкция для обучающихся

Внимательно прочитайте задание. Выполните опрессовку кабеля и розеток.

Время выполнения – 90 минут.

Задание

1: Аккуратно обрежьте конец кабеля резаком, встроенным в обжимной инструмент.

Вставьте фотографию выполненной работы

2: Снимите с кабеля изоляцию ножом, встроенным в обжимной инструмент.

Вставьте фотографию выполненной работы

3: Разведите и расплетите проводки, выровняйте их в один ряд. Обкусите проводки так, чтобы их осталось чуть больше сантиметра (см. примечание).

Примечание

На рис. 1 показан неправильный обжим витой пары. На примере слева оставлены слишком длинные жилы, из-за чего расстояние от коннектора до оплетки остается незащищенным. Также кабель теряет прочность. На втором примере жилы срезаны слишком коротко, оплетка входит в коннектор, и длина концов проводников не позволяет создать их полноценный контакт с коннектором.

Рис. 1. Ошибки обжима кабеля

Вставьте фотографию выполненной работы

4: Вставьте проводники в коннектор RJ-45. Убедитесь, все ли провода полностью вошли в разъем и уперлись в его переднюю стенку.

Вставьте фотографию выполненной работы

5: Вставьте коннектор в устройство для обжима коннектора.

Вставьте фотографию выполненной работы

6: Надавите на клещи так, чтобы контакты коннектора зажали проводники внутри него.

Вставьте фотографию выполненной работы

7: Для проверки правильности обжима соедините кабелем сетевую карту и HUB (коммутатор, свич) и убедитесь в правильной работе такого кабеля.

Вставьте фотографию выполненной работы

Эталон ответа

В ходе выполнения практической работы был произведён прямой обжим витой пары 5 класса и коннектора RJ-45.

Первым делом была определена необходимая длина кабеля, в нашем случае это был кабель длиной 1 метр.

Провода в коннекторе RJ-45 были расположены в определенном порядке, который называется распиновкой. Существует два ее типа: прямая и перекрестная (кросс-овер). Первая обозначается аббревиатурой «568B», а вторая (kross-over) — «568A». Прямая распиновка применяется при соединении свича (хаба, роутера) с персональным компьютером или другим устройством. Тип «кроссовер» необходим только для соединения двух компьютеров напрямую.

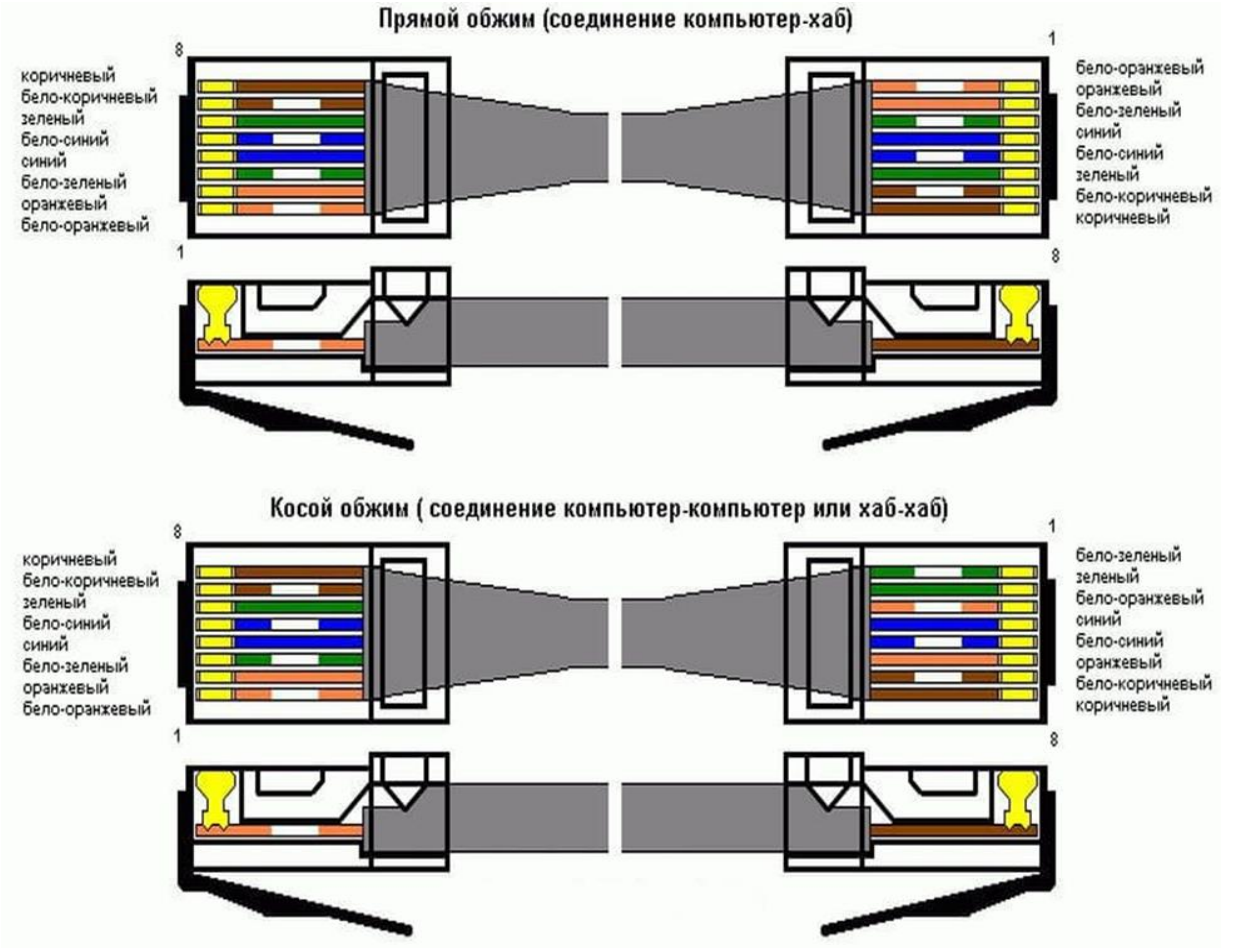


Рис. «Виды распиновки витой пары»

Для того, чтобы было удобно сделать распиновку, была обрезана изоляция провода на 1-1,5 см.

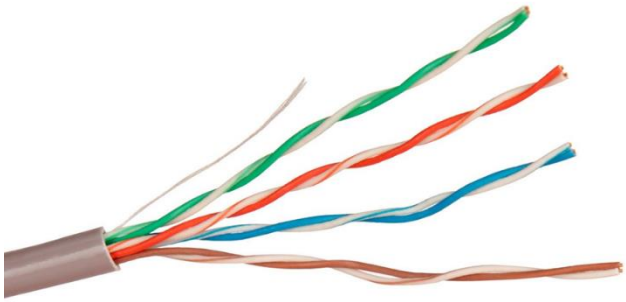


Рис. «Обрезка изоляции провода»

Все провода в ходе выполнения работы были расположены в следующем порядке:

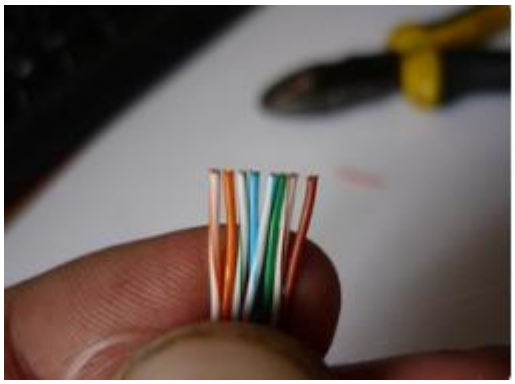


Рис. «Распиновка витой пары»

Провода на двух коннекторах располагаются одинаково. Нужно было правильно обжать интернет-кабель 8 жил, причем важным моментом является четкое соблюдение очередности расположения проводов.

Далее были выровнены концы провода, провод был вставлен в коннектор RJ-45, была выполнена обжимка витой пары.

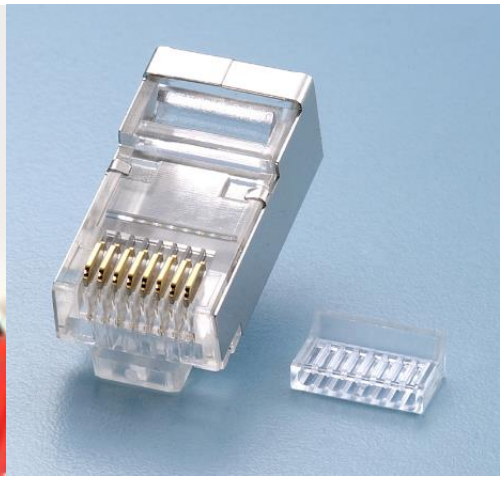


Рис. «Процесс обжимки и коннектор RJ-45»

В итоге получился следующий кабель для Интернет-соединения:

Рис. «Результат выполнения прямого обжима»

Для обжима розетки категории 5 под разъём RJ-45 потребовалась отвертка с плоским тонким жалом, по толщине, не превышающей диаметр медного проводника витой пары. Также заталкивать провода в щели розетки можно ножом с тонким лезвием, например, канцелярским ножом, у которого лезвие выдвигается.

Подготавливается для разделки кабель, снимается на длину не более 3 см его внешняя оболочка. Расплетаются пары на длину не более 13-15 мм. Далее, по схеме цветов, проводники по очереди заводятся в гребенку, заправляются боковой плоскостью лезвия отвертки и затем торцом лезвия заталкиваются до упора. В особых случаях (при необходимости) в одно гнездо можно вставить два кабеля витой пары, смонтированных на одну вилку.

Устный зачет по теме 1.2

Инструкция для обучающихся

Зачет сдается в рамках учебного занятия. Каждый студент отвечает в устной форме на предложенные преподавателем 7 мини-вопросов.

Выполнение задания: одному студенту на ответ выделяется 3 мин., группа сдает зачет за одно учебное занятие.

Перечень вопросов:

1. Что такое статическая маршрутизация?
2. Что такое адрес хоста?
3. Что такое маска подсети?
4. Что такое шлюз?
5. Что такое метрика сети?

6. Как работает broadcast?
7. Что что такое таблицы маршрутизации?

Эталоны ответов: приведены в учебном пособии по МДК.01.01 «Компьютерные сети».

Практическая работа № 2.
Знакомство со средой моделирования Cisco Packet Tracer, способами конфигурация сети, командной строкой, сценариями проверки

Инструкция для обучающихся

Внимательно прочитайте задание. Ознакомьтесь с теоретическим материалом и инструкциями по работе с программой Cisco packet tracer.

Время выполнения задания – 90 минут.

Задание

1. Запустите среду моделирования Cisco packet tracer. Ознакомьтесь с ее интерфейсом.
2. Сконфигурируйте в среде моделирования сеть, представленную на рисунке. Обратите внимание на используемые типы кабелей и модели оборудования (номера сетевых интерфейсов, которыми Вы соедините оборудование значение не имеют).
3. Добавьте в созданную сеть новый ноутбук и сервер. Сконфигурируйте их так, чтобы они подключались к беспроводной сети. Сервер должен иметь также подключение к проводной сети (в том же коммутаторе, что и точки беспроводного доступа).

Вставьте скриншот выполненной работы

4. Используя командную строку задайте сетевым узлам:
    a. Уникальные сетевые имена;
    b. Приветственные приглашения, в которых будет указываться краткая информация о сетевом устройстве;
    c. Пароли для прямого подключения к устройствам и режим их проверки;
    d. Для устройств, соединяющих главный и дополнительный офисы, задайте описания для соответствующих сетевых интерфейсов.
    e. Переведите сетевые интерфейсы в состояния, соответствующие рисунку.

Вставьте скриншот выполненной работы

5. Сохраните настройки сетевых устройств в их энергонезависимой памяти. Для маршрутизаторов, соединяющих основной и дополнительный офисы, сохраните конфигурацию в отдельные файлы.

Вставьте скриншот выполненной работы

6. Создайте сценарий проверки работоспособности сети, в котором необходимо проверить передачу следующих данных:
   a. ping от компьютера PC1 в главном офисе до компьютера PC2 в дополнительном офисе;

Вставьте скриншот выполненной работы

   b. ping от компьютера PC0 в главном офисе до сервера Server0 в главном корпусе;

Вставьте скриншот выполненной работы

   c. ping от компьютера PC2 в главном офисе до сервера Server2 в дополнительном офисе;

Вставьте скриншот выполненной работы

   d. http запрос от LaptopPT к Server2;

Вставьте скриншот выполненной работы

   e. DNS запрос от PDA-PT к Server1.

Вставьте скриншот выполненной работы

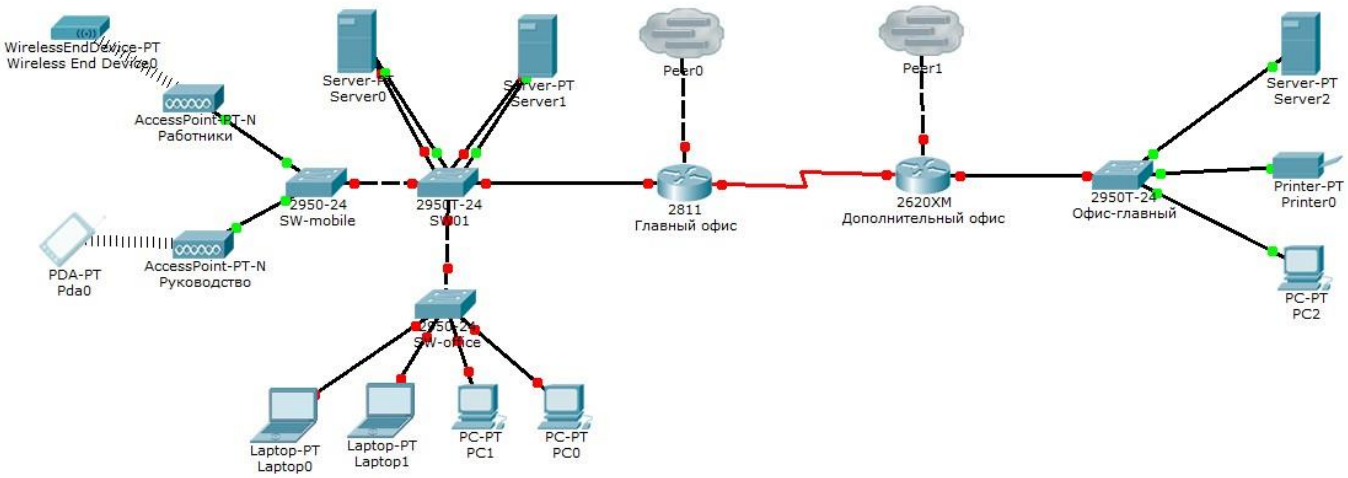


Рис. Конфигурируемая сеть

Эталон ответа

Было выполнено построение сети из 3 ПК и сетевого концентратора (хаба) в программе Cisco Packet Tracer 7.2.2.

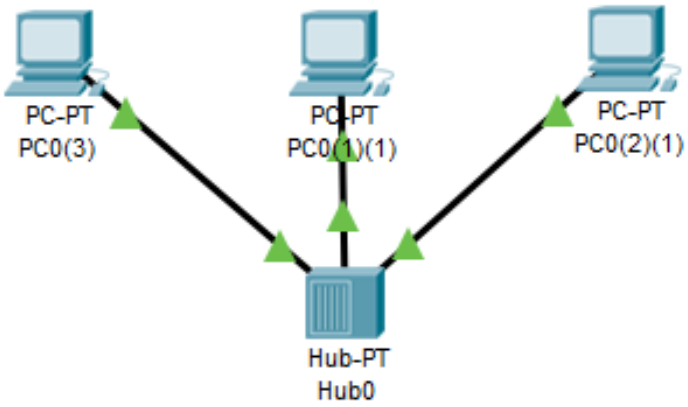


Рис. Сеть из 3 ПК и хаба

Также была выполнена проверка работоспособности сети с помощью простейшей команды ping.

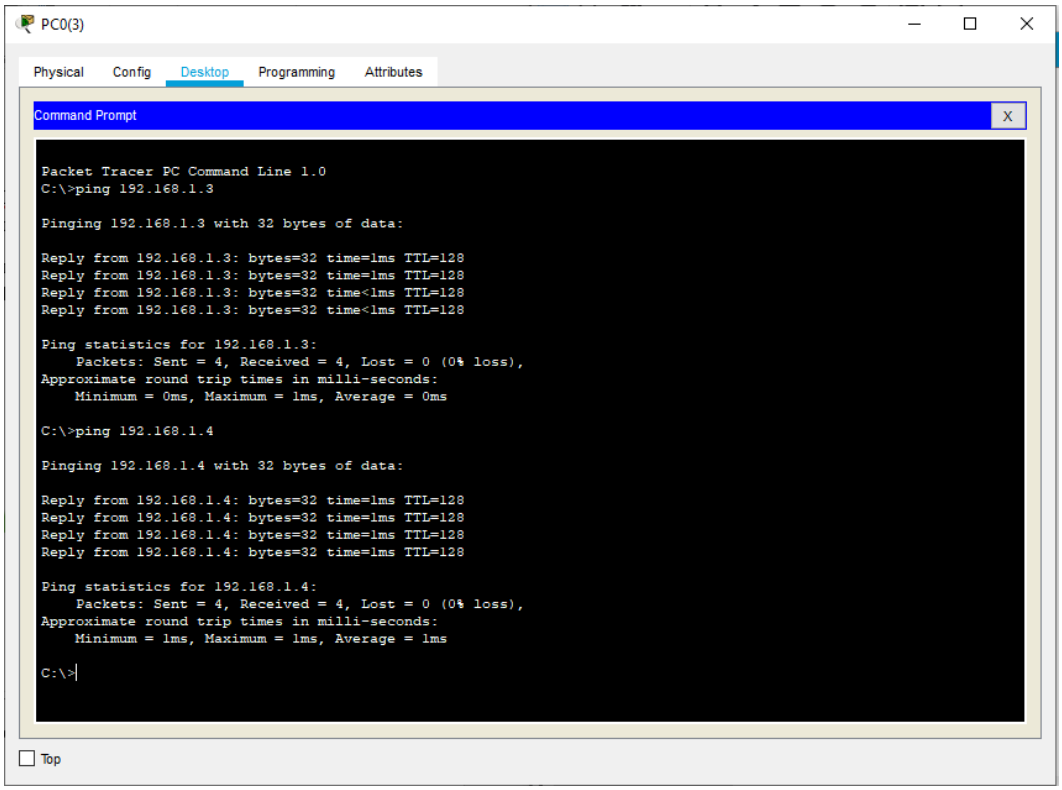


Рис. Процесс проверки работоспособности сети

Далее было выполнено построение сети из 3 ПК и сетевого коммутатора в программе Cisco Packet Tracer 7.2.2.

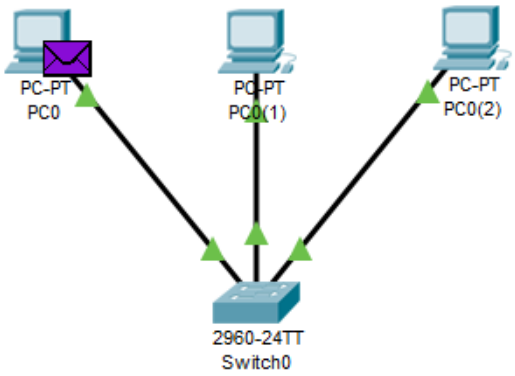


Рис. Сеть из 3 ПК и коммутатора

Также была выполнена проверка работоспособности сети с помощью простейшей команды ping.

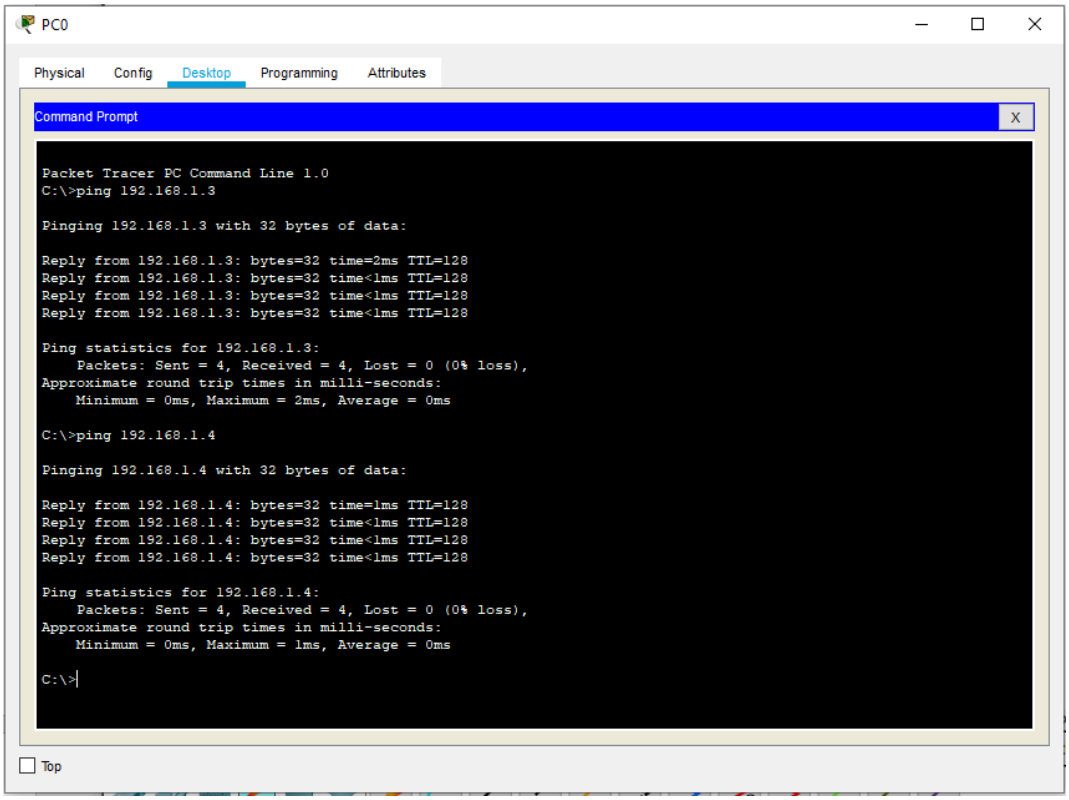


Рис. Процесс проверки работоспособности сети

Также для визуализации процесса передачи данных была выполнена отправка электронного сообщения в двух созданных сетях.

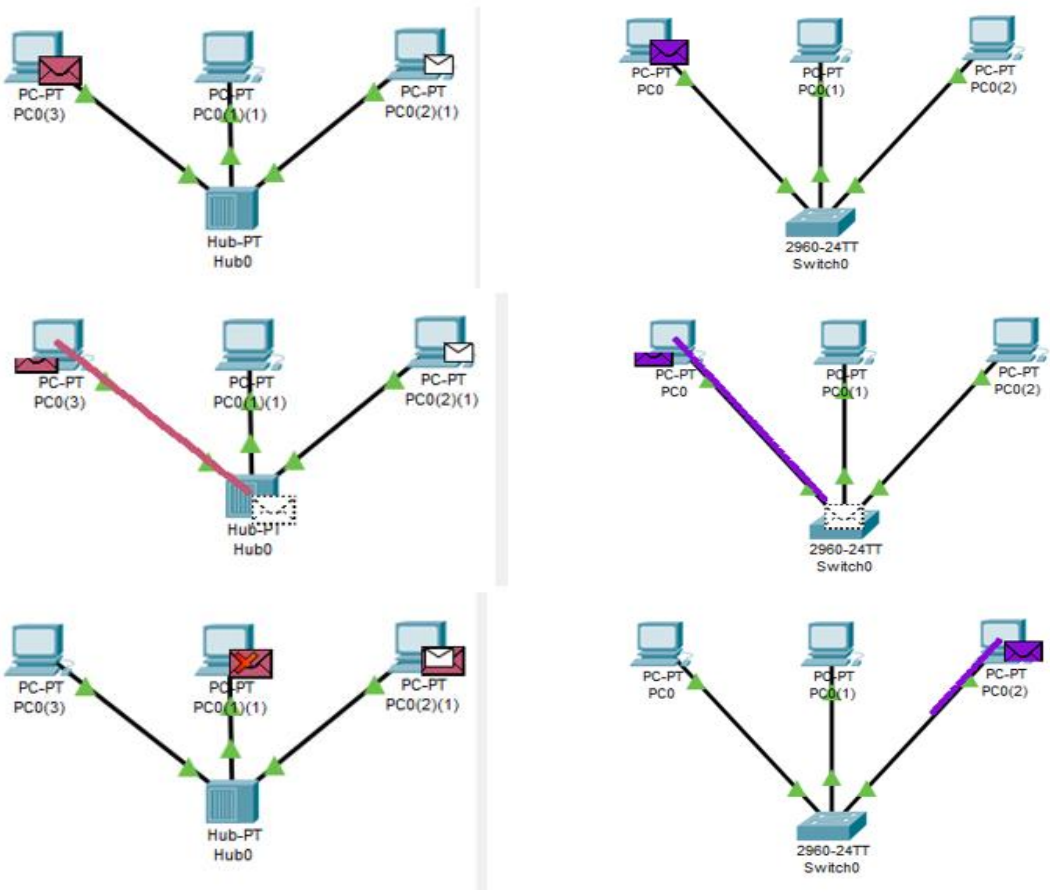


Рис. Процесс отправки сообщения через хаб или коммутатор в сравнении

Как видно из сравнения, хаб отправляет сообщение на все порты, а коммутатор отправляет только на определённое устройство благодаря использованию таблицы MAC-адресов.

Практическая работа №4
Настройка адресации и статической маршрутизации в локальных компьютерных сетях

Инструкция для обучающихся

Внимательно прочитайте задание. Осуществите конфигурирование адресации и статической маршрутизации в локальных компьютерных сетях, взаимодействующих с использованием стека протоколов TCP/IP версии 4.

Время выполнения задания – 90 минут.

Задание

Задание:

1. Измените конфигурацию сети, собранную в п.2 Практической работы № 3 (пример измененной сети представлен на рисунке):
   a. В маршрутизатор головного офиса добавьте модуль, реализующий 16-ти портовый коммутатор (NM-ESW-161);

Вставьте скриншот выполненной работы

b. Интерфейсы FastEthernet 0/1 серверов главного офиса переключите на коммутатор, включенный в состав маршрутизатора.

Вставьте скриншот выполненной работы

2. Для Вашей организации выделена сеть 10.N.0.0/16, где N – Ваш номер по списку в журнале преподавателя. Определите параметры следующих подсетей Вашей организации:
   a. Сеть Главного офиса (ноутбуки, серверы, точки доступа, рабочие станции, один порт маршрутизатора);

   Вставьте скриншот выполненной работы

   b. Сеть серверов Главного офиса (серверы, коммутатор маршрутизатора);

   Вставьте скриншот выполненной работы

   c. Сеть маршрутизаторов (последовательные интерфейса) предприятия;

   Вставьте скриншот выполненной работы

   d. Сеть дополнительного офиса (сервер, принтер, рабочая станция порт маршрутизатора).

   Вставьте скриншот выполненной работы

3. Сконфигурируйте ноутбуки, рабочие станции и серверы главного офиса согласно выбранной схеме подсетей.

   Вставьте скриншот выполненной работы

4. Убедитесь, что настройки верны (компьютеры имею связь друг с другом).

   Вставьте скриншот выполненной работы

   Проверьте таблицы физических адресов на коммутаторах и маршрутизаторе офиса. Во всех ли таблицах одинаковые записи?

   Поясните результат

5. Сконфигурируйте сетевые узлы дополнительного офиса. Проверьте, что они имеют связь друг с другом.

   Вставьте скриншот выполненной работы

6. Сконфигурируйте сеть между коммутаторами офисов. Появилась ли связь между узлами сети дополнительного офиса и главного офиса? Поясните результат.

   Вставьте скриншот выполненной работы

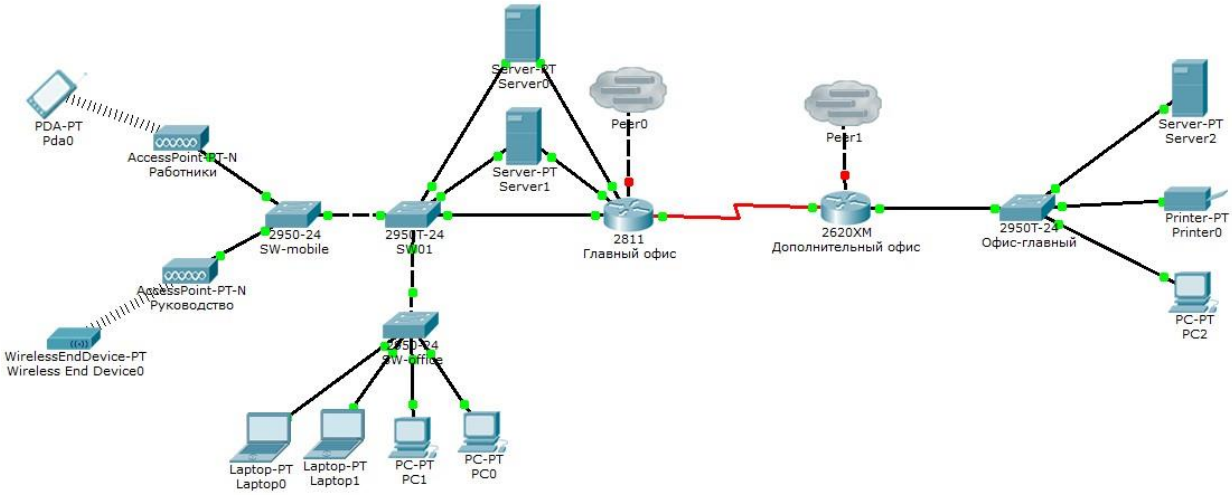


Рис. Пример конфигурации модернизированной сети

Эталон ответа

1. Изменяем конфигурацию сети, собранную в практической работе №3.

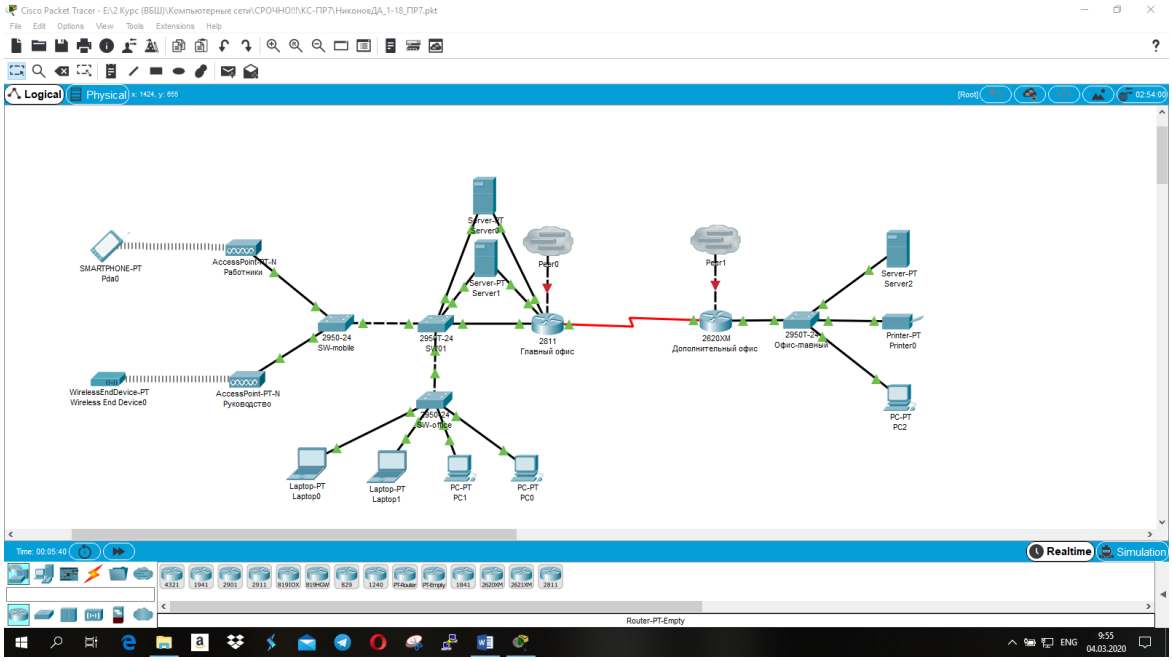
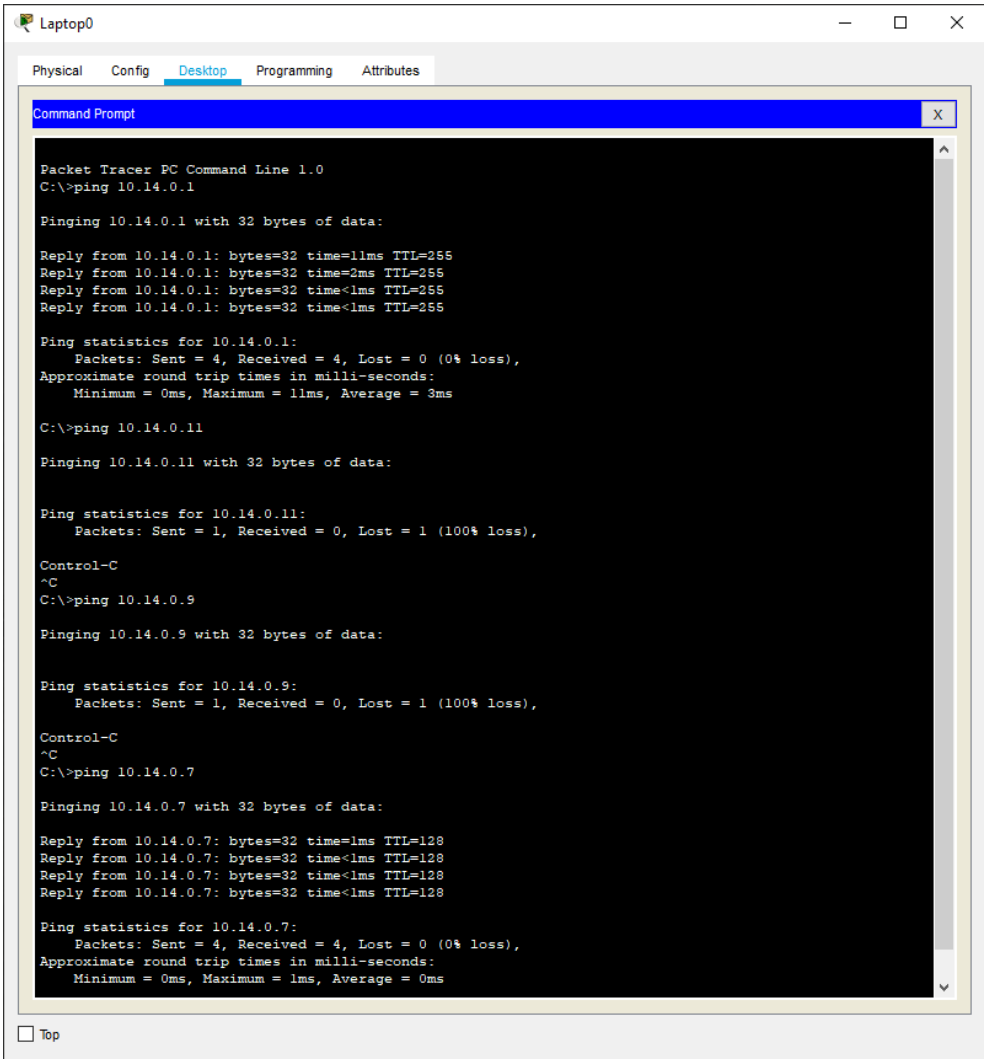


Рис. Обновлённая конфигурация сети

2. Определены параметры подсетей организации.

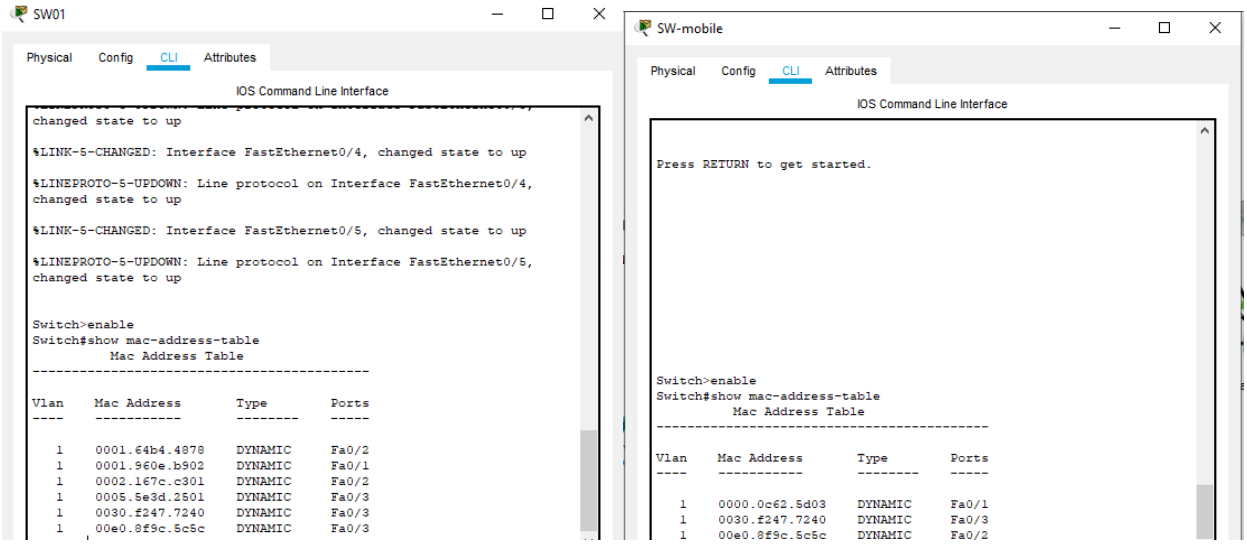
Все IP-адреса устройств были заменены на 10.14.0.X, где X – индивидуальное число для каждого устройства в сети.

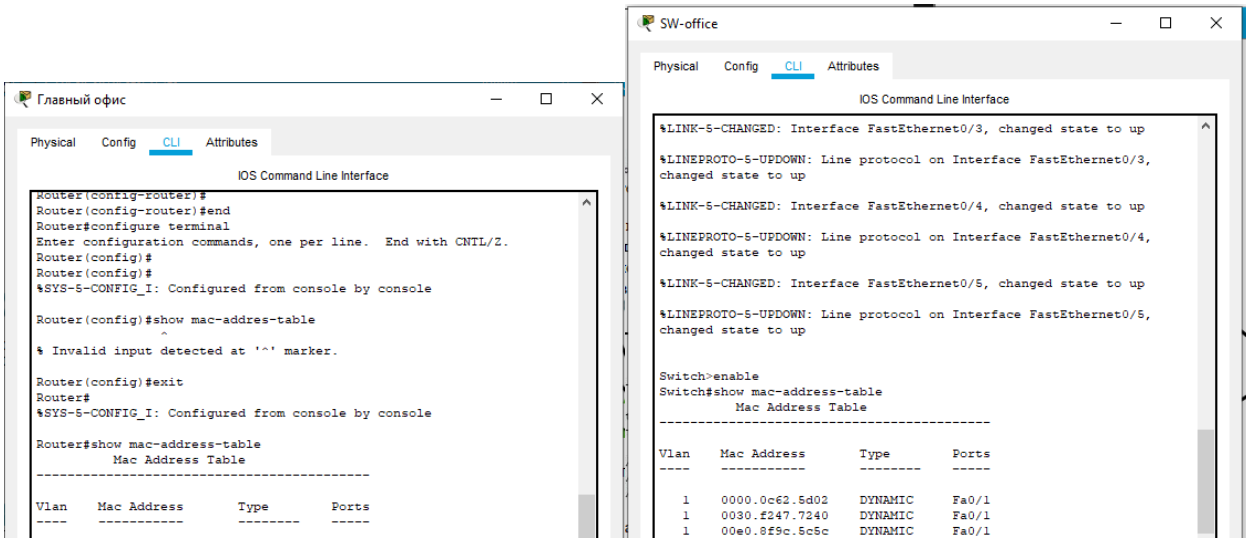
3.Осуществлено конфигурирование ноутбуков, рабочих станций и серверов главного офиса согласно выбранной схеме подсетей.



В главном и дополнительном офисе есть связи между устройствами, но сами офисы не имеют связи между собой, так как маршрутизаторы не настроены.

Проверка физических адресов:





Все таблицы разные, так как подключены разные устройства.

Таким образом, сеть сконфигурирована согласно поставленным задачам.

Устный зачет по теме 1.4

Инструкция для обучающихся

Зачет сдается в рамках учебного занятия. Каждый студент отвечает в устной форме на предложенные преподавателем 13 мини-вопросов.

Выполнение задания: одному студенту на ответ выделяется 3 мин., группа сдает зачет за одно учебное занятие.

Перечень вопросов:

1. С какой целью разрабатывают форматы кадров?
2. Формат кадра по протоколу HDLC. Назначение полей.
3. Протокол PPP. Формат кадра. Назначение полей.
4. Протоколы авторизации PAP и CHAP.
5. Форматы кадров стандарта Ethernet.
6. Алгоритм автоматического определения формата кадра Ethernet.
7. Стандарт IEEE 802.1Q. Назначение. Пример применения.
8. Конфигурирования последовательных интерфейсов на оборудовании CISCO.
9. Конфигурирование интерфейса Ethernet на оборудовании CISCO.
10. Настройка VLAN на оборудовании CISCO.
11. Реализация маршрутизации между VLAN.
12. Алгоритм циклического избыточного кодирования.
13. Таксономия алгоритмов циклического избыточного кодирования.

Эталоны ответов: приведены в учебном пособии по МДК.01.01 «Компьютерные сети».

Практическая работа № 19
Настройка протокола DHCP

Инструкция для обучающихся

Внимательно прочитайте задание. Осуществите работу с динамической маршрутизацией трафика в компьютерных сетях.

Время выполнения задания – 90 минут.

Задание:

1. В существующей сети Вашего предприятия удалите все статические маршруты и маршруты «по умолчанию» на маршрутизаторах главного и дополнительного офисов.

Вставьте скриншот выполненной работы

2. Сконфигурируйте маршрутизаторы Ваших офисов так, чтобы они по последовательному интерфейсу обменивались информацией о маршрутах с использованием протокола RIP. Таблицы RIP должны приниматься только по последовательным интерфейсам. Убедитесь в правильности сформированных таблиц маршрутизации.

Вставьте скриншот выполненной работы

3. Используя многопользовательское окружение подключите маршрутизатор дополнительного офиса к маршрутизаторам дополнительных офисов двух других предприятий (те, в свою очередь, тоже должны быть соединены между собой, образуя кольцо из трех сетей 172.16.N.0/24).

Вставьте скриншот выполненной работы

4. Сконфигурируйте в сетях 172.16.N.0/24 функционирование протокола OSPF (объединив все маршрутизаторы в зону и сделав их пограничными). Обеспечьте интеграцию информации, полученной по протоколу RIP в данные протокола OSPF и наоборот. Продемонстрируйте связь между сетевыми узлами разных предприятий.

Вставьте скриншот выполненной работы

Эталон ответа:

Динамическая маршрутизация — вид маршрутизации, при котором таблица маршрутизации редактируется программно.

Работа маршрутизатора, поддерживающего протокол RIP, выполняется в несколько этапов.

Этап 1. Создание минимальной таблицы. На этом этапе маршрутизатор формирует начальный вектор, в который включает информацию о всех сетях, к которым он имеет непосредственное подключение. Каждый коммутатор такую таблицу формирует самостоятельно.

Этап 2. Рассылка собственной таблицы своим соседям. После того, как сформирован локальный вектор он регулярно рассылается через все интерфейсы маршрутизатора (которые участвуют в формировании топологии сети).

Этап 3. Получение и обработка векторов от своих соседей. Получив вектор от своего соседа, маршрутизатор увеличивает значение метрик с учетом метрики канала, через который поступило RIP-сообщений.

Дистанционно-векторные алгоритмы применимы для небольших сетей. Ограничение связано с тем, что с увеличением количества сетей, о которых необходимо передавать информацию объем трафика и время конвергенции алгоритма резко увеличиваются.

К дистанционно-векторным относятся протоколы: RIP, IGRP, BGP, AODV и др.

В алгоритмах, основанных на состоянии связей, каждый маршрутизатор рассылает информацию только о сетях, к которым он имеет непосредственную связь. В результате каждый маршрутизатор самостоятельно строит топологию сети и выбирает наименьшие расстояния до каждой сети. Для расчета расстояний используется алгоритм Дейкстры.

К протоколам, основанным на состояниях каналов связей, относятся IS-IS, OSPF, NLSP, OLSR и др.

Метрика - расстояние до сети. В качестве метрик может использоваться единичное значение или показатель пропускной способности и/или надежность канала. В некоторых протоколах вводится дополнительная метрика, характеризующая недостижимость сети. Также может использоваться нулевая метрика, характеризующая непосредственное подключение маршрутизатора к сети. Обычно, чем меньше метрика, тем меньше расстояние.

Главная задача протоколов маршрутизации- формирование согласованных таблиц маршрутизации. Согласованная таблица – это такая таблица, которая обеспечивает передачу данных между сетями за конечное число шагов. При изменениях в сети таблицы становятся несогласованными, т.е. передача данных между некоторыми сетями оказывается невозможной.

Время, в течение которого таблицы приводятся в согласованное состояние называется временем конвергенции (или сходимости алгоритма).

Используя протокол RIP коммутатор R1 сообщает коммутатору R2 о том, что он имеет прямое подключение к сетям 192.168.1.0/24 или 10.0.0.0/24 (указывая метрику 0). Получив сообщение от R1 маршрутизатор увеличивает значение метрики и понимает, что через R1 ему доступны маршруты до указанных сетей с расстоянием 1 (было 0, прибавили метрику 1 канала между R1 и R2). Поскольку R2 уже в своей таблице имеет запись с маршрутом до сети 10.0.0.0/24 и его метрика меньше (она равна 0), то полученная запись об этой сети игнорируется, а запись о сети 192.168.1.0 заносится в таблицу.

Аналогичная ситуация происходит с таблицей маршрутизатора R1 и он узнает о маршруте до сети 172.16.0.0/24 с метрикой 1.

Задание:

Задание: настроить маршрутизацию в созданной в Практической работе №23 компьютерной сети.

Часть 1. По файлу PT (ПР№23) создать таблицу маршрутизации и настроить статическую маршрутизацию по созданной таблице.

Вставьте таблицу маршрутизации:

Вставьте скриншоты настройки маршрутизации.

Вставьте скриншоты проверки работоспособности маршрутизации.

Вопросы:

1. Какими командами настраивается статическая маршрутизация?
2. Какими командами проверяется работоспособность маршрутизации?

Часть 2. Создайте второй файл PT (ПР№23_2) и настройте динамическую маршрутизацию в сети.

Вставьте скриншоты настройки маршрутизации.

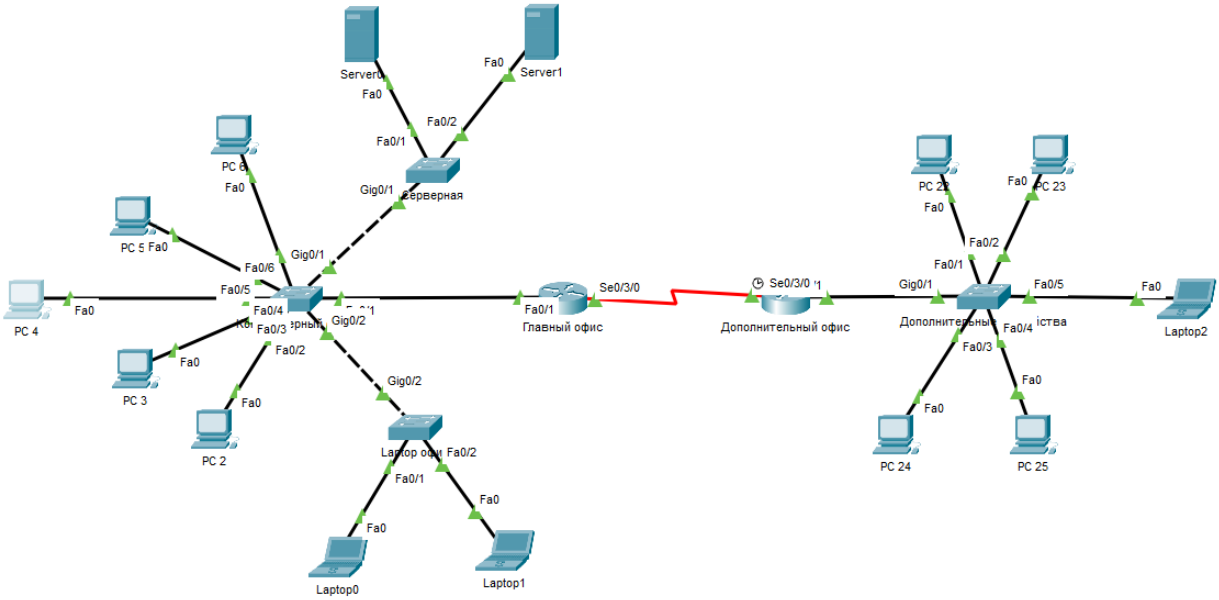
Вставьте скриншоты проверки работоспособности маршрутизации.

Вопросы:

1. Что такое динамическая маршрутизация? Для чего применяется?
2. Какие протоколы отвечают за настройку динамической маршрутизации? Принцип их работы.
3. Какими командами настраивается динамическая маршрутизация?

Эталон ответа:

Задание: настроить маршрутизацию в созданной в Практической работе №23 компьютерной сети.



Часть 1. По файлу PT (ПР№23) создать таблицу маршрутизации и настроить статическую маршрутизацию по созданной таблице.

Вставьте таблицу маршрутизации:

Устройство	интерфейс	ip-адрес	маска	маршрут по умолчанию
Главный офис	S0/3/0	192.168.3.1	255.255.255.252	____
	Fa0/1	192.168.1.1	255.255.255.0	
Дополнительный офис	S0/3/0	192.168.3.2	255.255.255.252	____

	Fa0/1	192.168.2.1	255.255.255.0	
PC2	Fa0	192.168.1.2	255.255.255.0	192.168.1.1
PC3	Fa0	192.168.1.3	255.255.255.0	192.168.1.1
PC4	Fa0	192.168.1.4	255.255.255.0	192.168.1.1
PC5	Fa0	192.168.1.5	255.255.255.0	192.168.1.1
PC6	Fa0	192.168.1.6	255.255.255.0	192.168.1.1
Server0	Fa0	192.168.1.9	255.255.255.0	192.168.1.1
Server1	Fa0	192.168.1.10	255.255.255.0	192.168.1.1
Laptop0	Fa0	192.168.1.7	255.255.255.0	192.168.1.1
Laptop1	Fa0	192.168.1.8	255.255.255.0	192.168.1.1
PC22	Fa0	192.168.2.2	255.255.255.0	192.168.2.1
PC23	Fa0	192.168.2.3	255.255.255.0	192.168.2.1
PC24	Fa0	192.168.2.4	255.255.255.0	192.168.2.1
PC25	Fa0	192.168.2.5	255.255.255.0	192.168.2.1
Laptop2	Fa0	192.168.2.6	255.255.255.0	192.168.2.1

Вставьте скриншоты настройки маршрутизации.

```
Device Name: Главный офис
Custom Device Model: 2811 IOS15
Hostname: R0

Port              Link   VLAN   IP Address         IPv6 Address                            MAC Address
FastEthernet0/0   Down   --     <not set>          <not set>                               000A.F307.2701
FastEthernet0/1   Up     --     192.168.1.1/24     <not set>                               000A.F307.2702
Serial0/3/0       Up     --     192.168.3.1/30     <not set>                               <not set>
Serial0/3/1       Down   --     <not set>          <not set>                               <not set>
Vlan1             Down   1      <not set>          <not set>                               0001.C772.EE8A

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Главный офис
```

```
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, FastEthernet0/1
L       192.168.1.1/32 is directly connected, FastEthernet0/1
S    192.168.2.0/24 [1/0] via 192.168.3.2
                    is directly connected, Serial0/3/0
     192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/30 is directly connected, Serial0/3/0
L       192.168.3.1/32 is directly connected, Serial0/3/0

R0#
```

```
Device Name: Дополнительный офис
Custom Device Model: 2811 IOS15
Hostname: R1

Port             Link   VLAN   IP Address         IPv6 Address                              MAC Address
FastEthernet0/0  Down   --     <not set>          <not set>                                 0060.5C44.6401
FastEthernet0/1  Up     --     192.168.2.1/24     <not set>                                 0060.5C44.6402
Serial0/3/0      Up     --     192.168.3.2/30     <not set>                                 <not set>
Serial0/3/1      Down   --     <not set>          <not set>                                 <not set>
Vlan1            Down   1      <not set>          <not set>                                 00D0.9716.A585

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Дополнительный офис
```

```
S    192.168.1.0/24 is directly connected, Serial0/3/0
     192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/24 is directly connected, FastEthernet0/1
L       192.168.2.1/32 is directly connected, FastEthernet0/1
     192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/30 is directly connected, Serial0/3/0
L       192.168.3.2/32 is directly connected, Serial0/3/0
```

Вставьте скриншоты проверки работоспособности маршрутизации.

```
C:\>ping 192.168.2.6

Pinging 192.168.2.6 with 32 bytes of data:

Reply from 192.168.2.6: bytes=32 time=1ms TTL=126
Reply from 192.168.2.6: bytes=32 time=1ms TTL=126
Reply from 192.168.2.6: bytes=32 time=1ms TTL=126
Reply from 192.168.2.6: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.2.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

```
C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time=1ms TTL=126
Reply from 192.168.2.2: bytes=32 time=2ms TTL=126
Reply from 192.168.2.2: bytes=32 time=1ms TTL=126
Reply from 192.168.2.2: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

```
C:\>ping 192.168.2.5

Pinging 192.168.2.5 with 32 bytes of data:

Reply from 192.168.2.5: bytes=32 time=2ms TTL=126
Reply from 192.168.2.5: bytes=32 time=1ms TTL=126
Reply from 192.168.2.5: bytes=32 time=1ms TTL=126
Reply from 192.168.2.5: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.2.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

Вопросы:

3. Какими командами настраивается статическая маршрутизация?

   Ip route

4. Какими командами проверяется работоспособность маршрутизации?

   Show ip route

   Show run

Часть 2. Создайте второй файл PT (ПР№23_2) и настройте динамическую маршрутизацию в сети.

Вставьте скриншоты настройки маршрутизации.

Вставьте скриншоты проверки работоспособности маршрутизации.

Вопросы:

4. Что такое динамическая маршрутизация? Для чего применяется?

Динамическая маршрутизация — вид маршрутизации, при котором таблица маршрутизации редактируется программно. Применяется для того, чтобы маршрутизаторы могли выбирать пути в соответствии с логическими изменениями структуры сети в реальном времени, в отличие от статической маршрутизации.

5. Какие протоколы отвечают за настройку динамической маршрутизации? Принцип их работы.

   RIP OSPF EIGRP EGP DHCP

- Маршрутизатор отправляет и принимает сообщения маршрутизации на свои интерфейсы.
- Маршрутизатор предоставляет общий доступ к сообщениям маршрутизации и данным о маршрутах для других маршрутизаторов, использующих тот же протокол маршрутизации.
- Маршрутизаторы осуществляют обмен данными маршрутизации для получения информации об удалённых сетях.
- При обнаружении маршрутизатором изменений в топологии, протокол маршрутизации может объявить это изменение для других маршрутизаторов.

6. Какими командами настраивается динамическая маршрутизация?

Route ospf 1

Network … area 1

```
router ospf 1
 log-adjacency-changes
 network 192.168.1.0 0.0.0.255 area 1
 network 192.168.2.0 0.0.0.255 area 1
 network 192.168.3.0 0.0.0.3 area 1
```

```
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, FastEthernet0/1
L       192.168.1.1/32 is directly connected, FastEthernet0/1
O    192.168.2.0/24 [110/65] via 192.168.3.2, 00:00:08, Serial0/3/0
     192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/30 is directly connected, Serial0/3/0
L       192.168.3.1/32 is directly connected, Serial0/3/0

R0#sh r
Gateway of last resort is not set

O    192.168.1.0/24 [110/65] via 192.168.3.1, 00:00:26, Serial0/3/0
     192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/24 is directly connected, FastEthernet0/1
L       192.168.2.1/32 is directly connected, FastEthernet0/1
     192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/30 is directly connected, Serial0/3/0
L       192.168.3.2/32 is directly connected, Serial0/3/0

R1#
```

```
C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time=1ms TTL=126
Reply from 192.168.2.2: bytes=32 time=1ms TTL=126
Reply from 192.168.2.2: bytes=32 time=2ms TTL=126
Reply from 192.168.2.2: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>ping 192.168.2.6

Pinging 192.168.2.6 with 32 bytes of data:

Reply from 192.168.2.6: bytes=32 time=1ms TTL=126
Reply from 192.168.2.6: bytes=32 time=1ms TTL=126
Reply from 192.168.2.6: bytes=32 time=2ms TTL=126
Reply from 192.168.2.6: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.2.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

Практическая работа № 30Обеспечение безопасности локальной сети

Инструкция для обучающихся

Внимательно прочитайте задание. Осуществите действия по обеспечению безопасности локальной сети.

Время выполнения задания – 90 минут.

Задание 1. Настройка основных параметров устройств

Шаг 1: Создайте сеть согласно топологии.

Подключите устройства, показанные в топологии, и кабели соответствующим образом.

Вставьте скриншот выполненной работы

Шаг 2: Выполните инициализацию и перезагрузку маршрутизатора и коммутатора.

Вставьте скриншот выполненной работы

Шаг 3: Выполните настройку маршрутизатора и коммутатора.

a. Подключитесь к устройству с помощью консольного подключения и активируйте привилегированный режим EXEC.

Вставьте скриншот выполненной работы

b. Назначьте устройству имя в соответствии с таблицей адресации.

Вставьте скриншот выполненной работы

c. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.

Вставьте скриншот выполненной работы

d. Назначьте **class** в качестве зашифрованного пароля привилегированного режима EXEC.

Вставьте скриншот выполненной работы

e. Назначьте **cisco** в качестве пароля консоли и включите вход в систему по паролю.

Вставьте скриншот выполненной работы

f. Назначьте **cisco** в качестве пароля VTY и включите вход в систему по паролю.

Вставьте скриншот выполненной работы

g. Создайте баннер с предупреждением о запрете несанкционированного доступа к устройству.

Вставьте скриншот выполненной работы

h. Настройте и активируйте на маршрутизаторе интерфейс G0/1, используя информацию, приведенную в таблице адресации.

Вставьте скриншот выполненной работы

i. Задайте для используемого по умолчанию интерфейса SVI сведения об IP-адресе согласно таблице адресации.

Вставьте скриншот выполненной работы

j. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

Вставьте скриншот выполненной работы

Задание 2. Настройка базовых мер безопасности на маршрутизаторе

Шаг 1: Зашифруйте открытые пароли.

R1(config)# **service password-encryption**

Вставьте скриншот выполненной работы

Шаг 2: Установите более надежные пароли.

a. Измените зашифрованный пароль привилегированного режима EXEC в соответствии с рекомендациями.

R1(config)# **enable secret Enablep@55**

Вставьте скриншот выполненной работы

b. Установите минимальную длину 10 символов для всех паролей.

R1(config)# **security passwords min-length 10**

Вставьте скриншот выполненной работы

Шаг 3: Разрешите подключения по протоколу SSH.

a. В качестве имени домена укажите **CCNA-lab.com**.

R1(config)# **ip domain-name CCNA-lab.com**

Вставьте скриншот выполненной работы

b. Создайте в базе данных локальных пользователей запись, которая будет использоваться при подключении к маршрутизатору через SSH. Пароль должен соответствовать стандартам надежных паролей, а пользователь — иметь права доступа уровня EXEC. Если уровень привилегий не задан в команде, то пользователь по умолчанию будет иметь права доступа EXEC (уровень 15).
R1(config)# **username SSHadmin privilege 15 secret Admin1p@55**

Вставьте скриншот выполненной работы

c. Настройте транспортный вход для линий VTY таким образом, чтобы они могли разрешать подключения по протоколу SSH, но не разрешали подключения по протоколу Telnet.
R1(config)# **line vty 0 4**
R1(config-line)# **transport input ssh**

Вставьте скриншот выполненной работы

d. Аутентификация на линиях VTY должна выполняться с использованием базы данных локальных пользователей.
R1(config-line)# **login local**
R1(config-line)# **exit**

Вставьте скриншот выполненной работы

e. Создайте ключ шифрования RSA с длиной 1024 бит.
R1(config)# **crypto key generate rsa modulus 1024**

Вставьте скриншот выполненной работы

Шаг 4: Обеспечьте защиту консоли и линий VTY.

a. Маршрутизатор можно настроить таким образом, чтобы он завершал сеанс подключения в случае отсутствия активности в течение заданного времени. Если сетевой администратор вошел в систему сетевого устройства, а потом был внезапно вынужден покинуть рабочее место, то по истечении установленного времени эта команда автоматически завершит сеанс подключения. Приведенные ниже команды обеспечивают закрытие сеанса линии связи через пять минут отсутствия активности.
R1(config)# **line console 0**
R1(config-line)# **exec-timeout 5 0**
R1(config-line)# **line vty 0 4**
R1(config-line)# **exec-timeout 5 0**
R1(config-line)# **exit**
R1(config)#

Вставьте скриншот выполненной работы

b. Команда, приведенная ниже, не разрешает вход в систему с использованием метода полного перебора. Маршрутизатор блокирует попытки входа в систему на 30 секунд, если в течение 120 секунд будет дважды введен неверный пароль.
R1(config)# **login block-for 30 attempts 2 within 120**

Вставьте скриншот выполненной работы

Что означает **2 within 120** в приведенной выше команде?

Ответ:_____

Что означает **block-for 30** в приведенной выше команде?

Ответ:_____

Шаг 5: Убедитесь, что все неиспользуемые порты отключены.

Порты маршрутизатора отключены по умолчанию, однако рекомендуется лишний раз убедиться, что все неиспользуемые порты отключены администратором. Для этого можно воспользоваться командой **show ip interface brief**. Все неиспользуемые порты, не отключенные администратором, необходимо отключить с помощью команды **shutdown** в режиме конфигурации интерфейса.

R1# **show ip interface brief**

Interface IP-Address OK? Method Status Protocol
Embedded-Service-Engine0/0 unassigned YES NVRAM administratively down down
GigabitEthernet0/0 unassigned YES NVRAM administratively down down
GigabitEthernet0/1 192.168.1.1 YES manual up up
Serial0/0/0 unassigned YES NVRAM administratively down down Serial0/0/1
unassigned YES NVRAM administratively down down
R1#

Вставьте скриншот выполненной работы

Шаг 6: Убедитесь, что все меры безопасности внедрены правильно.

a. С помощью программы Tera Term подключитесь к маршрутизатору R1 по протоколу Telnet.
Разрешает ли R1 подключение по протоколу Telnet? Дайте пояснение.
Ответ:_____

b. С помощью программы Tera Term подключитесь к маршрутизатору R1 по протоколу SSH. Разрешает ли R1 подключение по протоколу SSH?
Ответ:_____

c. Намеренно укажите неверное имя пользователя и пароль, чтобы проверить, будет ли заблокирован доступ к системе после двух неудачных попыток.
Что произошло после ввода неправильных данных для входа в систему во второй раз?
Ответ:_____

d. Из сеанса подключения к маршрутизатору с помощью консоли отправьте команду **show login**, чтобы проверить состояние входа в систему. В приведенном ниже примере команда **show login** была введена в течение 30-секундной блокировки доступа к системе и показывает, что маршрутизатор находится в режиме Quiet. Маршрутизатор не будет разрешать попытки входа в систему в течение еще 14 секунд.
R1# **show login**
A default login delay of 1 second is applied.
No Quiet-Mode access list has been configured.
Router enabled to watch for login Attacks.
If more than 2 login failures occur in 120 seconds or less, logins will be disabled for 30 seconds.
Router presently in Quiet-Mode.
Will remain in Quiet-Mode for 14 seconds.
Denying logins from all sources.
R1#

Вставьте скриншот выполненной работы

e. По истечении 30 секунд повторите попытку подключения к R1 по протоколу SSH и войдите в систему, используя имя **SSHadmin** и пароль **Admin1p@55**. Что отобразилось после успешного входа в систему?

Ответ:_____

f. Войдите в привилегированный режим EXEC и введите в качестве пароля **Enablep@55**.

Если вы неправильно вводите пароль, прерывается ли сеанс SSH после двух неудачных попыток в течение 120 секунд? Дайте пояснение.

Ответ:_____

Введите команду **show running-config** в строке приглашения привилегированного режима EXEC для просмотра установленных параметров безопасности.

Вставьте скриншот выполненной работы

Задание 3. Настройка базовых мер безопасности на коммутаторе

Шаг 1: Зашифруйте открытые пароли.

S1(config)# **service password-encryption**

Вставьте скриншот выполненной работы

Шаг 2: Установите более надежные пароли на коммутаторе.

Измените зашифрованный пароль привилегированного режима EXEC в соответствии с рекомендациями по установке надежного пароля.

S1(config)# **enable secret Enablep@55**

Вставьте скриншот выполненной работы

Примечание. Команда безопасности **password min-length** на коммутаторах модели 2960 недоступна.

Шаг 3: Разрешите подключения по протоколу SSH.

a. В качестве имени домена укажите **CCNA-lab.com**.

S1(config)# **ip domain-name CCNA-lab.com**

Вставьте скриншот выполненной работы

b. Создайте в базе данных локальных пользователей запись, которая будет использоваться при подключении к коммутатору через SSH. Пароль должен соответствовать стандартам надежных паролей, а пользователь — иметь права доступа уровня EXEC. Если уровень привилегий не задан в команде, то пользователь по умолчанию будет иметь права доступа EXEC (уровень 1).

S1(config)# **username SSHadmin privilege 1 secret Admin1p@55**

Вставьте скриншот выполненной работы

c. Настройте транспортный вход для линий VTY таким образом, чтобы они могли разрешать подключения по протоколу SSH, но не разрешали подключения по протоколу Telnet.

S1(config)# **line vty 0 15**

S1(config-line)# **transport input ssh**

Вставьте скриншот выполненной работы

d. Аутентификация на линиях VTY должна выполняться с использованием базы данных локальных пользователей.

S1(config-line)# **login local**

S1(config-line)# **exit**

Вставьте скриншот выполненной работы

e. Создайте ключ шифрования RSA с длиной 1024 бит.

S1(config)# **crypto key generate rsa modulus 1024**

Вставьте скриншот выполненной работы

Шаг 4: Обеспечьте защиту консоли и линий VTY.

a. Настройте коммутатор таким образом, чтобы он закрывал линию через десять минут отсутствия активности.

S1(config)# **line console 0**
S1(config-line)# **exec-timeout 10 0** S1(config-line)#
line vty 0 15
S1(config-line)# **exec-timeout 10 0**
S1(config-line)# **exit**
S1(config)#

Вставьте скриншот выполненной работы

b. Чтобы помешать попыткам входа в систему с использованием метода полного перебора, настройте коммутатор таким образом, чтобы он блокировал доступ к системе на 30 секунд после двух неудачных попыток входа в течение 120 секунд.
S1(config)# **login block-for 30 attempts 2 within 120** S1(config)# **end**

Вставьте скриншот выполненной работы

Шаг 5: Убедитесь, что все неиспользуемые порты отключены.

По умолчанию порты коммутатора включены. Отключите на коммутаторе все неиспользуемые порты. a. Состояние портов коммутатора можно проверить с помощью команды **show ip interface brief**.

S1# **show ip interface brief**

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	192.168.1.11	YES	manual	up	up
FastEthernet0/1	unassigned	YES	unset	down	down
FastEthernet0/2	unassigned	YES	unset	down	down
FastEthernet0/3	unassigned	YES	unset	down	down
FastEthernet0/4	unassigned	YES	unset	down	down
FastEthernet0/5	unassigned	YES	unset	up	up
FastEthernet0/6	unassigned	YES	unset	up	up
FastEthernet0/7	unassigned	YES	unset	down	down
FastEthernet0/8	unassigned	YES	unset	down	down
FastEthernet0/9	unassigned	YES	unset	down	down
FastEthernet0/10	unassigned	YES	unset	down	down
FastEthernet0/11	unassigned	YES	unset	down	down
FastEthernet0/12	unassigned	YES	unset	down	down
FastEthernet0/13	unassigned	YES	unset	down	down
FastEthernet0/14	unassigned	YES	unset	down	down
FastEthernet0/15	unassigned	YES	unset	down	down
FastEthernet0/16	unassigned	YES	unset	down	down
FastEthernet0/17	unassigned	YES	unset	down	down
FastEthernet0/18	unassigned	YES	unset	down	down
FastEthernet0/19	unassigned	YES	unset	down	down
FastEthernet0/20	unassigned	YES	unset	down	down
FastEthernet0/21	unassigned	YES	unset	down	down
FastEthernet0/22	unassigned	YES	unset	down	down
FastEthernet0/23	unassigned	YES	unset	down	down

FastEthernet0/24 unassigned YES unset down down
GigabitEthernet0/1 unassigned YES unset down down GigabitEthernet0/2
unassigned YES unset down down
S1#

Вставьте скриншот выполненной работы

b. Чтобы отключить сразу несколько интерфейсов, воспользуйтесь командой **interface range**.
S1(config)# **interface range f0/1–4 , f0/7-24 , g0/1-2**
S1(config-if-range)# **shutdown**
S1(config-if-range)# **end**
S1#

Вставьте скриншот выполненной работы

c. Убедитесь, что все неактивные интерфейсы отключены администратором.
S1# **show ip interface brief**

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	192.168.1.11	YES	manual	up	up
FastEthernet0/1	unassigned	YES	unset	administratively down	down
FastEthernet0/2	unassigned	YES	unset	administratively down	down
FastEthernet0/3	unassigned	YES	unset	administratively down	down
FastEthernet0/4	unassigned	YES	unset	administratively down	down
FastEthernet0/5	unassigned	YES	unset	up	up
FastEthernet0/6	unassigned	YES	unset	up	up
FastEthernet0/7	unassigned	YES	unset	administratively down	down
FastEthernet0/8	unassigned	YES	unset	administratively down	down
FastEthernet0/9	unassigned	YES	unset	administratively down	down
FastEthernet0/10	unassigned	YES	unset	administratively down	down
FastEthernet0/11	unassigned	YES	unset	administratively down	down
FastEthernet0/12	unassigned	YES	unset	administratively down	down
FastEthernet0/13	unassigned	YES	unset	administratively down	down
FastEthernet0/14	unassigned	YES	unset	administratively down	down
FastEthernet0/15	unassigned	YES	unset	administratively down	down
FastEthernet0/16	unassigned	YES	unset	administratively down	down
FastEthernet0/17	unassigned	YES	unset	administratively down	down
FastEthernet0/18	unassigned	YES	unset	administratively down	down
FastEthernet0/19	unassigned	YES	unset	administratively down	down
FastEthernet0/20	unassigned	YES	unset	administratively down	down
FastEthernet0/21	unassigned	YES	unset	administratively down	down
FastEthernet0/22	unassigned	YES	unset	administratively down	down
FastEthernet0/23	unassigned	YES	unset	administratively down	down
FastEthernet0/24	unassigned	YES	unset	administratively down	down
GigabitEthernet0/1	unassigned	YES	unset	administratively down	down
GigabitEthernet0/2	unassigned	YES	unset	administratively down	down

S1#

Вставьте скриншот выполненной работы

Шаг 6: Убедитесь, что все меры безопасности внедрены правильно.

a. Убедитесь, что протокол Telnet на коммутаторе отключен.

Вставьте скриншот выполненной работы

b. Подключитесь к коммутатору по протоколу SSH и намеренно укажите неверное имя пользователя и пароль, чтобы проверить, будет ли заблокирован доступ к системе.

Вставьте скриншот выполненной работы

c. По истечении 30 секунд повторите попытку подключения к R1 по протоколу SSH и войдите в систему, используя имя пользователя **SSHadmin** и пароль **Admin1p@55**. Появился ли баннер после успешного входа в систему?

Ответ:_____

d. Войдите в привилегированный режим EXEC, используя **Enablep@55** в качестве пароля.

Вставьте скриншот выполненной работы

Введите команду **show running-config** в строке приглашения привилегированного режима EXEC для просмотра установленных параметров безопасности.

Вставьте скриншот выполненной работы

Эталон ответа:

Задание 1. Настройка основных параметров устройств

- Router>enable*//Входим в привилегированный режим.*
- Router#
- Router#erase startup-config*//Очищаем маршрутизатор от предыдущих настроек.*
- Router#reload*//Перезагружаем маршрутизатор.*
- Would you like to enter the initial configuration dialog? [yes/no]: no*// Отказываемся.*
- Router>enable*//Снова входим в привилегированный режим.*
- Router#
- Router#configure terminal*//входим в режим глобальной конфигурации*
- Router(config)#hostname R1*//даём имя маршрутизатору, в данном случае R1*
- R1(config)#no ip domain-lookup*//выключаем поиск DNS*
- R1(config)#enable secret class*//включаем пароль на вход привилегированного режима*
- R1(config)#banner motd #*//Настраиваем сообщение дня (message of the day). Между знаками "#" пишем сообщение.*
  !!!ACCESS DENIED!!!
  #
- R1(config)#line console 0*//Входим в режим настройки консоли.*
- R1(config-line)#password cisco*//Назначаем пароль на вход.*
- R1(config-line)#login*//Включаем запрос пароля перед входом в консоль.*
- R1(config-line)#exit
- R1(config)#line vty 0 4*//Входим в режим настройки телнета.*
- R1(config-line)#password cisco*//Назначаем пароль на вход.*
- R1(config-line)#login*//Включаем запрос пароля перед входом с помощью телнета.*
- R1(config-line)#end
- R1#show running-config*//Проверяем введенные данные.*

- R1#copy running-config startup-config*//Сохраняем произведенную настройку в энерго-независимую память.*
- R1#configure terminal*//снова заходим в режим глобальной конфигурации*
- R1(config)#interface fastethernet 0/0*//заходим в режим конфигурации интерфейса*
- R1(config-if)#ip address 192.168.0.1 255.255.255.128*//назначаем IP-адрес интерфейсу и маску 255.255.255.128 (эта маска является расшифровкой префикса /25)*
- R1(config-if)#des Subnet A*//краткое описание интерфейса*
- R1(config-if)#no shutdown*//включаем интерфейс*
- R1(config)#interface fastethernet 0/1*//заходим в режим конфигурации интерфейса*
- R1(config-if)#ip address 192.168.0.129 255.255.255.192*//назначаем IP-адрес интерфейсу и маску 255.255.255.128 (эта маска является расшифровкой префикса /25)*
- R1(config-if)#des Subnet B*//краткое описание интерфейса*
- R1(config-if)#no shutdown*//включаем интерфейс*
- R1(config)#interface serial 0/0/0*//заходим в режим конфигурации интерфейса*
- R1(config-if)#ip address 192.168.0.193 255.255.255.252*//назначаем IP-адрес интерфейсу и маску 255.255.255.128 (эта маска является расшифровкой префикса /25)*
- R1(config-if)#des Link to R2*//краткое описание интерфейса*
- R1(config-if)#clock rate 64000*//задаем время сигнала для синхронизации со вторым роутером.*
- R1(config-if)#no shutdown*//включаем интерфейс*
- R1(config-line)#end*//выходим в привилегированный режим EXEC Mode*
- R1#show running-config*//Проверяем введенные данные.*
- R1#copy running-config startup-config*//Сохраняем произведенную настройку в энерго-независимую память.*.

Задание 2. Настройка базовых мер безопасности на маршрутизаторе

Шаг 1: Зашифруйте открытые пароли.

R1(config)# **service password-encryption** *//Зашифровываем пароли*

Шаг 2: Установите более надежные пароли.

R1(config)# **enable secret Enablep@55** *//установил зашифрованный пароль*

R1(config)# **security passwords min-length 10** *// Установил минимальную длину 10 символов*

Шаг 3: Разрешите подключения по протоколу SSH.

R1(config)# **ip domain-name CCNA-lab.com** *//В качестве имени домена указал CCNA-lab.com*

R1(config)# **username SSHadmin privilege 15 secret Admin1p@55** *//учётка для подключения к маршрутизатору через SSH*

R1(config)# **line vty 0 4**

R1(config-line)# **transport input ssh** *//доступ только по протоколу SSH*

R1(config-line)# **login local** *//Аутентификация выполняется с использованием базы данных локальных пользователей*

R1(config-line)# **exit**

R1(config)# **crypto key generate rsa modulus 1024** *//ключ шифрования RSA с длиной 1024 бит*

Шаг 4: Обеспечьте защиту консоли и линий VTY.

R1(config)# **line console 0**

R1(config-line)# **exec-timeout 5 0** *//отключение сеанса линии связи через пять минут отсутствия активности.*

R1(config-line)# **line vty 0 4**

R1(config-line)# **exec-timeout 5 0** *//отключение сеанса линии связи через пять минут отсутствия активности.*
R1(config-line)# **exit**
R1(config)#
R1(config)# **login block-for 30 attempts 2 within 120**

Что означает **2 within 120** в приведенной выше команде?

Ответ: Маршрутизатор блокирует попытки входа в систему, если в течение 120 секунд будет дважды введен неверный пароль

Что означает **block-for 30** в приведенной выше команде?
Ответ: Маршрутизатор блокирует попытки входа в систему на 30 секунд

Шаг 5: Убедитесь, что все неиспользуемые порты отключены.
R1# **show ip interface brief** *//проверяем все неиспользуемые порты*
Interface IP-Address OK? Method Status Protocol
Embedded-Service-Engine0/0 unassigned YES NVRAM administratively down down
GigabitEthernet0/0 unassigned YES NVRAM administratively down down
GigabitEthernet0/1 192.168.1.1 YES manual up up
Serial0/0/0 unassigned YES NVRAM administratively down down Serial0/0/1
unassigned YES NVRAM administratively down down
R1#

Шаг 6: Убедитесь, что все меры безопасности внедрены правильно.

g. С помощью программы Tera Term подключитесь к маршрутизатору R1 по протоколу Telnet.
Разрешает ли R1 подключение по протоколу Telnet? Дайте пояснение.
Ответ: Нет, только по SSH

h. С помощью программы Tera Term подключитесь к маршрутизатору R1 по протоколу SSH. Разрешает ли R1 подключение по протоколу SSH?
Ответ: Да, разрешает

i. Намеренно укажите неверное имя пользователя и пароль, чтобы проверить, будет ли заблокирован доступ к системе после двух неудачных попыток.
Что произошло после ввода неправильных данных для входа в систему во второй раз?
Ответ: Появится сообщение !!!ACCESS DENIED!!!

j. Из сеанса подключения к маршрутизатору с помощью консоли отправьте команду **show login**, чтобы проверить состояние входа в систему.
R1# **show login**
A default login delay of 1 second is applied.
No Quiet-Mode access list has been configured.
Router enabled to watch for login Attacks.
If more than 2 login failures occur in 120 seconds or less, logins will
be disabled for 30 seconds.
Router presently in Quiet-Mode.
Will remain in Quiet-Mode for 14 seconds.

Denying logins from all sources. *// Маршрутизатор не будет разрешать попытки входа в систему в течение еще 14 секунд*

R1#

k. По истечении 30 секунд повторите попытку подключения к R1 по протоколу SSH и войдите в систему, используя имя **SSHadmin** и пароль **Admin1p@55**. Что отобразилось после успешного входа в систему?

Ответ: приветственный баннер и R1>

l. Войдите в привилегированный режим EXEC и введите в качестве пароля **Enablep@55**.

Если вы неправильно вводите пароль, прерывается ли сеанс SSH после двух неудачных попыток в течение 120 секунд? Дайте пояснение.

Ответ: вход в систему будет заблокирован на 30 минут

Задание 3. Настройка базовых мер безопасности на коммутаторе

Шаг 1: Зашифруйте открытые пароли.

S1(config)# **service password-encryption** *//Зашифровываем пароли*

Шаг 2: Установите более надежные пароли на коммутаторе.

S1(config)# **enable secret Enablep@55** *//установил зашифрованный пароль*

Шаг 3: Разрешите подключения по протоколу SSH.

S1(config)# **ip domain-name CCNA-lab.com** *//В качестве имени домена указал CCNA-lab.com*

S1(config)# **username SSHadmin privilege 1 secret Admin1p@55** *//учётка для подключения к маршрутизатору через SSH*

S1(config)# **line vty 0 15**

S1(config-line)# **transport input ssh** *//доступ только по протоколу SSH*

S1(config-line)# **login local** *//Аутентификация выполняется с использованием базы данных локальных пользователей*

S1(config-line)# **exit**

S1(config)# **crypto key generate rsa modulus 1024** *//ключ шифрования RSA с длиной 1024 бит*

Шаг 4: Обеспечьте защиту консоли и линий VTY.

S1(config)# **line console 0**

S1(config-line)# **exec-timeout 10 0** *//отключение сеанса линии связи через десять минут отсутствия активности*

S1(config-line)# **line vty 0 15**

S1(config-line)# **exec-timeout 10 0** *//отключение сеанса линии связи через десять минут отсутствия активности*

S1(config-line)# **exit**

S1(config)#

S1(config)# **login block-for 30 attempts 2 within 120** *//блокировка входа на 30 минут если пароль дважды был введён неверно в течение 120 секунд*

S1(config)# **end**

Шаг 5: Убедитесь, что все неиспользуемые порты отключены.

S1# **show ip interface brief** *//проверяем все неиспользуемые порты*

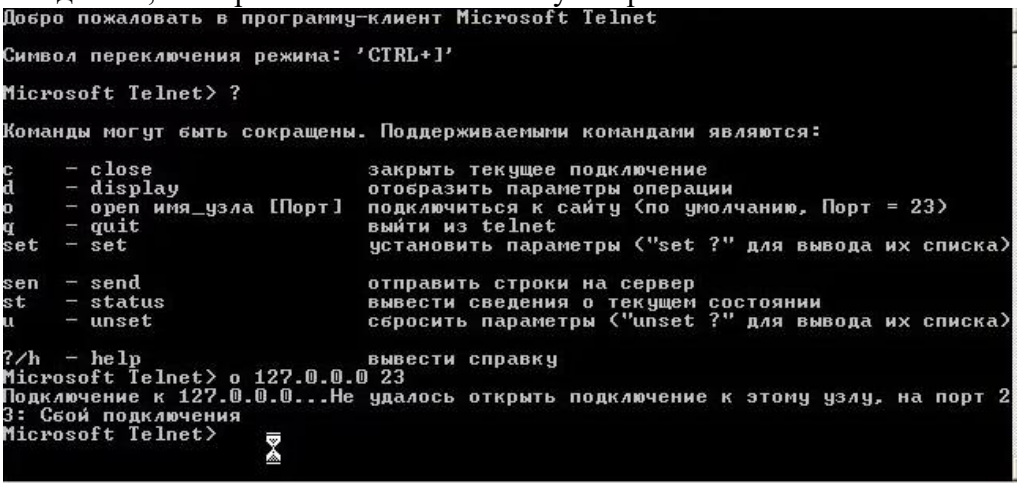
Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	192.168.1.11	YES	manual	up	up
FastEthernet0/1	unassigned	YES	unset	down	down

```
FastEthernet0/2       unassigned      YES unset  down                  down
FastEthernet0/3       unassigned      YES unset  down                  down
FastEthernet0/4       unassigned      YES unset  down                  down
FastEthernet0/5       unassigned      YES unset  up                    up
FastEthernet0/6       unassigned      YES unset  up                    up
FastEthernet0/7       unassigned      YES unset  down                  down
FastEthernet0/8       unassigned      YES unset  down                  down
FastEthernet0/9       unassigned      YES unset  down                  down
FastEthernet0/10      unassigned      YES unset  down                  down
FastEthernet0/11      unassigned      YES unset  down                  down
FastEthernet0/12      unassigned      YES unset  down                  down
FastEthernet0/13      unassigned      YES unset  down                  down
FastEthernet0/14      unassigned      YES unset  down                  down
FastEthernet0/15      unassigned      YES unset  down                  down
FastEthernet0/16      unassigned      YES unset  down                  down
FastEthernet0/17      unassigned      YES unset  down                  down
FastEthernet0/18      unassigned      YES unset  down                  down
FastEthernet0/19      unassigned      YES unset  down                  down
FastEthernet0/20      unassigned      YES unset  down                  down
FastEthernet0/21      unassigned      YES unset  down                  down
FastEthernet0/22      unassigned      YES unset  down                  down
FastEthernet0/23      unassigned      YES unset  down                  down
FastEthernet0/24      unassigned      YES unset  down                  down
GigabitEthernet0/1    unassigned      YES unset  down                  down
GigabitEthernet0/2    unassigned      YES unset  down                  down
S1#
S1(config)# interface range f0/1–4 , f0/7-24 , g0/1-2 //отключаем сразу несколько интерфейсов
S1(config-if-range)# shutdown
S1(config-if-range)# end
S1#
S1# show ip interface brief //проверяем все неиспользуемые порты
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  192.168.1.11    YES manual up                    up
FastEthernet0/1        unassigned      YES unset  administratively down down
FastEthernet0/2        unassigned      YES unset  administratively down down
FastEthernet0/3        unassigned      YES unset  administratively down down
FastEthernet0/4        unassigned      YES unset  administratively down down
FastEthernet0/5        unassigned      YES unset  up                    up
FastEthernet0/6        unassigned      YES unset  up                    up
FastEthernet0/7        unassigned      YES unset  administratively down down
FastEthernet0/8        unassigned      YES unset  administratively down down
FastEthernet0/9        unassigned      YES unset  administratively down down
FastEthernet0/10       unassigned      YES unset  administratively down down
FastEthernet0/11       unassigned      YES unset  administratively down down
```

```
FastEthernet0/12       unassigned      YES unset  administratively down down
FastEthernet0/13       unassigned      YES unset  administratively down down
FastEthernet0/14       unassigned      YES unset  administratively down down
FastEthernet0/15       unassigned      YES unset  administratively down down
FastEthernet0/16       unassigned      YES unset  administratively down down
FastEthernet0/17       unassigned      YES unset  administratively down down
FastEthernet0/18       unassigned      YES unset  administratively down down
FastEthernet0/19       unassigned      YES unset  administratively down down
FastEthernet0/20       unassigned      YES unset  administratively down down
FastEthernet0/21       unassigned      YES unset  administratively down down
FastEthernet0/22       unassigned      YES unset  administratively down down
FastEthernet0/23       unassigned      YES unset  administratively down down
FastEthernet0/24       unassigned      YES unset  administratively down down
GigabitEthernet0/1     unassigned      YES unset  administratively down down
GigabitEthernet0/2     unassigned      YES unset  administratively down down
S1#
```

Шаг 6: Убедитесь, что все меры безопасности внедрены правильно.

e. Убедитесь, что протокол Telnet на коммутаторе отключен.



f. Подключитесь к коммутатору по протоколу SSH и намеренно укажите неверное имя пользователя и пароль, чтобы проверить, будет ли заблокирован доступ к системе.

```
banner motd ^C
!!!ACCESS DENIED!!!
```

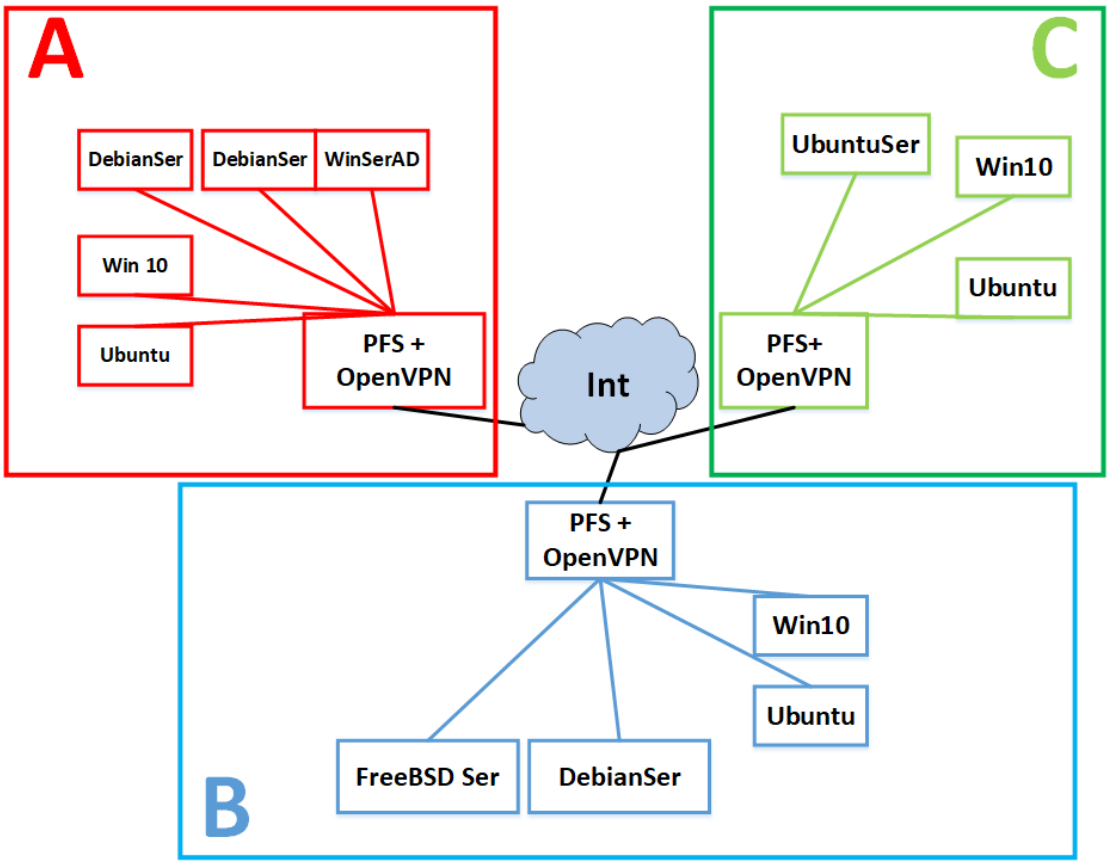
g. По истечении 30 секунд повторите попытку подключения к R1 по протоколу SSH и войдите в систему, используя имя пользователя **SSHadmin** и пароль **Admin1p@55**. Появился ли баннер после успешного входа в систему?

Ответ: _ приветственный баннер и S1>

h. Войдите в привилегированный режим EXEC, используя **Enablep@55** в качестве пароля.

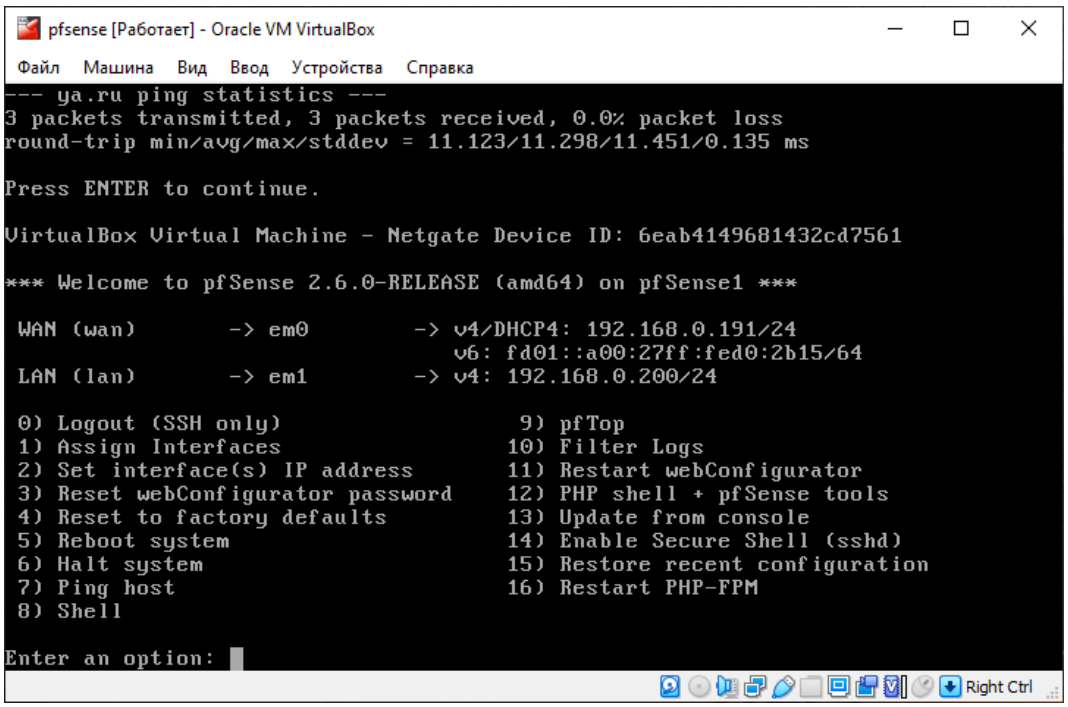
Router> **enable**
Password:<**Enablep@55**>
Router#

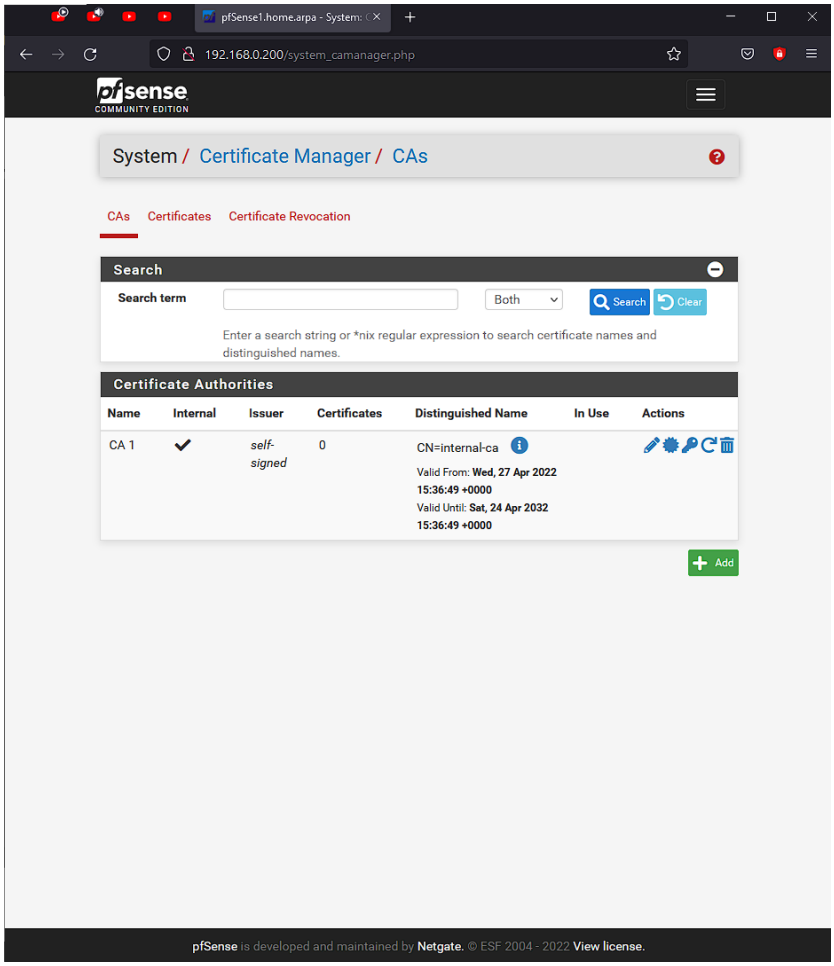
Задание:
Продумать IP-адресацию сети. Создать логическую схему сети и таблицу адресации. Построить компьютерную сеть организации.



Практическое занятие №41. Настройка Microtik на базе Router ОС

Задание:
Продумать IP-адресацию сети. Создать логическую схему сети и таблицу адресации. Построить компьютерную сеть организации.





1. Добавьте виртуальную машину с Router OS в VB.

2. Установите маршрутизатор Router OS, дождитесь полной загрузки виртуальной машины. Не забудьте подключить сетевой мост.

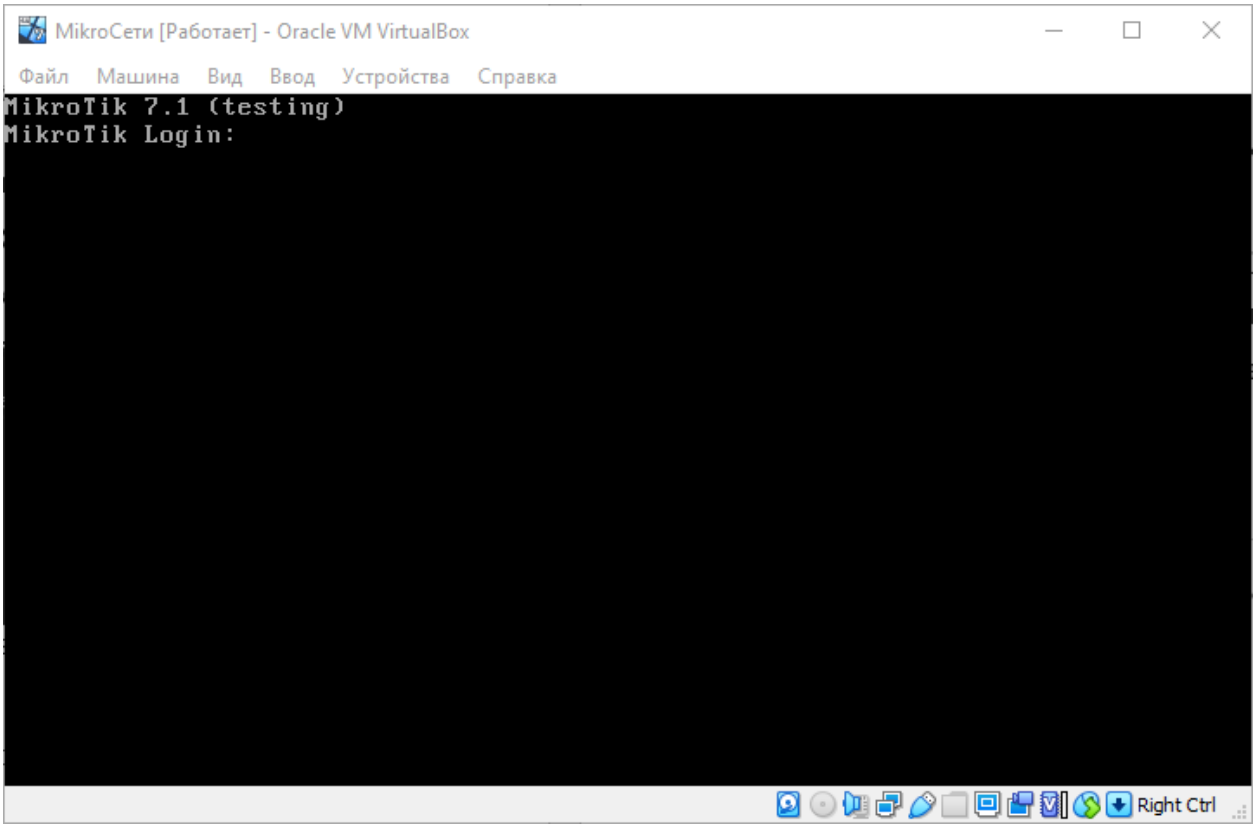
3. Смените логин/пароль для администратора на более надежный. Добавьте дополнительного администратора, установив ему сложный пароль.

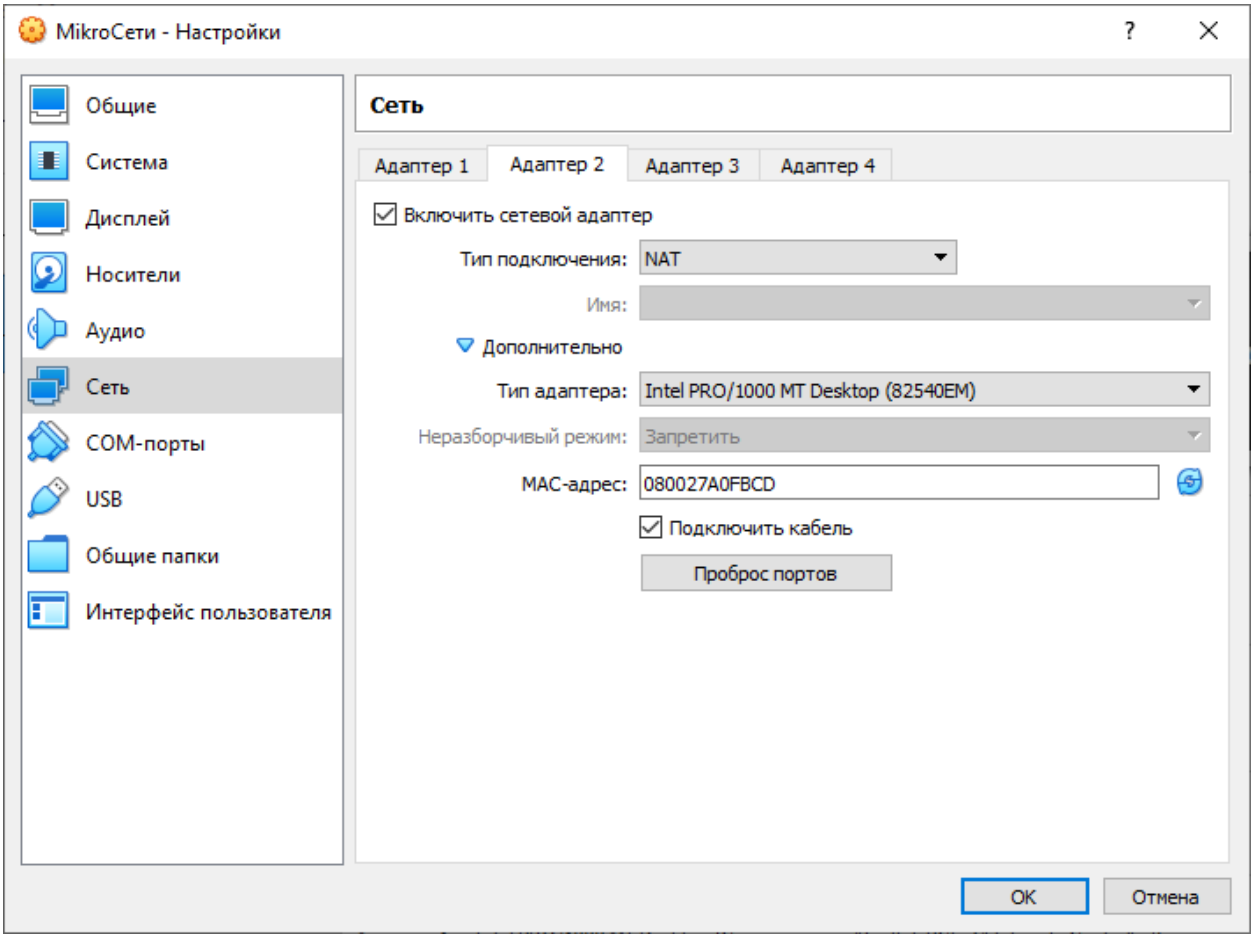
4. Сделайте бэкап машины.
5. Настройте IP-адреса на интерфейсах машины.
6. Отключите лишние включенные сервисы.
7. Настройке Vlan для включенных интерфейсов.
8. Настройте DHCP-пулы.
9. Сделайте повторный бэкап машины.

Эталон ответа:

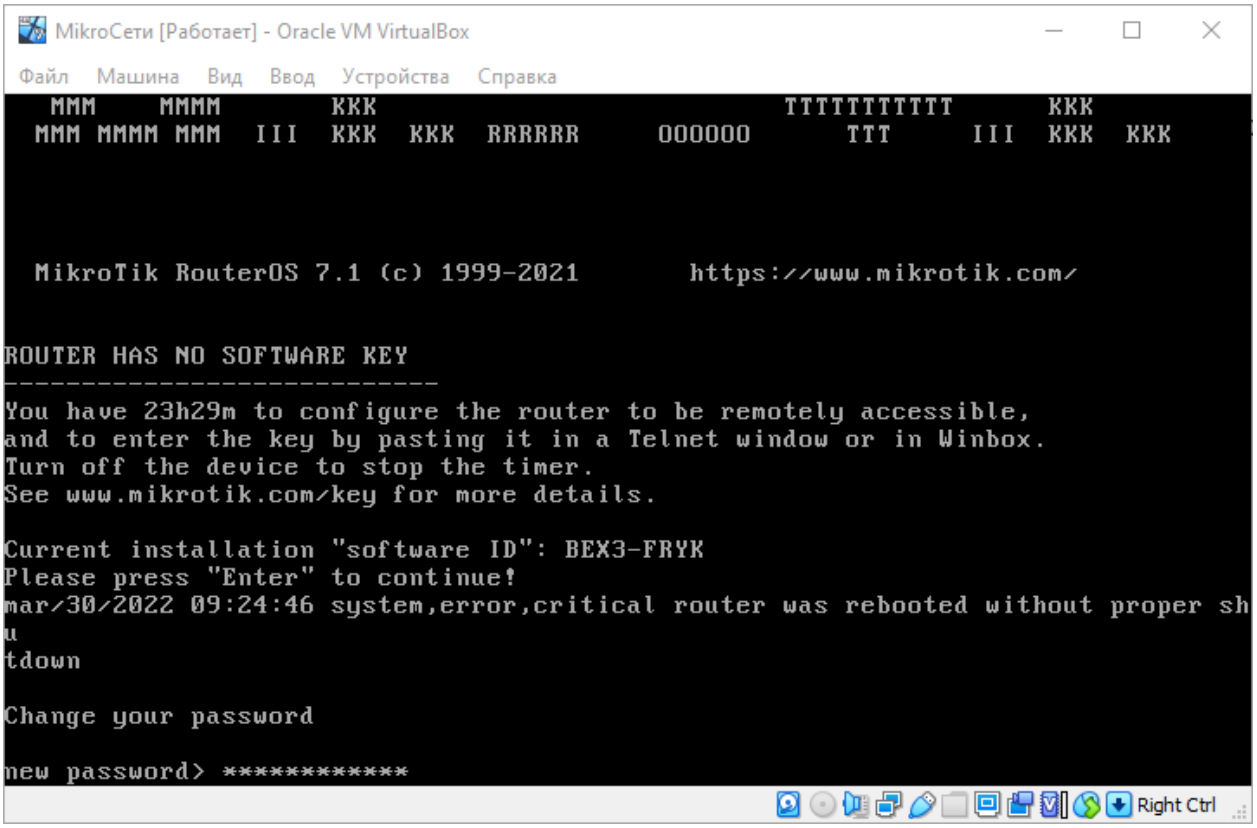
Задания:

1. Добавьте виртуальную машину с Router OS в VB.
2. Установите маршрутизатор Router OS, дождитесь полной загрузки виртуальной машины. Не забудьте подключить сетевой мост.

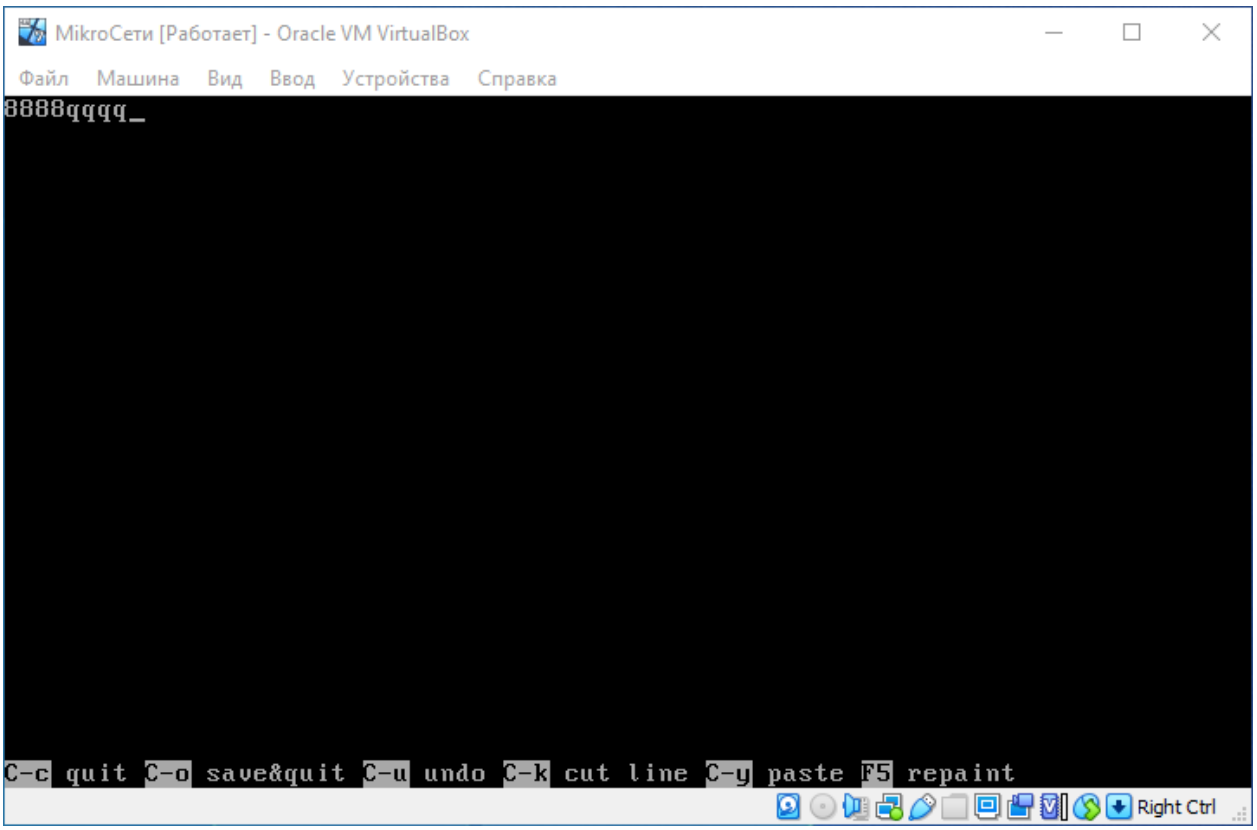

MikroСети [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
MikroTik 7.1 (testing)
MikroTik Login:
Right Ctrl


MikroСети - Настройки
Общие
Система
Дисплей
Носители
Аудио
Сеть
COM-порты
USB
Общие папки
Интерфейс пользователя
Сеть
Адаптер 1
Адаптер 2
Адаптер 3
Адаптер 4
Включить сетевой адаптер
Тип подключения: NAT
Имя:
Дополнительно
Тип адаптера: Intel PRO/1000 MT Desktop (82540EM)
Неразборчивый режим: Запретить
MAC-адрес: 080027A0FBCD
Подключить кабель
Проброс портов
OK
Отмена

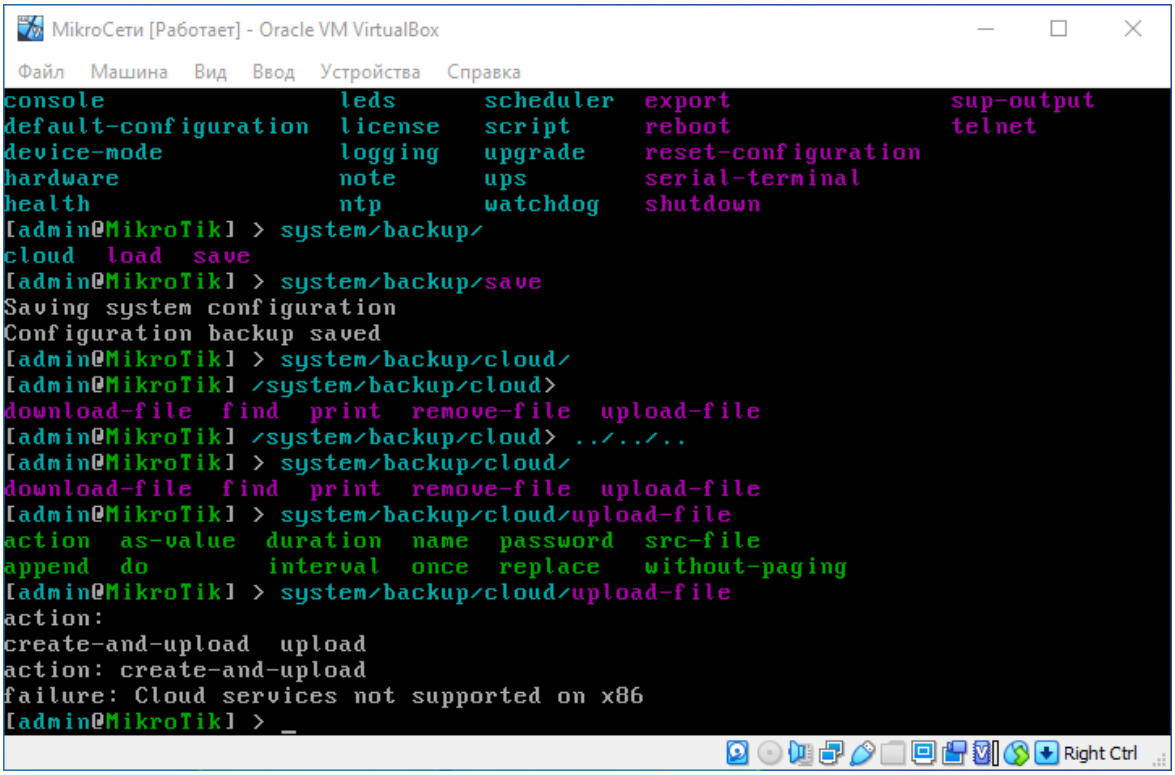
3. Смените логин/пароль для администратора на более надежный. Добавьте дополнительного администратора, установив ему сложный пароль.



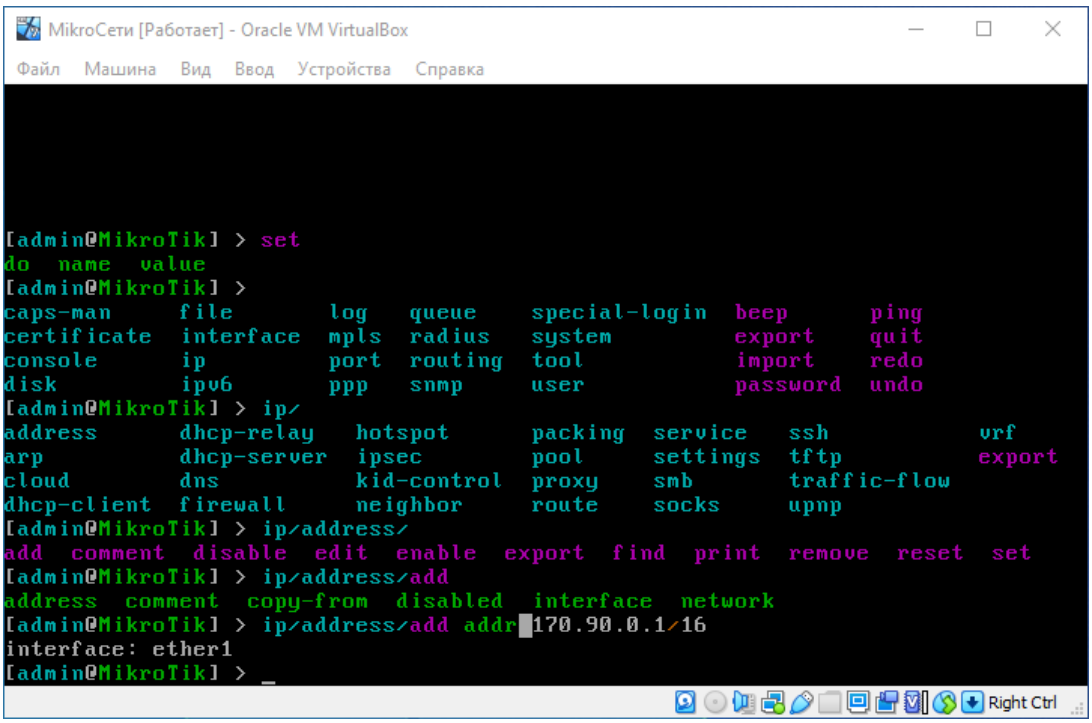

```
[admin@MikroTik] /user> add
name: administrator
group:
full  read  write
group: full
```



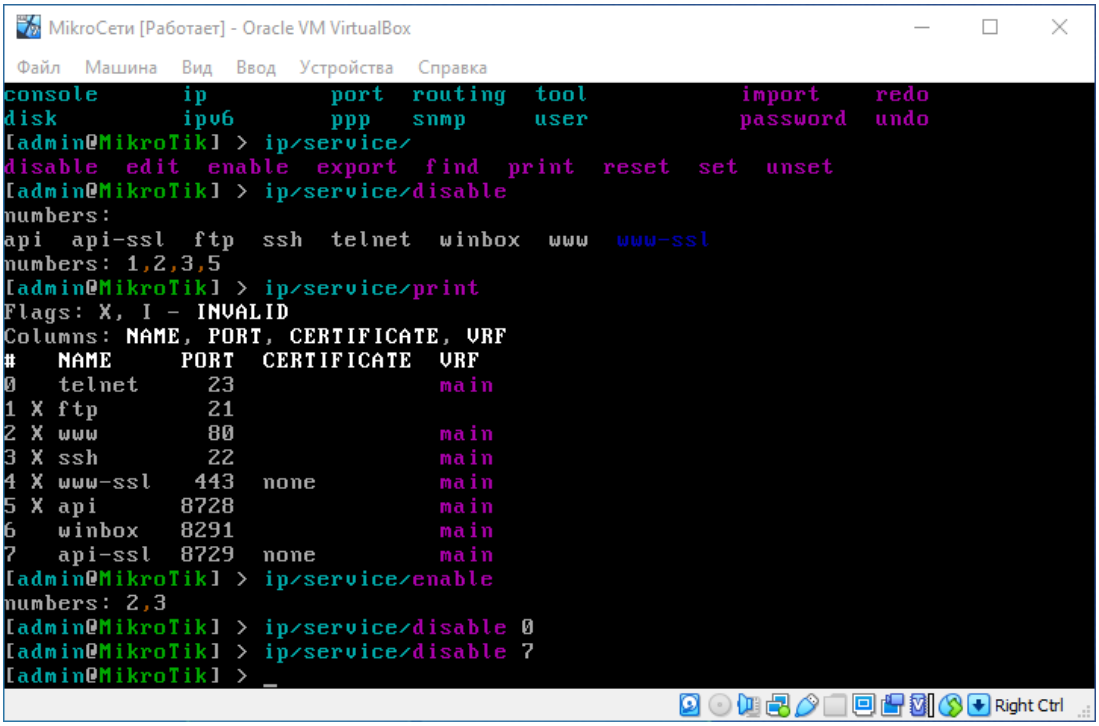
4. Сделайте бэкап машины.

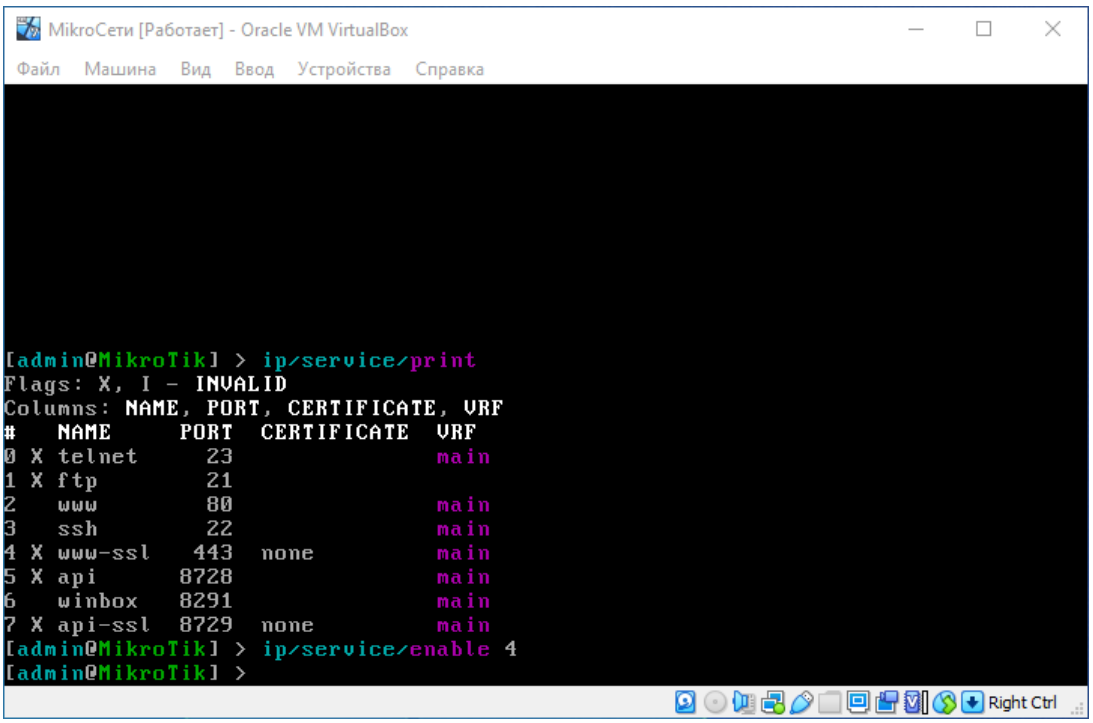


5. Настройте IP-адреса на интерфейсах машины.

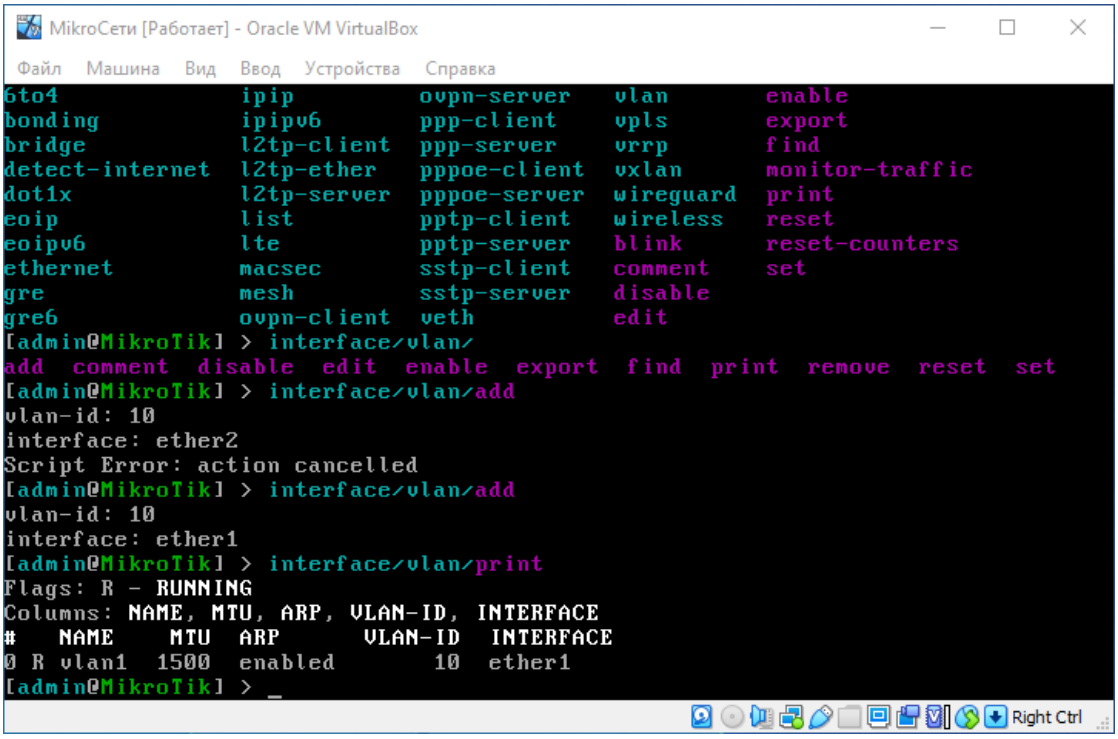


6. Отключите лишние включенные сервисы.

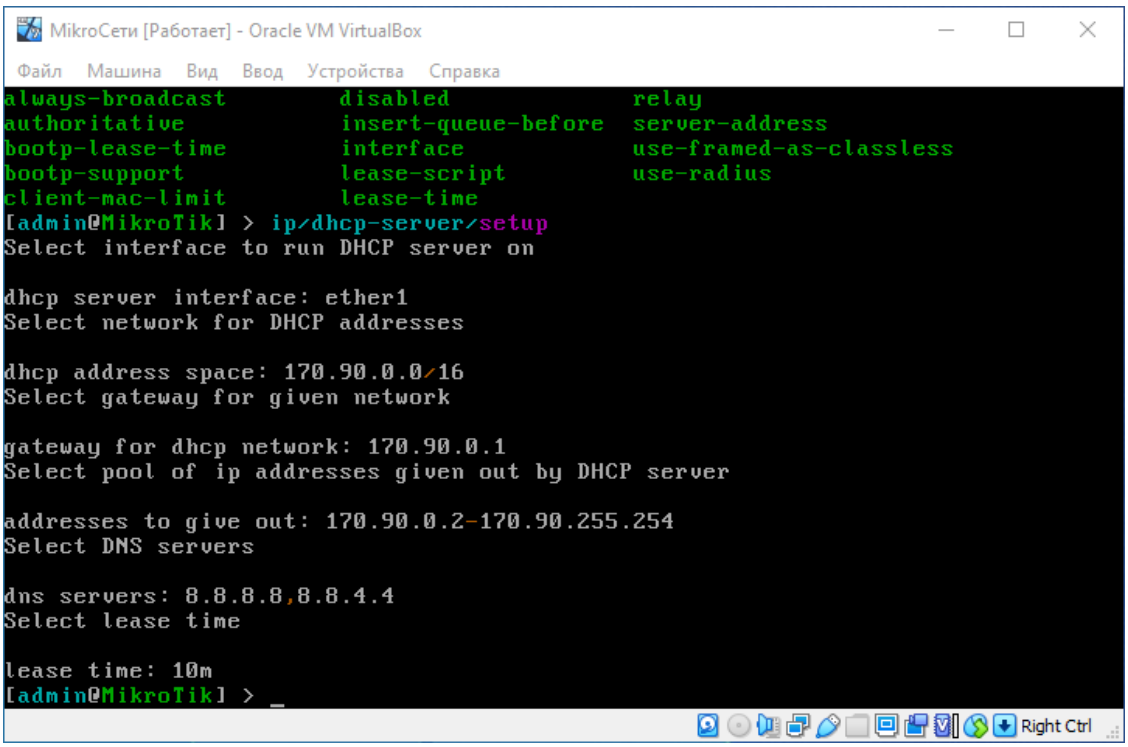




7. Настройке Vlan для включенных интерфейсов.



8. Настройте DHCP-пулы.



9. Сделайте повторный бэкап машины.

Практическое занятие №58. Использование CMS для размещения информации в локальных и глобальных компьютерных сетях.

Скачать и распаковать в директорию var/www CMS –WordPress на Ubuntu Server в сети C.

Настройте виртуальные хосты в Apache.

Настройка CMS:

— Установить CMS WordPress. Во время установки укажите название и описание сайта в соответствии с вариантом;
— Используя инструменты WordPress создайте одностраничный сайт по теме из варианта.

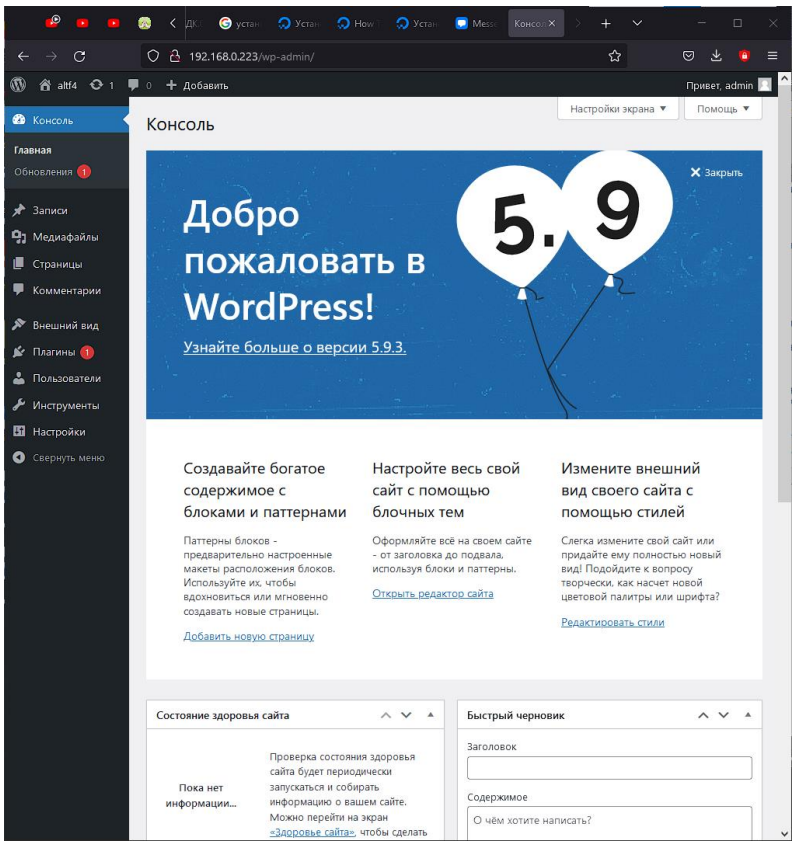
Скачать CMS –WordPress на Debian Server в сети C.

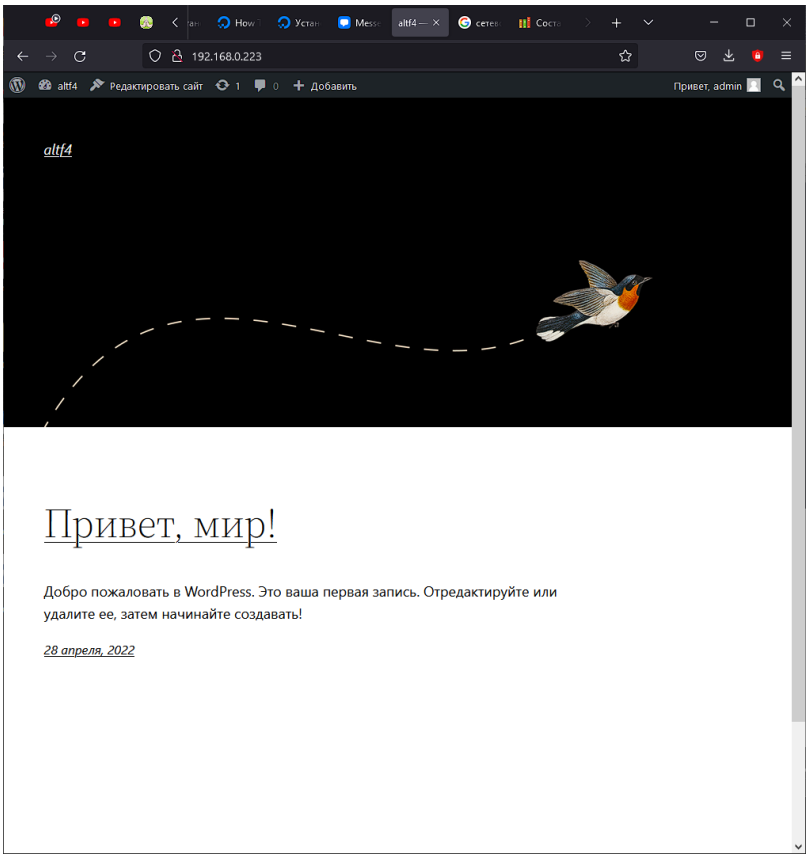
Настройте виртуальные хосты в Nginx.

Настройка CMS:

— *Установить CMS WordPress. Во время установки укажите название и описание сайта в соответствии с вариантом;*
— *Используя инструменты WordPress создайте одностраничный сайт по теме из варианта.*

Эталон ответа:


192.168.0.223/wp-admin/
altf4
Добавить
Привет, admin
Консоль
Главная
Обновления
Записи
Медиафайлы
Страницы
Комментарии
Внешний вид
Плагины
Пользователи
Инструменты
Настройки
Свернуть меню
Консоль
Настройки экрана
Помощь
Закрыть
Добро пожаловать в WordPress!
Узнайте больше о версии 5.9.3.
5.9
Создавайте богатое содержимое с блоками и паттернами
Паттерны блоков - предварительно настроенные макеты расположения блоков. Используйте их, чтобы вдохновиться или мгновенно создавать новые страницы.
Добавить новую страницу
Настройте весь свой сайт с помощью блочных тем
Оформляйте всё на своем сайте - от заголовка до подвала, используя блоки и паттерны.
Открыть редактор сайта
Измените внешний вид своего сайта с помощью стилей
Слегка измените свой сайт или придайте ему полностью новый вид! Подойдите к вопросу творчески, как насчет новой цветовой палитры или шрифта?
Редактировать стили
Состояние здоровья сайта
Пока нет информации...
Проверка состояния здоровья сайта будет периодически запускаться и собирать информацию о вашем сайте. Можно перейти на экран «Здоровье сайта», чтобы сделать
Быстрый черновик
Заголовок
Содержимое
О чём хотите написать?


192.168.0.223
altf4
Редактировать сайт
Добавить
Привет, admin
altf4
Привет, мир!
Добро пожаловать в WordPress. Это ваша первая запись. Отредактируйте или удалите ее, затем начинайте создавать!
28 апреля, 2022

3.1.2. Оценка освоения теоретического курса профессионального модуля по МДК.01.02

Дидактические единицы	Проверяемые ОК, ПК, У, З	Формы контроля (наименование контрольной точки)		
		Текущая аттестация		Промежуточная аттестация
Тема 2.1. Маршрутизация и коммутация. Масштабирование сетей.	У8, З1, З3, ОК1-ОК11 ПК 1.1	Практическая работа № 1. Определение топологии и протоколов для указанной сети	Устный зачет по теме 2.1	Теоретические вопросы на дифференцированном зачете
	У7, З1, З6, ОК1-ОК11 ПК 1.4	Практическая работа № 2. Поиск аналогов устаревшего оборудования		
	У2, З1, З5, ОК1-ОК11 ПК 1.2	Практическая работа № 4. Настройка беспроводного маршрутизатора и клиента		
Тема 2.2. Проектирование компьютерных сетей	У8, УЗ, З5 ОК1-ОК12 ПК 1.5	Практическая работа № 7. Проектирование подсистемы рабочего места.	Устный зачет по теме 2.2	
Тема 2.3. Соединение сетей. Маршрутизация	У7, З1, З6, ОК1-ОК11 ПК 1.3	Практическая работа № 18. Защита информации в сетях	Устный зачет по теме 2.3	

Устный зачет по теме 1

Инструкция для обучающихся

Зачет сдается в рамках учебного занятия. Каждый студент отвечает в устной форме на предложенные преподавателем 7 мини-вопросов.

Выполнение задания: одному студенту на ответ выделяется 3 мин., группа сдает зачет за одно учебное занятие.

Перечень вопросов:

1. Кто создает статическую маршрутизацию??

2. Каковы преимущества и недостатки статической маршрутизации по сравнению с динамической?
3. При подключении к Интернету какие маршруты обычно конфигурируется на граничном маршрутизаторе провайдера?
4. Что собой представляет технология CEF?
5. Что такое метрика сети?
6. Как работает broadcast?
7. Что что такое таблицы маршрутизации?

Эталоны ответов: приведены в учебном пособии по МДК.01.02 «Организация, принципы построения и функционирования компьютерных сетей».

1. Практическая работа № 2 «Определение топологии и протоколов для указанной сети»

Инструкция для обучающихся

Внимательно прочитайте задание. Проведите обследование объектов на предмет состояния инженерно-технического укрепления.

Время выполнения – 90 минут.

Задание

1. Изучить теоретический материал по определению топологии и протоколов для указанной сети
2. Можно ли определить топологию сети средствами OS Windows? Если можно, то опишите эти средства.
3. Дать ответы на вопросы:
    1. Дайте определение топологии.
    2. Опишите физические топологии.
    3. Опишите логические топологии.
    4. Перечислите программные средства для определения топологии сети, опишите функции трех программных средств.
4. Сделать выводы о проделанной работе.

Эталон ответа:

Сетевая топология (от греч. τόπος, - место) — способ описания конфигурации сети, схема расположения и соединения сетевых устройств.
Топология –
это схема соединения каналами связи компьютеров или узлов сети между собой.
Сетевая топология может быть

- ***физической*** — описывает реальное расположение и связи между узлами сети.
- ***логической*** — описывает хождение сигнала в рамках физической топологии.
- ***информационной*** — описывает направление потоков информации, передаваемых по сети.

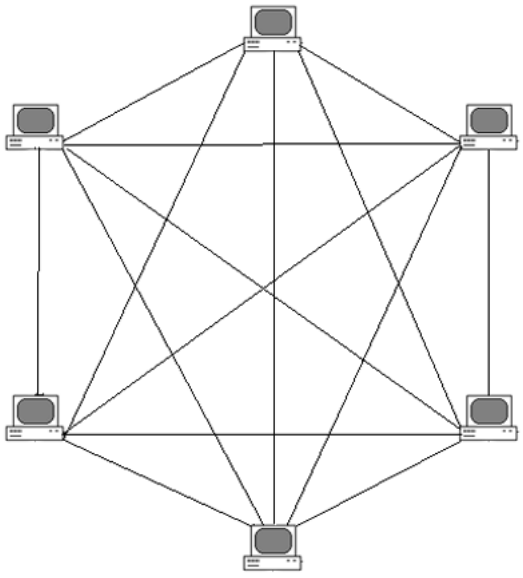
- ***управления обменом*** — это принцип передачи права на пользование сетью.

Существует множество способов соединения сетевых устройств. Выделяют следующие топологии:

- полносвязная
- ячеистая
- общая шина
- звезда
- кольцо
- снежинка

Рассмотрим каждую из них по подробнее.

1) Полносвязная топология — топология компьютерной сети, в которой каждая рабочая станция подключена ко всем остальным. Этот вариант является громоздким и неэффективным, несмотря на свою логическую простоту. Для каждой пары должна быть выделена независимая линия, каждый компьютер должен иметь столько коммуникационных портов сколько компьютеров в сети. По этим причинам сеть

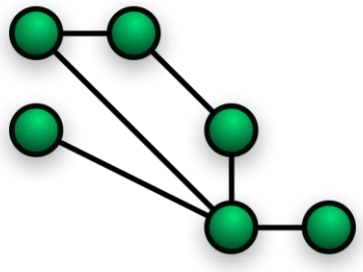


может иметь только сравнительно небольшие конечные размеры. Чаще всего эта топология используется в многомашинных комплексах или глобальных сетях при малом количестве рабочих станций.

Технология доступа в сетях этой топологии реализуется методом передачи маркера. Маркер – это пакет, снабженный специальной последовательностью бит (его можно сравнить с конвертом для письма). Он последовательно предается по кольцу от компьютера к компьютеру в одном направлении. Каждый узел ретранслирует передаваемый маркер. Компьютер может передать свои данные, если он получил пустой маркер. Маркер с пакетом передается, пока не обнаружится компьютер, которому предназначен пакет. В этом компьютере данные принимаются, но маркер движется дальше и возвращается к отправителю.
После того, как отправивший пакет компьютер убедится, что пакет доставлен адресату, маркер освобождается.

Недостаток: громоздкий и неэффективный вариант, т.к. каждый компьютер должен иметь большое кол-во коммуникационных портов.

2) Ячеистая топология - базовая полносвязная топология компьютерной сети, в которой каждая рабочая станция сети соединяется с несколькими другими рабочими станциями этой же сети. Характеризуется высокой отказоустойчивостью, сложностью настройки и переизбыточным расходом кабеля. Каждый компьютер имеет множество возможных путей соединения с другими компьютерами. Обрыв кабеля не приведёт к потере соединения между двумя компьютерами.



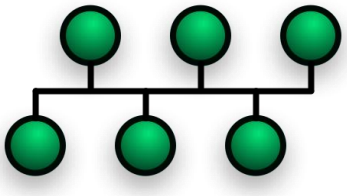
Получается из полносвязной путем удаления некоторых возможных связей. Эта топология допускает соединение большого количества компьютеров и характерна, как правило, для крупных сетей.

3) Общая шина, представляет собой общий кабель (называемый шина или магистраль), к которому подсоединены все рабочие станции. На концах кабеля находятся терминаторы, для предотвращения отражения сигнала.

Сравнение с другими топологиями.

Достоинства:

- Небольшое время установки сети;
- Дешевизна (требуется меньше кабеля и сетевых устройств);
- Простота настройки;
- Выход из строя рабочей станции не отражается на работе сети.

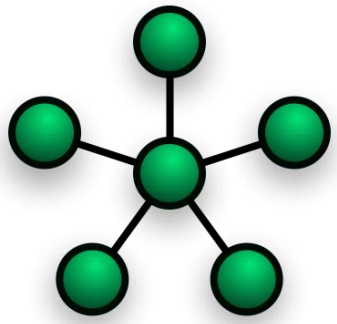


Недостатки:

- Неполадки в сети, такие как обрыв кабеля и выход из строя терминатора, полностью блокируют работу всей сети;
- Сложная локализация неисправностей;
- С добавлением новых рабочих станций падает производительность сети.

Шинная топология представляет собой топологию, в которой все устройства локальной сети подключаются к линейной сетевой среде передачи данных. Такую линейную среду часто называют каналом, шиной или трассой. Каждое устройство, например, рабочая станция или сервер, независимо подключается к общему шинному кабелю с помощью специального разъема. Шинный кабель должен иметь на конце согласующий резистор, или терминатор, который поглощает электрический сигнал, не давая ему отражаться и двигаться в обратном направлении по шине.

4) Звезда - базовая топология компьютерной сети, в которой все компьютеры сети присоединены к центральному узлу (обычно коммутатор), образуя физический сегмент сети. Подобный сегмент сети может функционировать как отдельно, так и в составе сложной сетевой топологии (как правило, «дерево»). Весь обмен информацией идет исключительно через центральный компьютер, на который таким способом возлагается очень большая нагрузка, поэтому ничем другим, кроме сети, он заниматься не может. Как правило, именно центральный компьютер является самым мощным, и именно на него возлагаются все функции по управлению обменом. Никакие конфликты в сети с топологией звезда в принципе невозможны, потому что управление полностью централизовано.



Метод доступа реализуется с помощью технологии
Arcnet. Этот метод доступа также использует маркер для передачи данных. Маркер переда ет-
ся от компьютера к компьютеру в порядке возрастания адреса. Как и в кольцевой тополог ии, каждый компьютер регенерирует маркер.

Сравнение с другими топологиями.

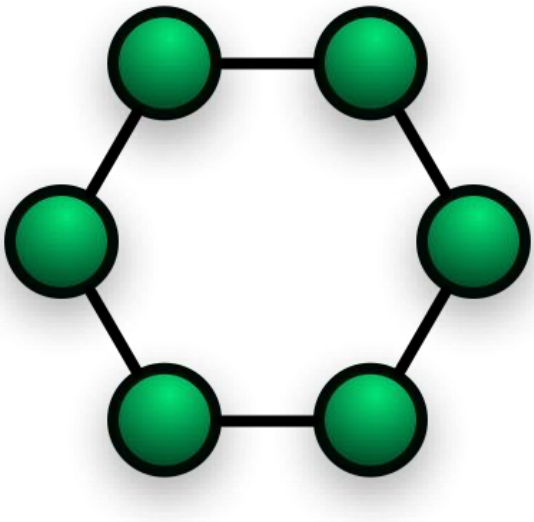
Достоинства:

- выход из строя одной рабочей станции не отражается на работе всей сети в целом;
- хорошая масштабируемость сети;
- лёгкий поиск неисправностей и обрывов в сети;
- высокая производительность сети (при условии правильного проектирования);
- гибкие возможности администрирования.

Недостатки:

- выход из строя центрального концентратора обернётся неработоспособностью сети (или сегмента сети) в целом;
- для прокладки сети зачастую требуется больше кабеля, чем для большинства других топологий;
- конечное число рабочих станций в сети (или сегменте сети) ограничено количеством портов в центральном концентраторе.

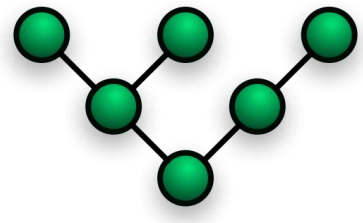
5) Кольцо - это топология, в которой каждый компьютер соединен линиями связи только с двумя другими: от одного он только получает информацию, а другому только передает. На каждой линии связи, как и в случае звезды, работает только один передатчик и один приемник. Это позволяет отказаться от применения внешних терминаторов.
Работа в сети кольца заключается в том, что каждый компьютер ретранслирует (возобновляет) сигнал, то есть выступает в роли повторителя, потому затухание сигнала во всем кольце не имеет никакого значения, важно только затухание между соседними компьютерами кольца. Четко выделенного центра в этом случае нет, все компьютеры могут быть одинаковыми. Однако достаточно часто в кольце выделяется специальный абонент, который управляет обменом или контролирует обмен. Понятно, что наличие такого управляющего абонента снижает надежность сети, потому что выход его из строя сразу же парализует весь обмен.



Компьютеры в кольце не являются полностью равноправными (в отличие, например, от шинной топологии). Одни из них обязательно получают информацию от компьютера, который ведет передачу в этот момент, раньше, а другие — позже. Именно на этой особенности топологии и строятся методы управления обменом по сети, специально рассчитанные на «кольцо». В этих методах право на следующую передачу (или, как еще говорят, на захват сети) переходит последовательно к следующему по кругу компьютеру.
Подключение новых абонентов в «кольцо» обычно совсем безболезненно, хотя и требует обязательной остановки работы всей сети на время подключения. Как и в случае топологии «шина», максимальное количество абонентов в кольце может быть достаточно большое (1000 и больше). Кольцевая топология обычно является самой стойкой к перегрузкам, она обеспечивает уверенную работу с самыми большими потоками переданной по сети

информации, потому что в ней, как правило, нет конфликтов (в отличие от шины), а также отсутствует центральный абонент (в отличие от звезды).
В кольце, в отличие от других топологий (звезда, шина), не используется конкурентный метод посылки данных, компьютер в сети получает данные от стоящего предыдущим в списке адресатов и перенаправляет их далее, если они адресованы не ему. Список адресатов генерируется компьютером, являющимся генератором маркера. Сетевой модуль генерирует маркерный сигнал (обычно порядка 2—10 байт во избежание затухания) и передает его следующей системе (иногда по возрастанию MAC-адреса). Следующая система, приняв сигнал, не анализирует его, а просто передает дальше. Это так называемый нулевой цикл.
Последующий алгоритм работы таков — пакет данных GRE, передаваемый отправителем адресату начинает следовать по пути, проложенному маркером. Пакет передаётся до тех пор, пока не доберётся до получателя.
Сравнение с другими топологиями.
Достоинства:
Простота установки;
Практически полное отсутствие дополнительного оборудования;
Возможность устойчивой работы без существенного падения скорости передачи данных при интенсивной загрузке сети, поскольку использование маркера исключает возможность возникновения коллизий.
Недостатки:
Выход из строя одной рабочей станции, и другие неполадки (обрыв кабеля), отражаются на работоспособности всей сети;
Сложность конфигурирования и настройки;
Сложность поиска неисправностей.
Необходимость иметь две сетевые платы, на каждой рабочей станции.

6) Снежинка (Иерархическая Звезда или древовидная топология) - тополо-
гия типа звезды, но используется несколько концентратов, иерархически соединенных между собой связями типа звезда. *Топология "снежинка" требует меньшей длины кабеля, чем "звезда", но больше элементов.*



Самый распространенный способ связей как в локальных сетях, так и в глобальных.

2. Практическая работа № 2 «Поиск аналогов устаревшего оборудования»

Инструкция для обучающихся

Внимательно прочитайте задание. Проведите обследование объектов на предмет состояния инженерно-технического укрепления.

Время выполнения – 90 минут.

Задание

1. Существует компьютерная кабельная локальная сеть для офиса. В состав оборудования данной сети входит сервер, 25 рабочих станций, маршрутизатор, 3 концентратора. Необходимо с помощью глобальной сети создать спецификацию сетевого оборудования последней модели.
2. В спецификации указать вид оборудования, основные характеристики, цену 1 единицы оборудования, стоимость оборудования и всей сети. Также в спецификацию вставить фотографию сетевого оборудования и координаты компьютерного магазина. Также к спецификации приложить скриншоты прайс-листов магазинов с датой обновления
3. Сохранить модернизированную спецификацию сети в свою рабочую папку, показать преподавателю и защитить работу.

Пример спецификации:

№	Наименование оборудования	Характеристики	Фотография	Стоимость 1 единицы	Количество	Общая тоимость

Эталон ответа:

Наименование	Ед. измерения	Количество	Цена	Итого
Раздел 1. Активное оборудование				
Сервер Dell PowerEdge T320	Шт.	1	41 104	41 104
Коммутатор D-Link DES-3810-52	Шт.	2	18 940	37 880
Сетевые платы Intel PWLA8490MT	Шт.	35	4 339	151 865
Модем ZyXEL Prestige 791R V2	Шт.	1	7 820	7 820
Итого по разделу				238 669
Раздел 2. Пассивное оборудование				

ИБП VoltGuard HR1102S	Шт.	1	30 779	30 779
Патч-панель AESP 48458-C6	Шт.	1	5 896	5 896
Патч-корды Lanmaster FTP, RJ-45 - RJ-45	Шт.	35	100	3 500
Кабеля Landmaster FTP 4-х парный cat.5E	М	10	2 000	20 000
розетки Landmaster 45 х 45 мм, 1 порт, со шторкой	Шт.	35	50	1 750
Коммутационный шкаф Cabeus SH-05C-22U60/60	Шт.	1	12 000	12 000
Короб 75х20	М	100	300	30 000
Заглушка торцевая	Шт.	40	30	120
Шуруп универсальный с потайной головкой 4,5х70	Кг	3	100	300
Дюбель пластмассовый	100 шт.	2	50	100
Итого по разделу				84 445
Наименование	Ед. измерения	Количество	Цена	Итого
Раздел 3. Программное обеспечение				
Windows Server Standard R2 2012	Шт.	1	27 808	27 808
Microsoft Windows Professional 8.1 Russian Upgrade Government	Шт.	35	4 893	171 255
Итого по разделу				199 063
Раздел 4. Строительные работы				
Сверление вертикальных отверстий в ж. б. конструкциях глубиной 200	100	0,03	2000	60

мм диаметром 100 мм				
Сверление отверстий сверление горизонтальных отверстий в ж. б. конструкциях глубиной 70 мм диаметром 45 мм	100	0,2	1000	200
Итого по разделу				260
Раздел 5. Монтажные работы				
Электрическая проверка коммутаторов	Шт.	1	1 000	1 000
Установка ОС, ПО	Раб. Станция	35	1 000	35 000
Контрольные испытания системы передачи данных	Объект	1	2 000	2 000
Монтаж пластового короба	100 м	1,5	1 000	1 500
Разделка кабеля	10 концов кабеля	344	50	17 200
Герметизация проходов кабеля	Проход	25	50	1 250
Итого по разделу				57 950
Итого по таблице				580 387
Страхование рисков				58 038,7
НДС 18%				104 469,66
Итого с учетом НДС				742 895,36

3. Практическая работа № 4 «Настройка беспроводного маршрутизатора и клиента»

Инструкция для обучающихся

Внимательно прочитайте задание. Проведите обследование объектов на предмет состояния инженерно-технического укрепления.

Время выполнения – 90 минут.

Задание

Настройки маршрутизатора Linksys

Имя сети (SSID)	Сеть CCNA
Пароль сети	cisconet
Пароль маршрутизатора	cisco123

Исходные данные/сценарий

В наши дни доступ к сети Интернет из любого места, будь то дом или офис — широко распространенное явление. Без беспроводной связи пользователи были бы ограничены возможностью подключения только при наличии проводного соединения. Пользователи по достоинству оценили гибкость и возможности, которые предоставляют беспроводные маршрутизаторы в рамках доступа к сети и Интернету.

В этой лабораторной работе вам предстоит настроить маршрутизатор Linksys Smart Wi-Fi, применить настройки безопасности WPA2 и активировать службы DHCP. Вы рассмотрите некоторые дополнительные функции, доступные на этих маршрутизаторах, например, USB-накопители, родительский контроль и ограничения по времени. Вам также предстоит настроить беспроводной клиент для компьютера.

Необходимые ресурсы:

- 1 маршрутизатор Linksys EA Series (EA4500 с версией микропрограммного обеспечения
  2.1.39.145204 или сопоставимой версией);
- 1 кабельный или DSL-модем (необязательно; требуется для работы интернет-службы и обычно предоставляется интернет-провайдером);
- 1 компьютер с беспроводным сетевым адаптером (ОС Windows 7, Vista или XP);
- кабели Ethernet, расположенные в соответствии с топологией.

Эталон ответа:

Шаг 1: Вставляем установочный компакт-диск Linksys EA-Series в компьютер.

Когда отобразится соответствующий запрос, выбераем **Set up your Linksys Router (Настройка маршрутизатора Linksys)**. Предложено ознакомиться с условиями лицензии на использование программного обеспечения и принять их. Применяем условия лицензии нажмите **Next > (Далее >)**.

Шаг 2: Подключаем кабели в сети в соответствии с топологией.

Следуйте инструкциям по подключению кабеля питания и кабельного модема или DSL-модема с помощью Ethernet-кабеля, которые отобразятся в следующем окне. Можно подключить компьютер к одному из четырех неиспользуемых Ethernet-портов на задней стенке маршрутизатора. После подключения всех необходимых элементов нажмите **Next > (Далее >)**.

Шаг 3: Настраиваем параметры маршрутизатора Linksys.

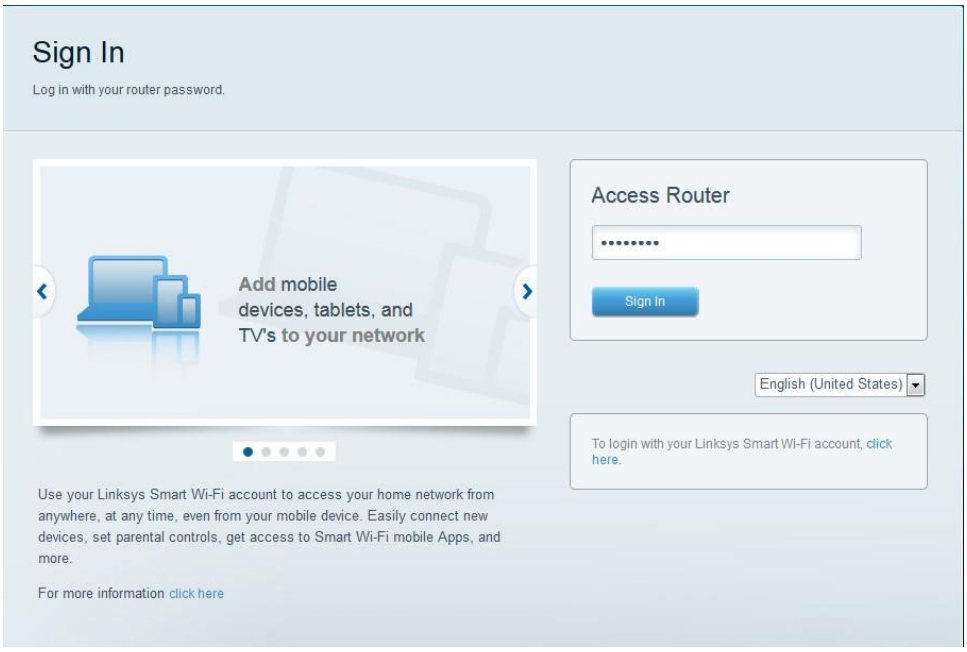
a. Дождитесь, когда отобразится окно **Linksys router settings (Настройки маршрутизатора Linksys)**. Для заполнения полей в этом окне используйте данные таблицы **Linksys router settings (Настройки маршрутизатора Linksys)**, приведённой в начале лабораторной работы. Нажмите **Next (Далее)**, чтобы отобразить экран со сводной информацией о настройках маршрутизатора.

Нажмите **Next (Далее)**.

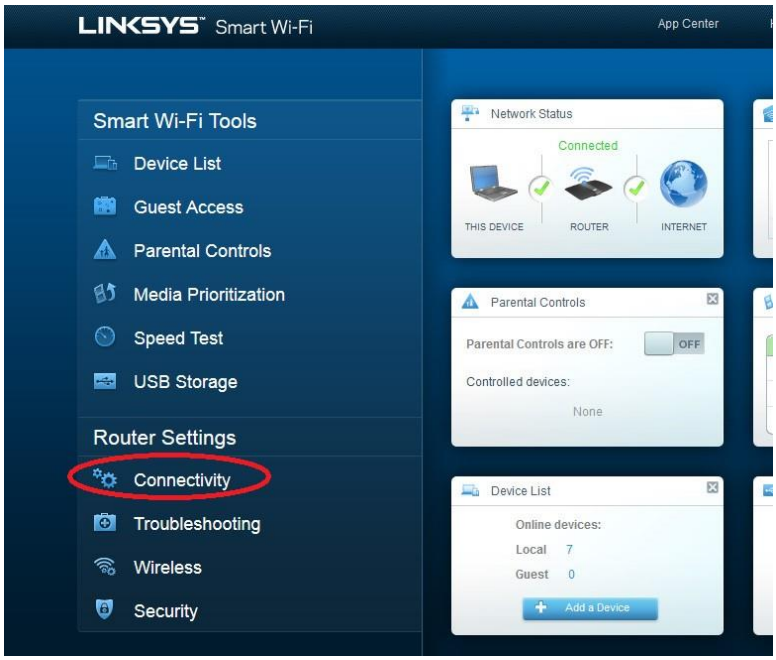
b. Отобразится окно **Create your Linksys Smart Wi-Fi account (Создание учетной записи Linksys Smart Wi-Fi)**. Учетная запись Linksys Smart Wi-Fi используется для ассоциации маршрутизатора к учетной записи, что позволяет удалённо управлять маршрутизатором с помощью браузера или мобильного устройства, на котором запущено приложение Smart Wi-Fi. В рамках этой лабораторной работы пропустите процесс настройки учетной записи. Щелкните поле **No, thanks (Нет, спасибо)** и нажмите **Continue (Продолжить)**.

Примечание. Чтобы настроить учетную запись, перейдите на веб-сайт www.linksyssmartwifi.com.

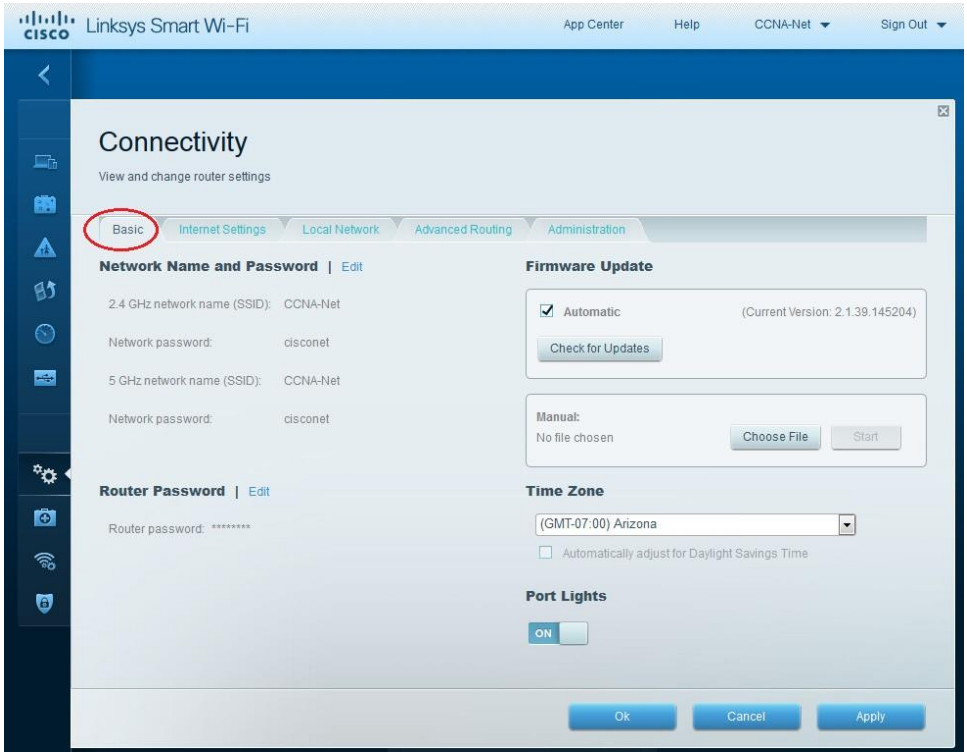
c. Отобразится окно **Sign in (Вход в систему)**. В поле **Access Router (Доступ к маршрутизатору)** введите **cisco123** и нажмите **Sign in (Войти)**.



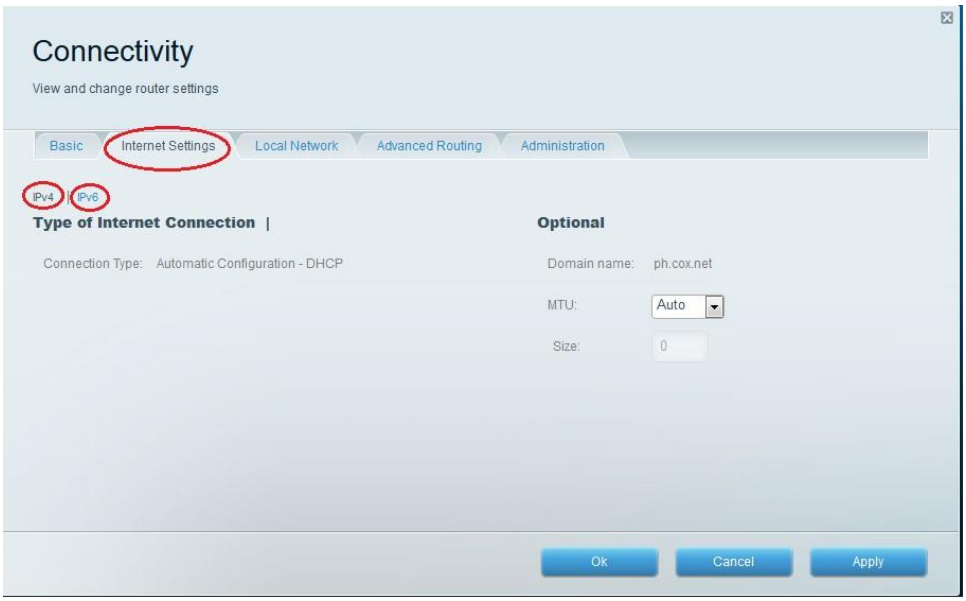
d. На домашней странице Linksys Smart Wi-Fi нажмите **Connectivity (Соединение)** чтобы просмотреть и изменить основные настройки маршрутизатора.



e. На вкладке **Basic (Основные настройки)** можно изменить имя и пароль сети, изменить пароль маршрутизатора, выполнить обновление микропрограммного обеспечения и задать часовой пояс для маршрутизатора. Пароль маршрутизатора и данные о сети настроены в шаге 3a. В раскрывающемся списке выберите соответствующий часовой пояс для маршрутизатора и нажмите **Apply (Применить)**.



f. На вкладке **Internet Settings (Настройки Интернета)** отображены сведения об интернетподключении. В этом примере маршрутизатор автоматически настраивает подключение для DHCP. На этом экране можно отобразить сведения как об IPv4, так и об IPv6.



g. На вкладке **Local Network (Локальная сеть)** доступны параметры настройки локального DHCPсервера. В настройках локальной сети по умолчанию задана сеть 192.168.1.0/24 и локальный IPадрес маршрутизатора по умолчанию 192.168.1.1. Эти настройки можно изменить, нажав **Edit (Изменить)** рядом с разделом **Router Details (Сведения о маршрутизаторе)**. На этом экране можно изменить настройки DHCP-сервера. Можно задать начальный адрес DHCP, максимальное число пользователей DHCP, срок аренды клиента и статические DNS-серверы. Нажмите **Apply (Применить)**, чтобы принять все изменения, внесённые на этом экране.

Устный зачет по теме 2

Инструкция для обучающихся

Зачет сдается в рамках учебного занятия. Каждый студент отвечает в устной форме на предложенные преподавателем 7 мини-вопросов.

Выполнение задания: одному студенту на ответ выделяется 3 мин., группа сдает зачет за одно учебное занятие.

Перечень вопросов:

1. При разработке схемы именования для сети, какие два элемента данных являются наиболее важными при определении имени компьютера?
2. Какие три элемента данных включены в физическую карту сети?
3. В какой области сети трафик, поступающий от других хостов, может привести к остановке передачи данных передающим хостом, после чего передающий хост ждет в течение произвольного количества времени, прежде чем повторно переслать сообщение?
4. Назовите три характеристики кабеля на основе неэкранированной витой пары
5. Сколько сетей класса C зарезервированы для пространства частных адресов?
6. Какие функции выполняет NAT в ISR?
7. Что происходит, если часть сообщения с использованием TCP не доставляется на конечный хост?

Эталоны ответов: приведены в учебном пособии по МДК.01.02 «Организация, принципы построения и функционирования компьютерных сетей».

4. Практическая работа № 7 «Проектирование подсистемы рабочего места»

Инструкция для обучающихся

Внимательно прочитайте задание. Проведите обследование объектов на предмет состояния инженерно-технического укрепления.

Время выполнения – 90 минут.

Задание

1. Дан план офиса. Необходимо спроектировать подсистему рабочего места. Исходными данными для этого является практическая работа №6.
2. Необходимо на плане офиса указать рабочее место (компьютер, ноутбук), 1 штепсельную и 1 сетевую розетки. На всех планах указать имя компьютера (план с указанием рабочих мест, структурно-функциональная схема).
3. С помощью глобальной компьютерной сети подобрать сетевое оборудование для подсистемы рабочего места, указать его характеристики. Составить список необходимого ПО, указать системные требования для каждого вида ПО, стоимость лицензии.
4. Составить спецификацию для рабочего места (сетевое оборудование и программное обеспечение).

Таблица 1 - Конфигурация рабочей станции (пример)

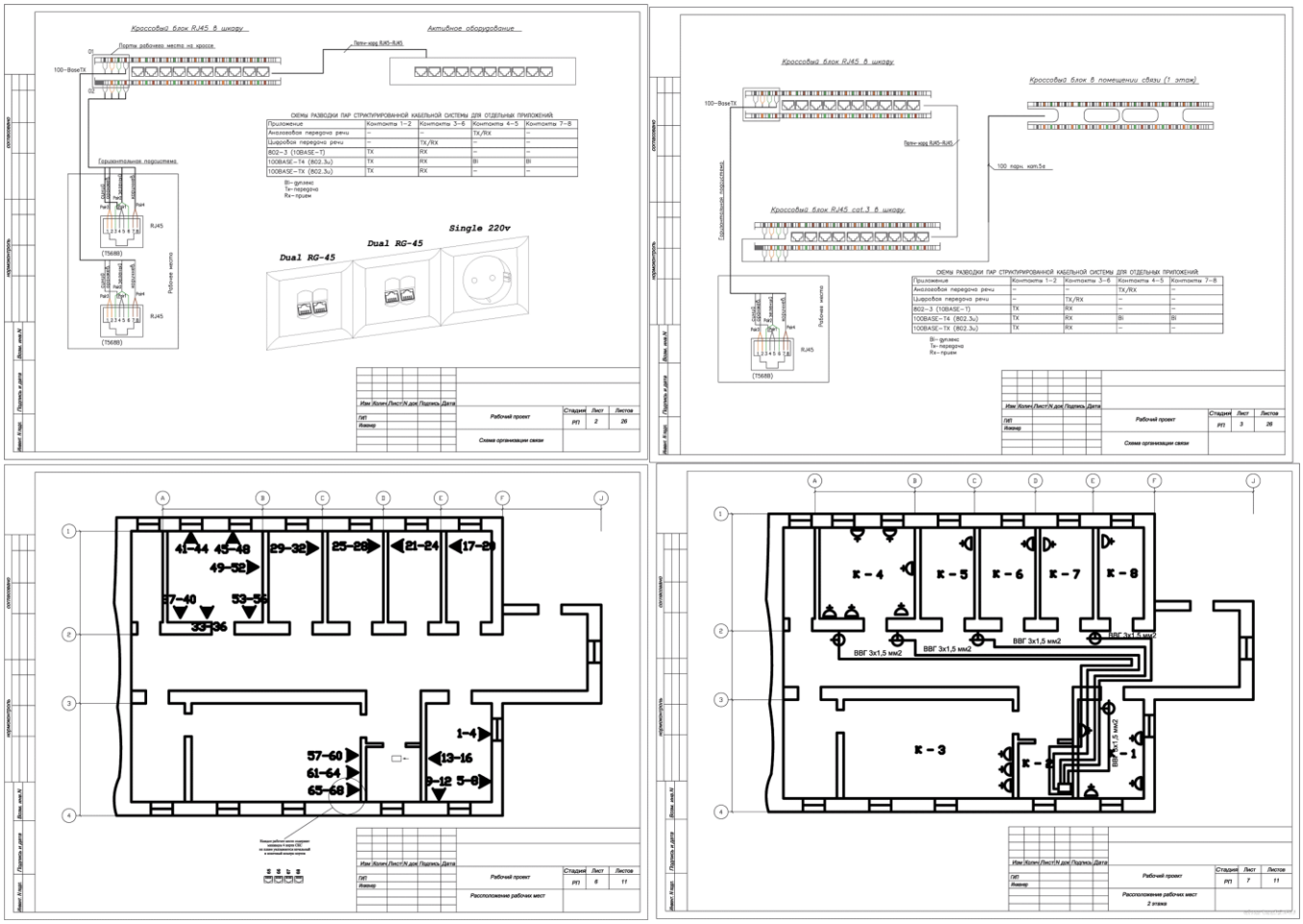
Наименование	Тип	Цена,руб.
Материнская плата	AsusTek P3V133	2759.00
Процессор	Intel Pentium II – 400 512k MMX	2790.00
Память	64Mb (DIMM)	868.00
Видеокарта	SVGA 8Mb	961.00
HDD	10,2Gb Fujitsu MPF3102AT	3813.00
FDD	3.5”	341.00
CD-ROM	Asus 50-X	1441.50
Клавиатура	Turbo RUS, Win’95	127.10
Мышь	Genius Easy COM / PS/2	93.00
Монитор	Scott 570 15”	4557.00
Сетевая карта	NE-2000 Acorp UTP (10Base-T; 100Base-TX)	272.80
Итого:		18023.40

Таблица 2 – Спецификация программного обеспечения

Наименование	Описание	Стоимость лицензии	Кол-во	Цена,руб.

Сохранить схемы и спецификации в свою рабочую папку.

Эталон ответа:



Устный зачет по теме 3

Инструкция для обучающихся

Зачет сдается в рамках учебного занятия. Каждый студент отвечает в устной форме на предложенные преподавателем 7 мини-вопросов.

Выполнение задания: одному студенту на ответ выделяется 3 мин., группа сдает зачет за одно учебное занятие.

Перечень вопросов:

1. Сколько адресов может иметь хост?
2. Может ли у хоста быть прописано несколько шлюзов и почему?
3. Может ли у хоста быть прописано несколько шлюзов по умолчанию и почему?
4. Чем отличаются таблицы у разных классов сетевых устройств и почему?
5. Почему начальный адрес подсети должен быть кратен ее размеру?
6. Чем Вы руководствовались при выборе шлюзов по умолчанию?
7. Может ли физический сегмент сети содержать несколько сетевых подсетей?

Эталоны ответов: приведены в учебном пособии по МДК.01.02 «Организация, принципы построения и функционирования компьютерных сетей».

5. Практическая работа № 18 «Защита информации в сетях»

Инструкция для обучающихся

Внимательно прочитайте задание. Проведите обследование объектов на предмет состояния инженерно-технического укрепления.

Время выполнения – 90 минут.

Задание

Задание №1. Определите общий ресурс компьютера. Для этого:

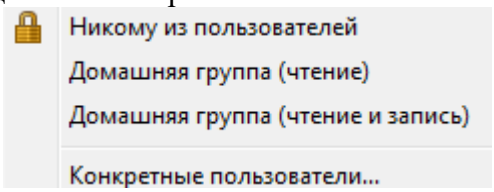
1. В операционной системе Windows найти на рабочем столе значок Сеть.
2. Открыть папку, где будут видны все компьютеры, которые подключены в одну сеть.

В данном окне появятся все компьютеры, которые подключены к сети.

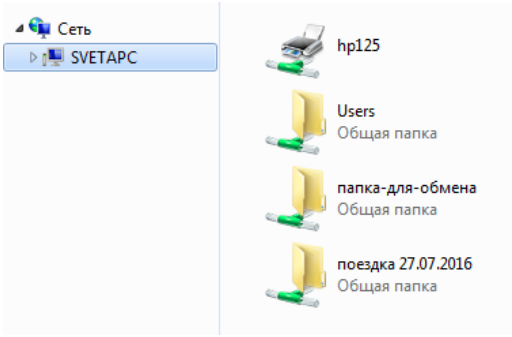
1. Открыть один из них. Посмотреть ресурсы компьютера, которыми можно воспользоваться. Такие ресурсы называются общими.
   Вставьте скриншот выполненной работы

Задание № 2. Предоставьте доступ для пользователей локальной сети к папке на своем компьютере, подключенном к локальной сети. Для этого:

1. В операционной системе Windows открыть окно папки Компьютер и на диске D: создать свою папку. Назвать ее номером своей группы.
2. Щелкнуть правой кнопкой мыши по значку папки и в контекстном меню папки выберите команду Общий доступ.
3. Выбрать нужное подменю: Конкретные пользователи



В списке Сеть внизу появится новая папка: поездка 27.07.2016



1. Если все правильно сделано, то на диске (у вашей папки) появится значок, который показывает, что папка является общей.
   Вставьте скриншот выполненной работы

Задание №3. Максимальная скорость передачи данных в локальной сети 100 Мбит/с. Сколько страниц текста можно передать за 1 сек, если 1 страница текста содержит 50 строк и на каждой строке - 70 символов?

Решение:

50*70=3500 символов на страницу.

Так как не указано, сколько символов в алфавите, возьмем 1 байт на символ. Итого 3500 байт или (умножить на 8) 28000 бит.

Теперь делим 100,000,000 на 28,000. Получаем 3571.43 страниц.

Решить самостоятельно по следующим данным:

1 страница текста содержит 70 строк и на каждой строке - 50 символов?

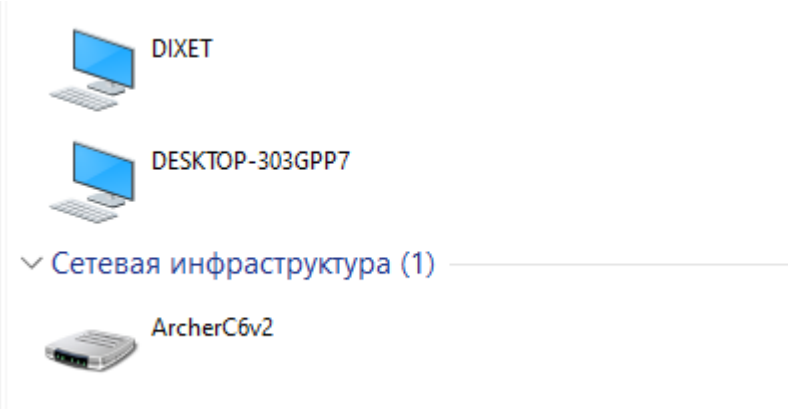
Вставьте расчет выполненной работы

Задание №4. Ответьте на вопросы:

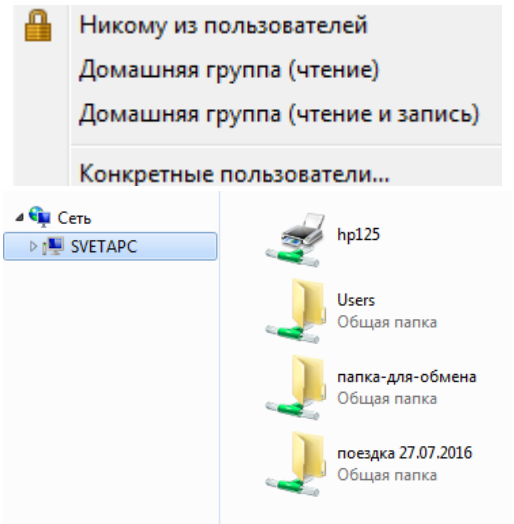
1.Указать основное назначение компьютерной сети.	
2.Указать основную характеристику каналов связи.	
3.Указать объект, который является абонентом сети.	

Эталон ответа:

Задание №1



Задание №2



Задание №3

50*70=3500 символов на страницу.
Так как не указано, сколько символов в алфавите, возьмем 1 байт на символ. Итого 3500 байт или (умножить на 8) 28000 бит.
Теперь делим 100,000,000 на 28,000. Получаем 3571.43 страниц.
Задание №4

1.Указать основное назначение компьютерной сети.	Коммутация сетевых устройств
2.Указать основную характеристику каналов связи.	Пропускная способность
3.Указать объект, который является абонентом сети.	Персональный компьютер

3.1.3. Оценка освоения теоретического курса профессионального модуля по МДК.01.03

Дидактические единицы	Проверяемые ОК, ПК, У, З	Формы контроля (наименование контрольной точки)	
		Текущая аттестация	Промежуточная аттестация
Тема 3.1. Безопасность компьютерных сетей	ОК 1-9 ПК 1.1 ПК 1.7	Устный зачет по теме 3.1	Теоретические вопросы на экзамене
		Практическая работа **№8** Настройка безопасного доступа к маршрутизатору	
		Практическая работа **№ 17** Обеспечение информационной безопасности	

Устный зачет по теме 2.1.1. – 2.1.10

Инструкция для обучающихся

Зачет сдается в рамках учебного занятия. Каждый студент отвечает в устной форме на предложенные преподавателем 5 случайных вопроса.

Выполнение задания: одному студенту на ответ выделяется 3 мин., группа сдает зачет за одно учебное занятие.

Перечень вопросов:

1. Фундаментальные принципы безопасной сети
2. Современные угрозы сетевой безопасности.
3. Вирусы, черви и троянские кони.
4. Методы атак.
5. Безопасность Сетевых устройств OSI
6. Безопасный доступ к устройствам.
7. Назначение административных ролей.
8. Мониторинг и управление устройствами.
9. Использование функция автоматизированной настройки безопасности.
10. Авторизация, аутентификация и учет доступа (AAA)

Эталоны ответов: приведены в учебном пособии по МДК.01.03 «Безопасность компьютерных сетей»

Практическая работа № 8 Эксплуатация объектов сетевой инфраструктуры

Инструкция для обучающихся

Внимательно прочитайте задание. Проведите установку и настройку контроллеров.

Время выполнения – 90 минут.

Задание

Задание:

Топология

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсе-ти	Шлюз по умолчанию
R1	**G0/1**	**192.168.1.1**	**255.255.255.0**	**Недоступно**
S1	**VLAN 1**	**192.168.1.11**	**255.255.255.0**	**192.168.1.1**
ПК-А	**Сетевой адаптер**	**192.168.1.3**	**255.255.255.0**	**192.168.1.1**

Задачи

Часть 1. Настройка основных параметров устройства
Часть 2. Настройка маршрутизатора для доступа по протоколу SSH
Часть 3. Проверка сеанса связи по протоколу Telnet с помощью программы Wireshark
Часть 4. Проверка сеанса связи по протоколу SSH с помощью программы Wireshark
Часть 5. Настройка коммутатора для доступа по протоколу SSH
Часть 6. Настройка протокола SSH в интерфейсе командной строки коммутатора

Исходные данные/сценарий

Раньше для удалённой настройки сетевых устройств в основном применялся протокол Telnet. При этом протоколы типа Telnet не включают проверку подлинности и шифрование информации, передаваемой между клиентом и сервером, что позволяет сетевым средствам слежения перехватывать пароли и данные конфигурации.

Secure Shell(SSH)— это сетевой протокол, устанавливающий безопасное подключение эмулятора терминала к маршрутизатору или иному сетевому устройству. Протокол SSH шифрует все сведения, которые поступают по сетевому каналу, и предусматривает аутентификацию удалённого компьютера. Протокол SSH всё больше заменяет Telnet — именно его выбирают сетевые специалисты в качестве средства удалённого входа в систему. Чаще всего протокол SSH применяется для входа на удалённое устройство и выполнения команд, но может также передавать файлы по связанным протоколам SFTP или SCP.

Чтобы протокол SSH работал, на взаимодействующих сетевых устройствах должна быть настроена его поддержка. В ходе лабораторной работы вы активируете на маршрутизаторе SSH-сервер и подключитесь к маршрутизатору, используя ПК с клиентом SSH. В локальной сети подключение обычно устанавливается с помощью Ethernet и IP-адреса. Кроме того, в ходе лабораторной работы вы настроите маршрутизатор для приёма подключений по протоколу SSH и воспользуетесь программой Wireshark для перехвата и просмотра сеансов Telnet и SSH. Это покажет, какую важную роль играет шифрование данных, осуществляемое протоколом SSH. И, наконец, вам придётся самостоятельно настроить коммутатор для подключения по протоколу SSH.

Примечание. Маршрутизаторы, используемые на практических занятиях CCNA: маршрутизаторы с интеграцией сервисов серии Cisco 1941 (ISR) установленной версии Cisco IOS 15.2(4) M3 (образ universalk9). Используемые коммутаторы: семейство коммутаторов

Cisco Catalyst 2960 версии CISCO IOS 15.0(2) (образ lanbasek9). Можно использовать другие маршрутизаторы, коммутаторы и версии CISCO IOS. В зависимости от модели и версии Cisco IOS выполняемые доступные команды и выводы могут отличаться от данных, полученных в ходе лабораторных работ. Точные идентификаторы интерфейса см. в таблице сводной информации об интерфейсах маршрутизаторов в конце данной лабораторной работы.

Примечание. Убедитесь, что информация, имеющаяся на маршрутизаторе и коммутаторе, удалена и они не содержат файлов загрузочной конфигурации. Если вы не уверены, что сможете это сделать, обратитесь к инструктору.

Необходимые ресурсы

- 1 маршрутизатор (Cisco 1941 с универсальным образом M3 версии CISCO IOS 15.2(4) или аналогичным)
- 1 коммутатор (серия Cisco 2960, с программным обеспечением Cisco IOS версии 15.0(2), образ lanbasek9 или аналогичный)
- Один ПК (Windows 7, Vista или XP с эмулятором терминала, например Tera Term, и установленной программой Wireshark)
- Консольные кабели для настройки устройств CISCO IOS через консольные порты
- Кабели Ethernet в соответствии с топологией

Часть 1: Основные настройки устройства

В части 1 потребуется настройка топологии сети и основных параметров, таких как IP-адреса интерфейсов, доступ к устройствам и пароли на маршрутизаторе.

Шаг 1: Создайте сеть в соответствии с изображенной на схеме топологией.

Шаг 2: Выполните инициализацию и перезагрузку маршрутизатора и коммутатора.

Шаг 3: Настройте маршрутизатор.

a. Подключите консоль к маршрутизатору и активируйте привилегированный режим.
b. Войдите в режим конфигурации.
c. Отключите поиск в DNS, чтобы предотвратить попытки маршрутизатора преобразовывать неверно введённые команды таким образом, как будто они являются именами узлов.
d. Назначьте **class** в качестве пароля привилегированного режима.
e. Назначьте **cisco** в качестве пароля консоли и включите вход по паролю.
f. Назначьте **cisco** в качестве пароля виртуального терминала и включите вход по паролю. g. Зашифруйте пароли.
h. Создайте баннер, который предупреждает о запрете несанкционированного доступа.
i. Настройте и активируйте интерфейс маршрутизатора G0/1 с помощью сведений, содержащихся в таблице адресации.
j. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

Шаг 4: Настройте ПК-A.

a. Настройте на ПК-A IP-адрес и маску подсети.
b. Настройте на ПК-A шлюз по умолчанию.

Шаг 5: Проверьте подключение к сети.

Отправьте эхо-запрос с помощью команды ping с ПК-A на маршрутизатор R1. Если эхо-запрос с помощью команды ping не проходит, найдите и устраните неполадки подключения.

Часть 2: Настройка маршрутизатора для доступа по протоколу SSH

Подключение к сетевым устройствам по протоколу Telnet сопряжено с риском для безопасности, поскольку вся информация передаётся в виде открытого текста. Протокол SSH шифрует данные сессии и требует аутентификации устройств, поэтому для удалённых подключений рекомендуется использовать именно его. В части 2 вам нужно настроить маршрутизатор для приёма соединений по протоколу SSH по линиям VTY.

Шаг 1: Настройте аутентификацию устройств.

При генерации ключа шифрования используются имя устройства и домен. Это значит, что эти имена необходимо указать перед вводом команды **crypto key**.

a. Укажите имя устройства.

Router(config)# **hostname R1**

b. Укажите домен для устройства.

R1(config)# **ip domain-name ccna-lab.com**

Шаг 2: Создайте ключ шифрования с указанием его длины.

R1(config)# **crypto key generate rsa modulus 1024**

The name for the keys will be: R1.ccna-lab.com

% The key modulus size is 1024 bits % Generating 1024 bit RSA keys, keys will be non-exportable...

[OK] (elapsed time was 1 seconds)

R1(config)#

*Jan 28 21:09:29.867: %SSH-5-ENABLED: SSH 1.99 has been enabled

Шаг 3: Создайте имя пользователя в локальной базе учётных записей.

R1(config)# **username admin privilege 15 secret adminpass**

R1(config)#

*Feb 6 23:24:43.971: End->Password:QHjxdsVkjtoP7VxKIcPsLdTiMIvyLkyjT1HbmYxZigc

R1(config)#

Примечание. Пятнадцатый уровень привилегий предоставляет пользователю права администратора.

Шаг 4: Активируйте протокол SSH на линиях VTY.

a. Активируйте протоколы Telnet и SSH на входящих линиях VTY с помощью команды **transport input**.

R1(config)# **line vty 0 4**

R1(config-line)# **transport input telnet ssh**

b. Измените способ входа в систему — выберите проверку пользователей по локальной базе учётных записей.

R1(config-line)# **login local**

R1(config-line)# **end** R1#

Шаг 5: Сохраните текущую конфигурацию в файл загрузочной конфигурации.

R1# **copy running-config startup-config**

Destination filename [startup-config]?

Building configuration...

[OK]

R1#

Часть 3: Проверка сеанса связи по протоколу Telnet с помощью программы Wireshark

В части 3 вы воспользуетесь программой Wireshark для перехвата и просмотра данных, передаваемых во время сеанса связи маршрутизатора по протоколу Telnet. С помощью программы Tera Term вы подключитесь к маршрутизатору R1 по протоколу Telnet, войдёте в систему и запустите на маршрутизаторе команду show run.

Примечание. Если на вашем компьютере нет программного обеспечения клиента Telnet/SSH, его необходимо установить. Чаще всего для работы с протоколами Telnet и SSH используются программы Tera Term (http://download.cnet.com/Tera-Term/3000-20432_4-75766675.html) и PuTTy (www.putty.org).

Примечание. По умолчанию доступ к Telnet из командной строки вWindows 7 отключён. Чтобы

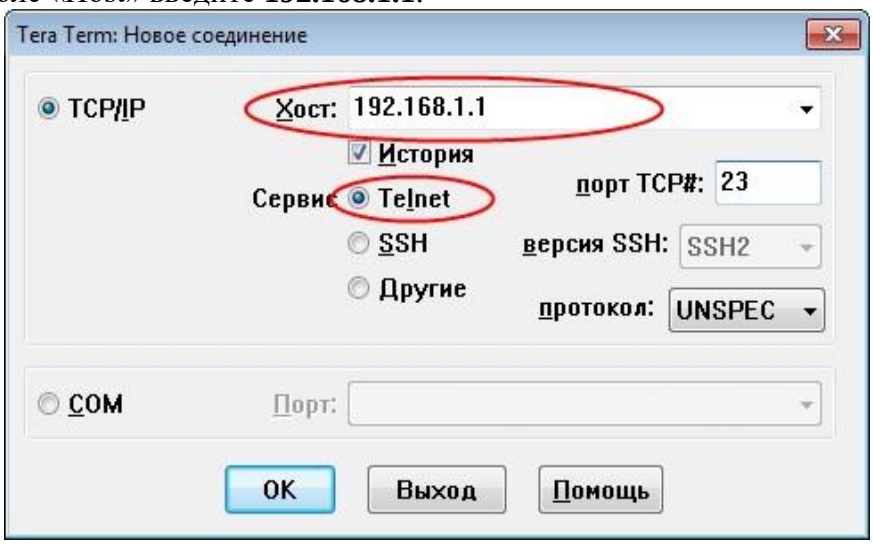
активировать подключение по протоколу Telnet из окна командной строки, нажмите кнопку
Пуск >Панель управления>Программы>Программы и компоненты>Включение или отключение компонентов Windows. Установите флажок рядом с компонентом **Клиент Telnet** и нажмите кнопку **OK**.

Шаг 1: Откройте Wireshark и начните сбор данных в интерфейсе локальной сети.

Примечание. Если перехват данных в интерфейсе локальной сети запустить не удаётся, попробуйте открыть программу Wireshark с помощью параметра **Запуск от имени администратора**.

Шаг 2: Начните сеанс подключения к маршрутизатору по протоколу Telnet.

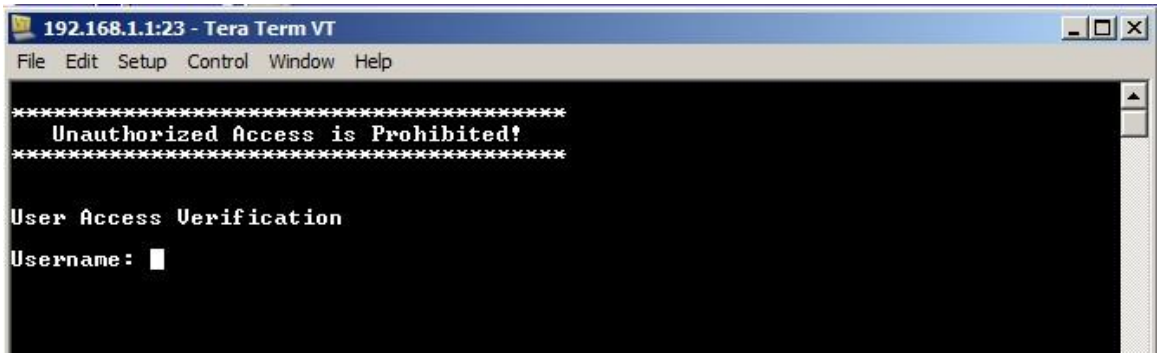
a. Запустите программу Tera Term, установите переключатель сервиса **Telnet**, а в поле «Host» введите **192.168.1.1**.



Какой порт TCP используется для сеансов Telnet по умолчанию?

_____

a. В окне командной строки после приглашения Username: (Имя пользователя) введите **admin**, а после Password: (Пароль) — **adminpass**. Эти запросы появляются потому, что командой **login local** вы настроили линии VTY на использование локальной базы учётных записей.



c. Введите команду **show run**.

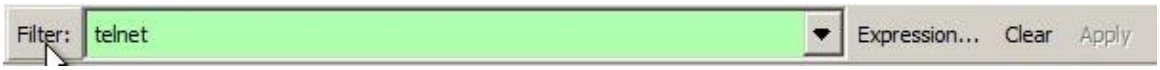
R1# **show run**

d. Введите команду **exit**, чтобы завершить сеанс работы с протоколом Telnet и выйти из программы Tera Term.

R1# **exit**

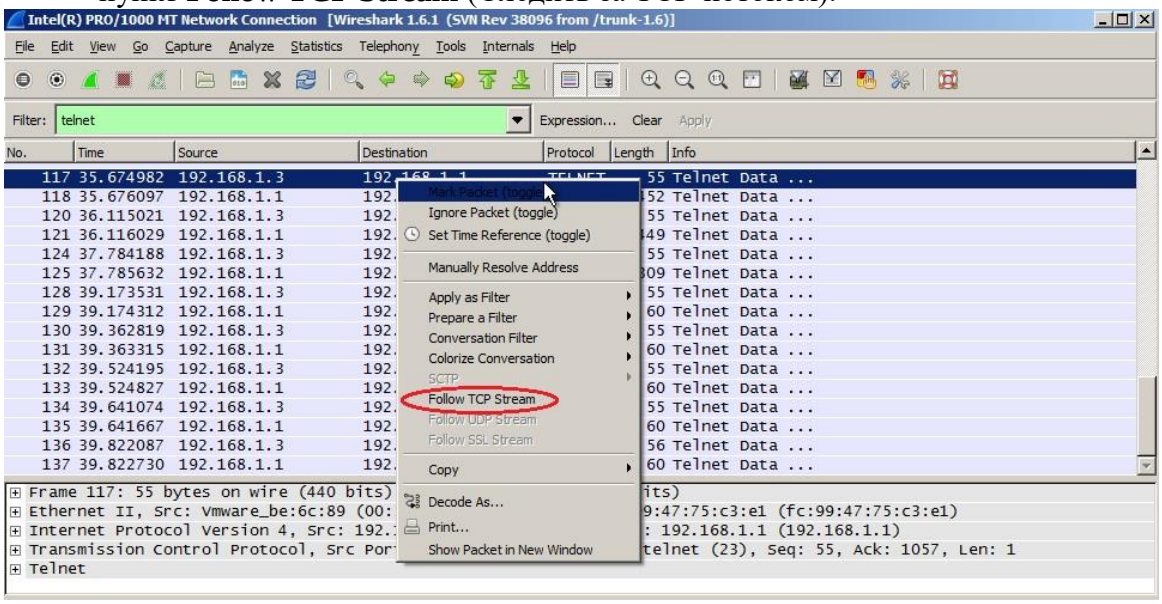
Шаг 3: Остановите сбор данных программой Wireshark.

Шаг 4: Примените один из фильтров Telnet для данных, собираемых программой Wireshark.



Шаг 5: Используйте функцию TCP в Wireshark для просмотра сеанса Telnet.

a. Нажмите правой кнопкой мыши на одну из строк **Telnet** в разделе **Packet list** (Список пакетов) программы Wireshark и выберите в раскрывающемся списке пункт **Follow TCP Stream** (Следить за TCP-потоком).



b. В окне Follow TCP Stream (Следить за TCP-потоком) отображаются данные о текущем сеансе подключения к маршрутизатору по протоколу Telnet. Весь сеанс связи (включая пароль) отображается открытым текстом. Обратите внимание на то, что введённые имя пользователя и команда **show run** отображаются с повторяющимися символами. Это связано с настройкой отображения в Telnet, которая позволяет выводить на экран символы, набираемые на клавиатуре.

Эталон ответа

Задание:

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1	192.168.1.1	255.255.255.0	Недоступно

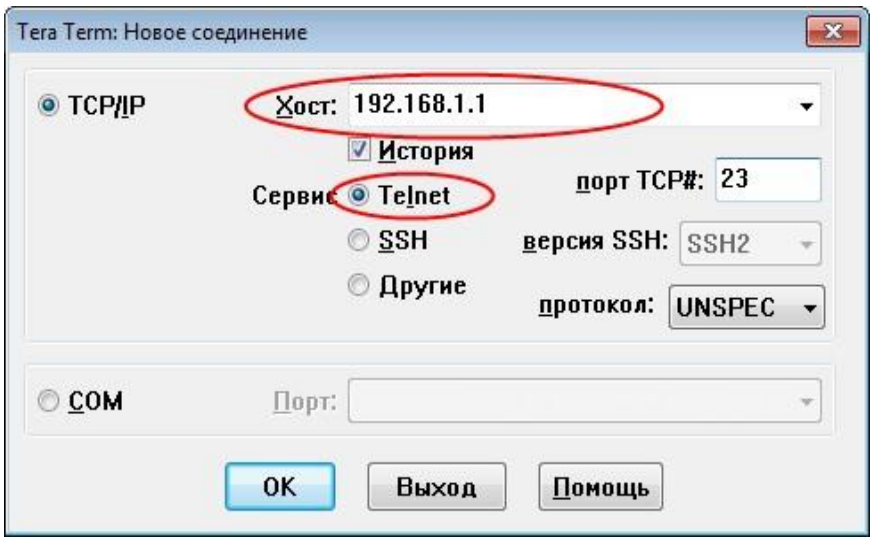
S1	**VLAN 1**	**192.168.1.11**	**255.255.255.0**	**192.168.1.1**
ПК-А	**Сетевой адаптер**	**192.168.1.3**	**255.255.255.0**	**192.168.1.1**

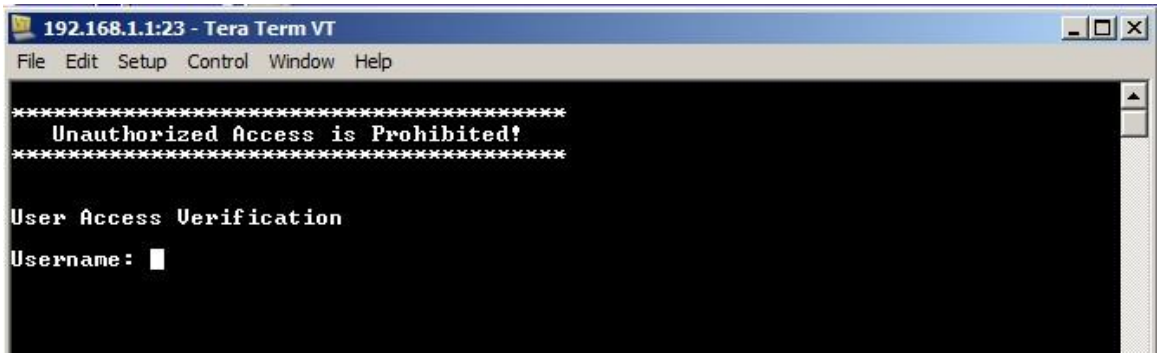
R1(config)# **username admin privilege 15 secret adminpass**

R1(config)#

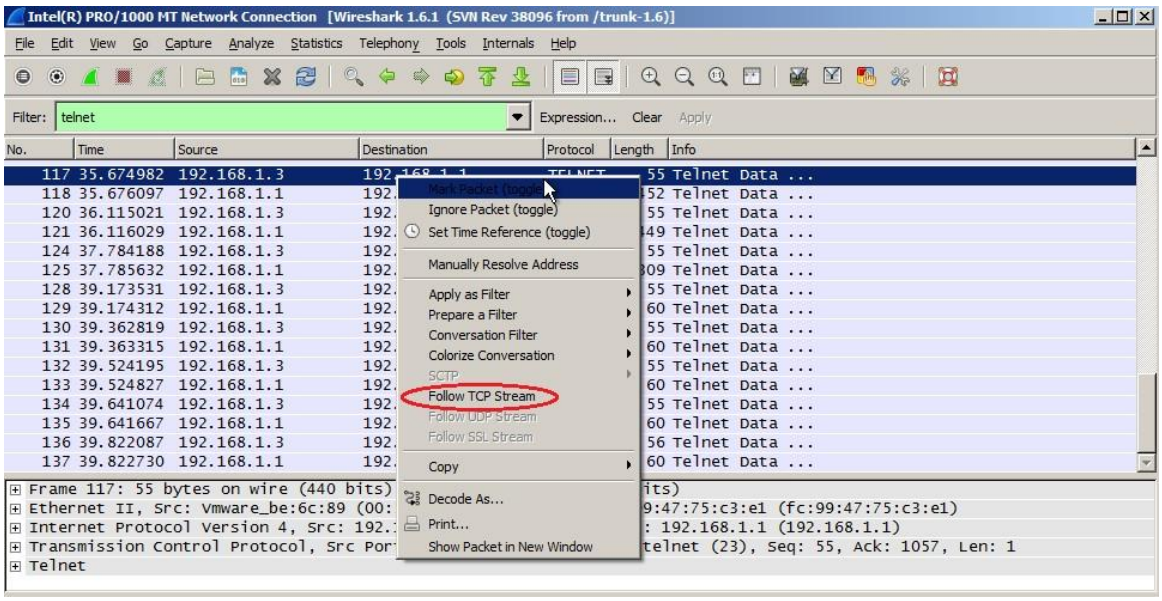
*Feb 6 23:24:43.971: End->Password:QHjxdsVkjtoP7VxKIcPsLdTiMIvyLkyjT1HbmYxZigc

R1(config)#





с. Введите команду **show run**.



Практическая работа № 17 Настройка безопасного доступа к маршрутизатору

Инструкция для обучающихся

Внимательно прочитайте задание. Проведите установку и настройку контроллеров.

Время выполнения – 90 минут.

Задание

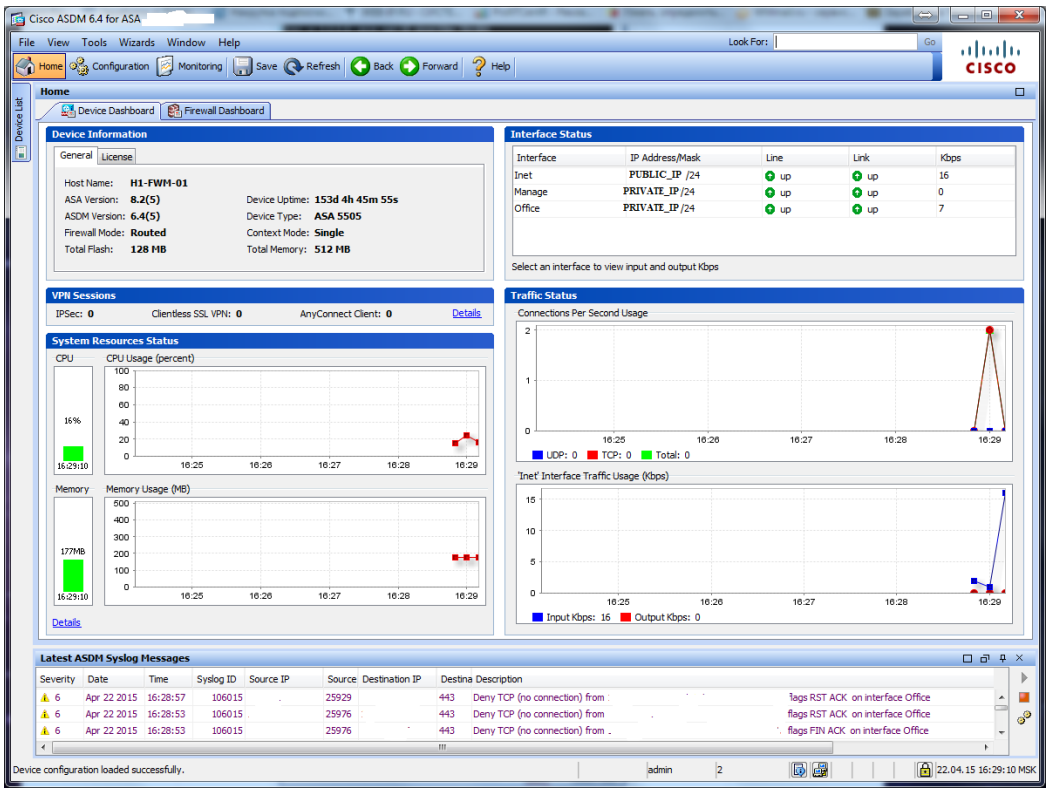
Задание:

Удаленный клиент при подключении через браузер непосредственно к cisco, скачивает специальное клиентское приложение Cisco AnyConnect Client на свой компьютер.

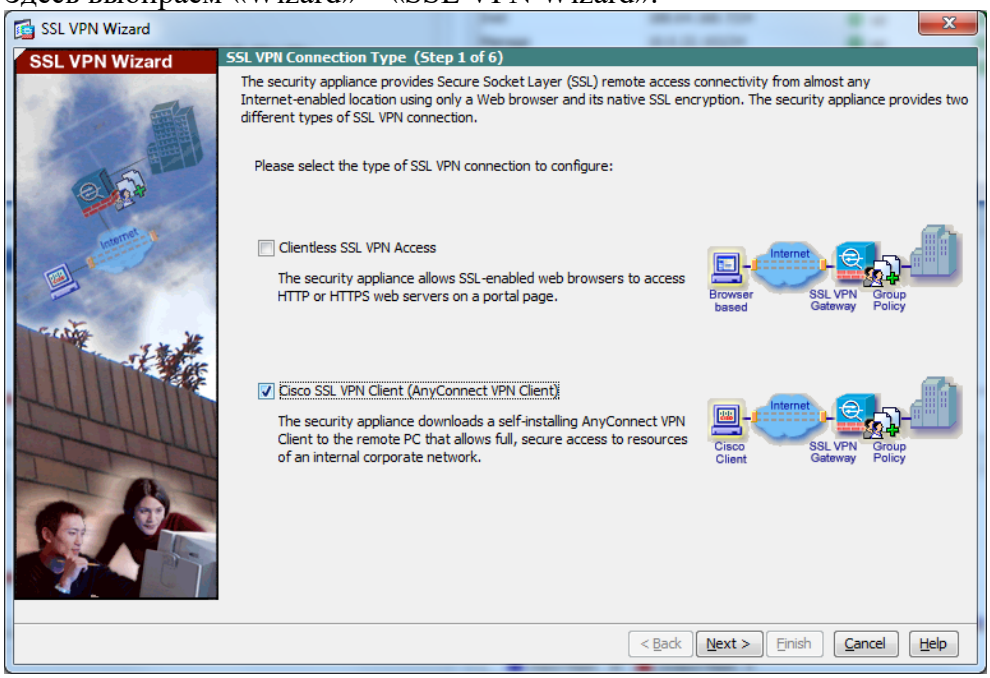
Будем рассматривать настройку SSL VPN параллельно 2-мя способами через графический интерфейс Cisco ASDM и через консоль CLI.
Используемое оборудование Cisco ASA-5505 (Security Appliance Software Version 9.1(6)6)

Настройка с помощью ASDM

Запускаем Cisco ASDM, откроется основной экран

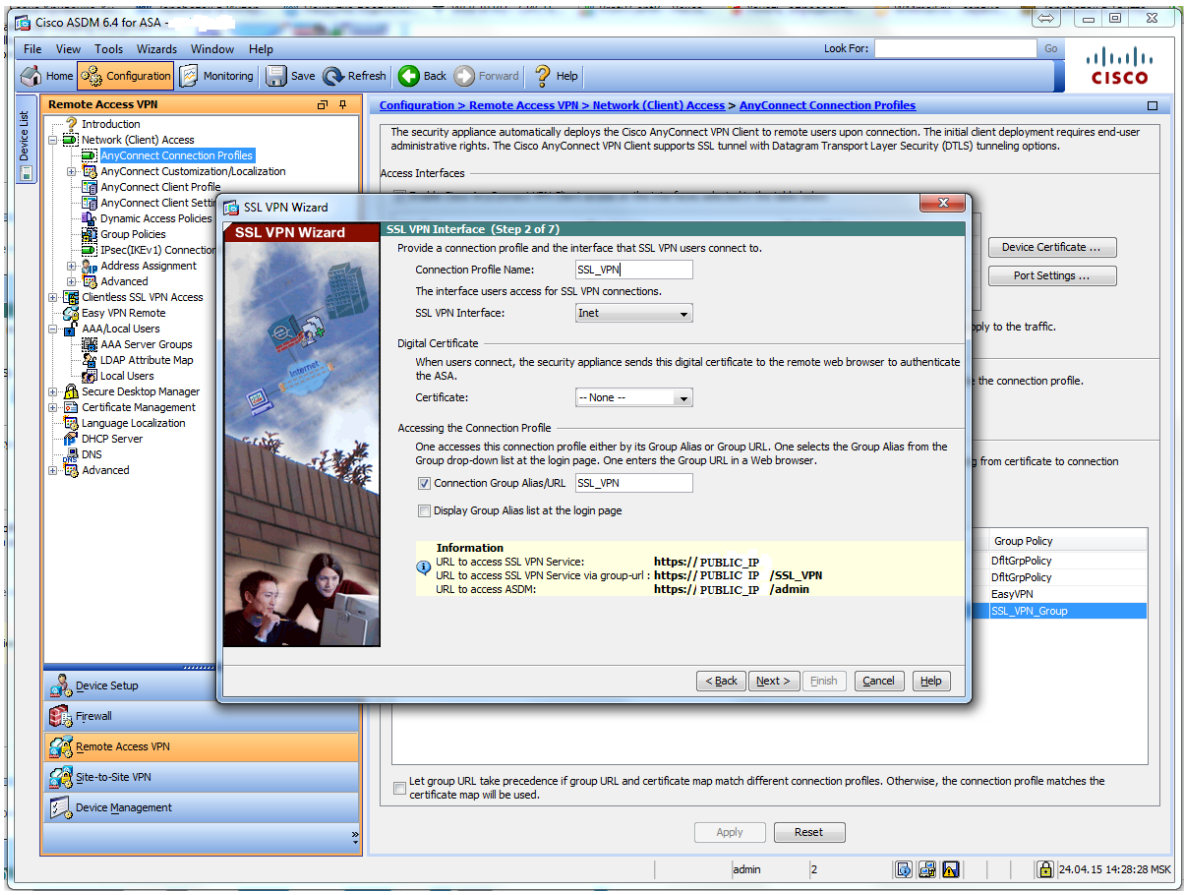


Здесь выбираем «Wizard»---«SSL VPN Wizard».



В открывшемся окне выбираем пункт «Cisco SSL VPN Client (AnyConnect VPN Client)» и

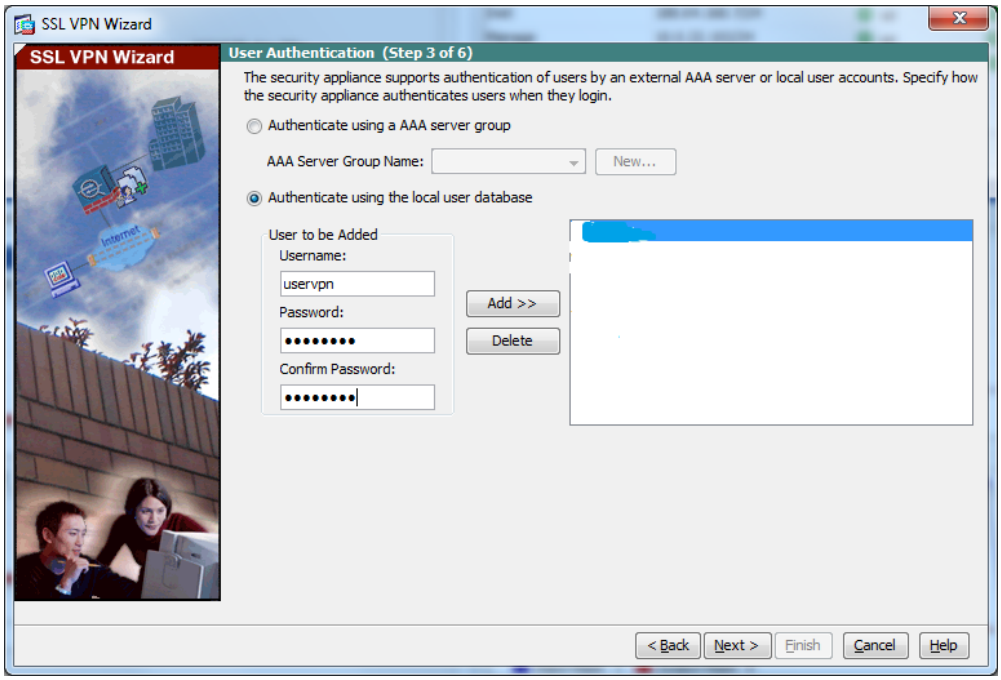
нажимаем «Next»:



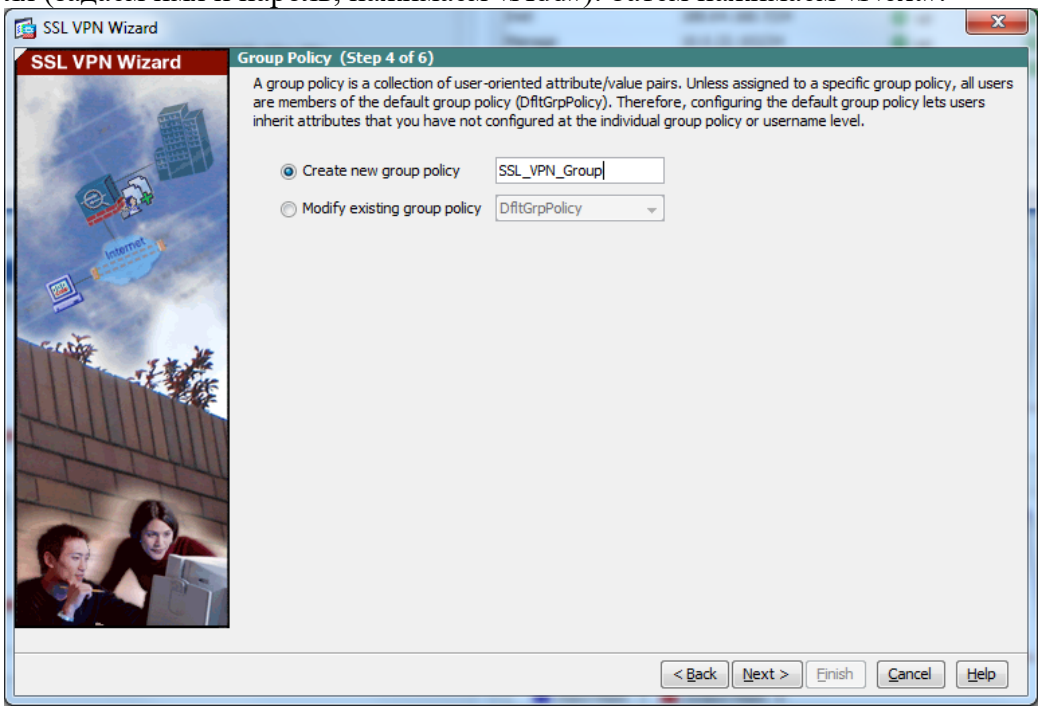
Здесь вводим имя нашего профайла, проверяем, что стоит имя нашего внешнего интерфейса (в данном случае Inet).

Если на cisco настроено несколько vpn подключений, то также указываем имя алиаса. Запоминаем доступы к SSL VPN Service и ASDM.

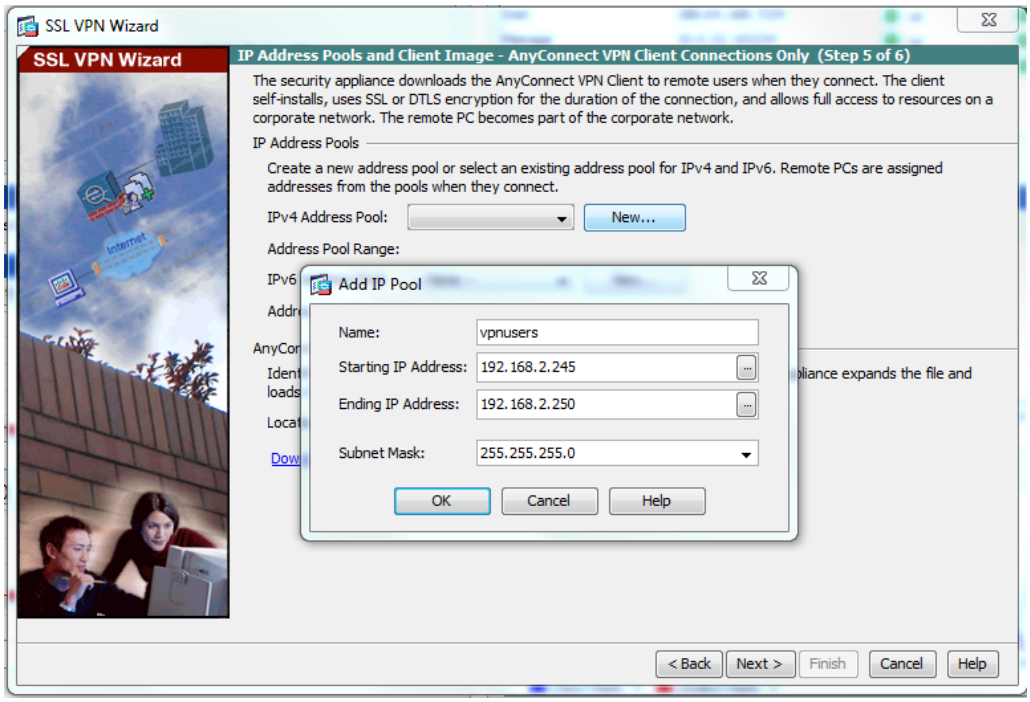
Затем нажимаем «Next»:



Ставим аутентификацию с использованием локальной базы и создаем нового пользователя (задаем имя и пароль, нажимаем «Add»). Затем нажимаем «Next»:

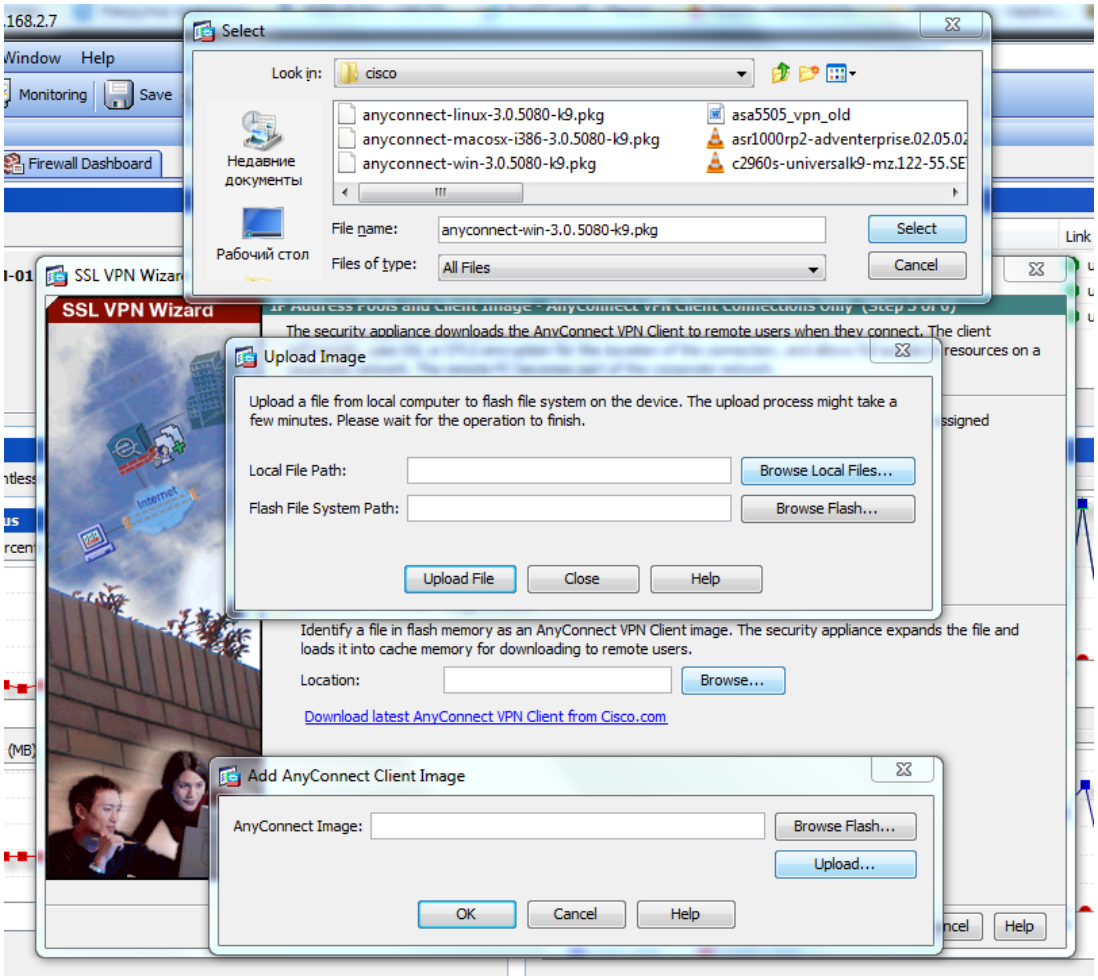


Здесь указываем имя отдельной групповой политики для SSL клиентов и нажимаем «Next»:

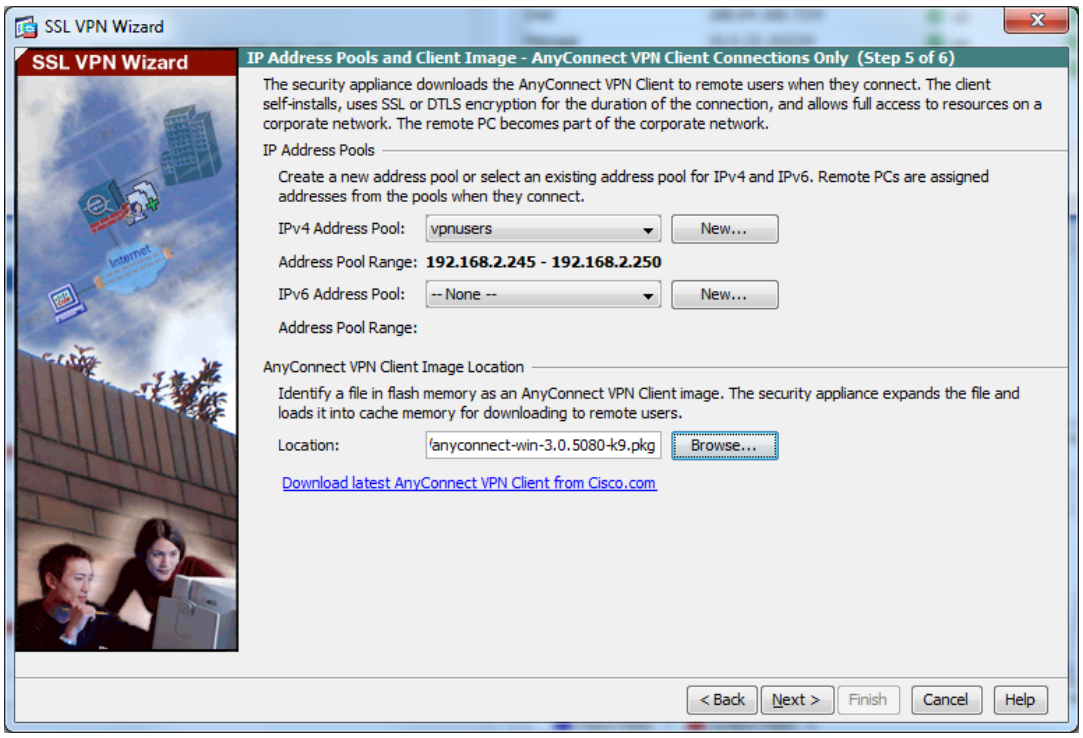


Здесь сначала создаем пул ip адресов, из которого будут выдаваться ip адреса для SSL VPN клиентов.

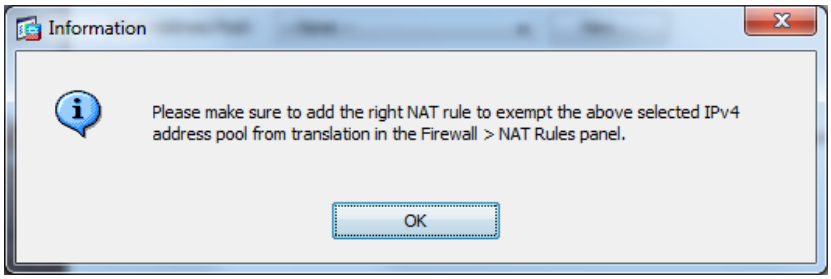
Задаем название pool-а, начальный и конечный адреса и маску подсети. Нажимаем «OK».



На этой же странице загружаем образ клиента Cisco AnyConnect под Windows.
Для того чтобы его загрузить во flash cisco ASA, необходимо нажать в соответствующем пункте «Browse», в следующем появившемся окошке «Upload»,
затем в следующем окошке «Browse local files» и указать нужный файл из списка. Далее нажимаем по порядку «Select»---«Upload File»---«OK»
(после нажатий будут всплывать информационные окошки об успешном выполнении). В итоге, получиться вот такое окно:

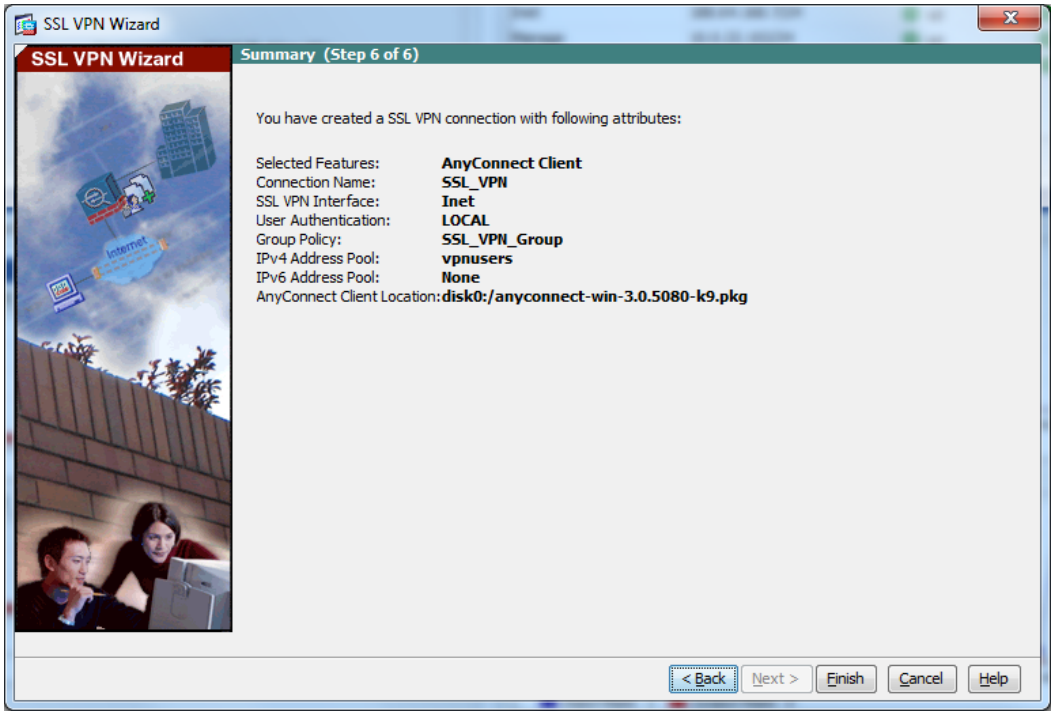


Нажимаем «Next»:



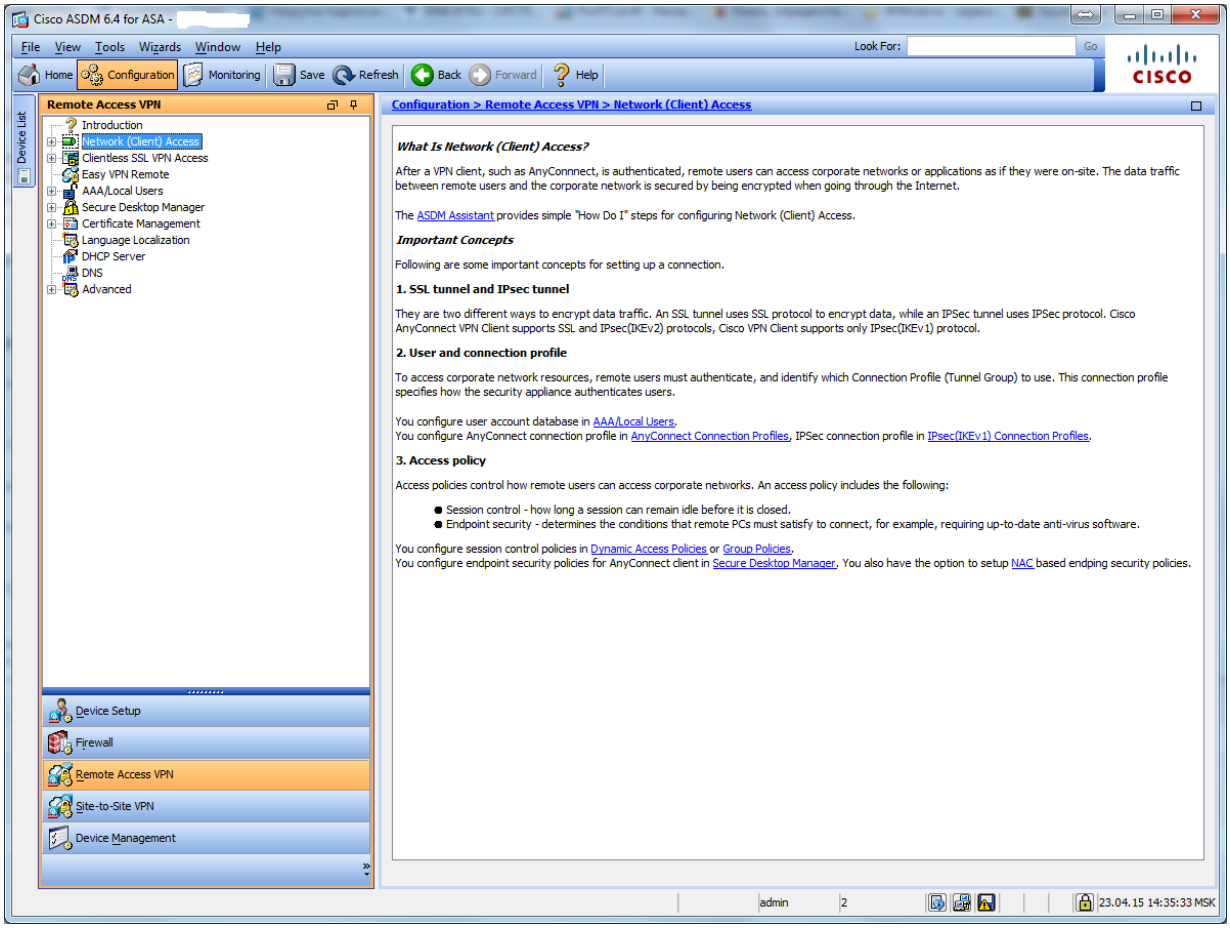
Это окно напоминает, что адреса, которые используются в пуле не должны попадать под политики NAT, если он настроен на cisco.

Нажимаем «OK».

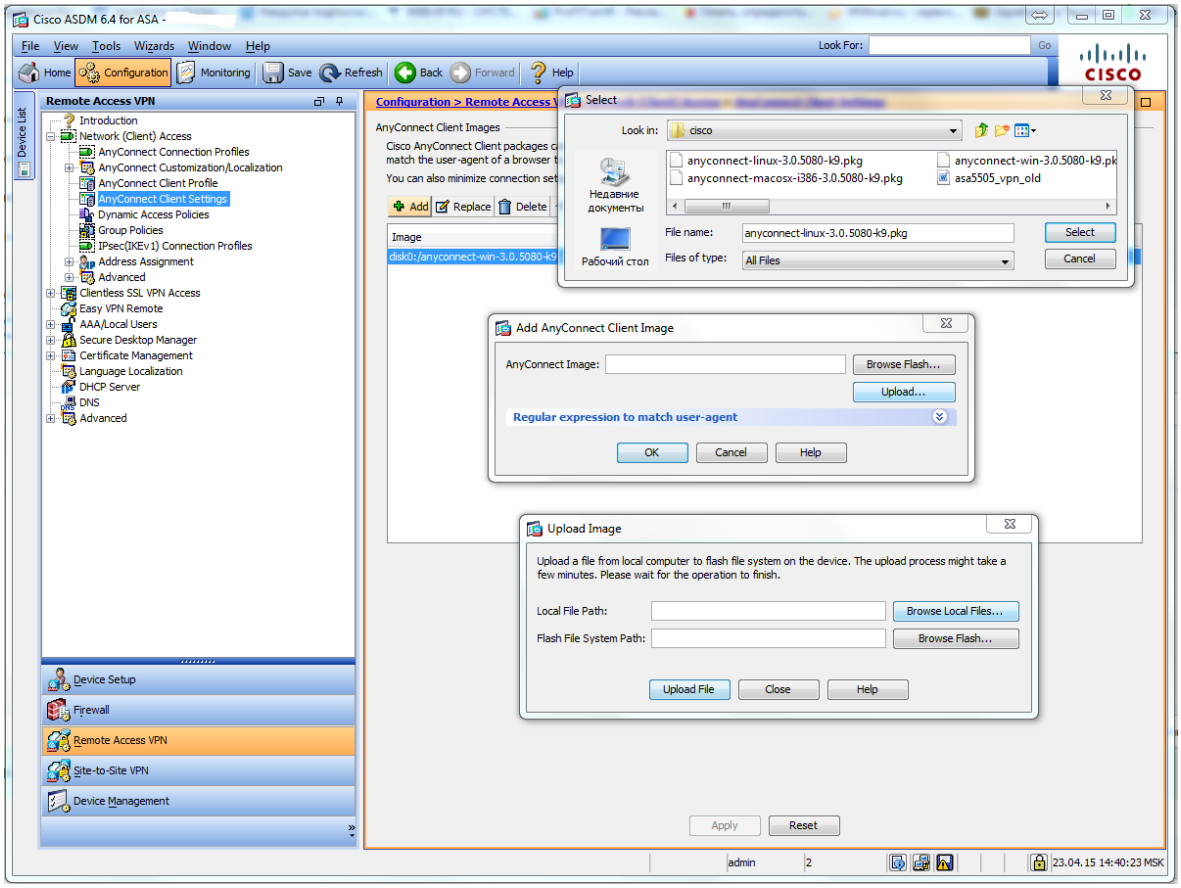


Здесь показаны все наши настройки, которые будут сконфигурированы. Нажимаем «Finish».

Более точные настройки (не через Wizard) можно посмотреть в разделе Configuration - Remote Access VPN



Нам необходимо добавить образы клиента под Mac и Linux, для этого заходим в раздел Network (Client) Access - AnyConnect Client Settings,
Здесь мы увидим уже загруженный образ клиента под Windows, нажимаем кнопку с зеленым плюсиком Add, и по аналогии как в Wizard добавляем образы под Linux и Mac.
После чего нажимаем кнопку "Aplly" внизу страницы.



По умолчанию весь трафик клиента попадает в туннель, так как эта настройка наследуется из политики по умолчанию.

Для того чтобы указать какой трафик должен попадать в туннель, необходимо создать ACL, который будет его описывать и изменить политику туннелирования.

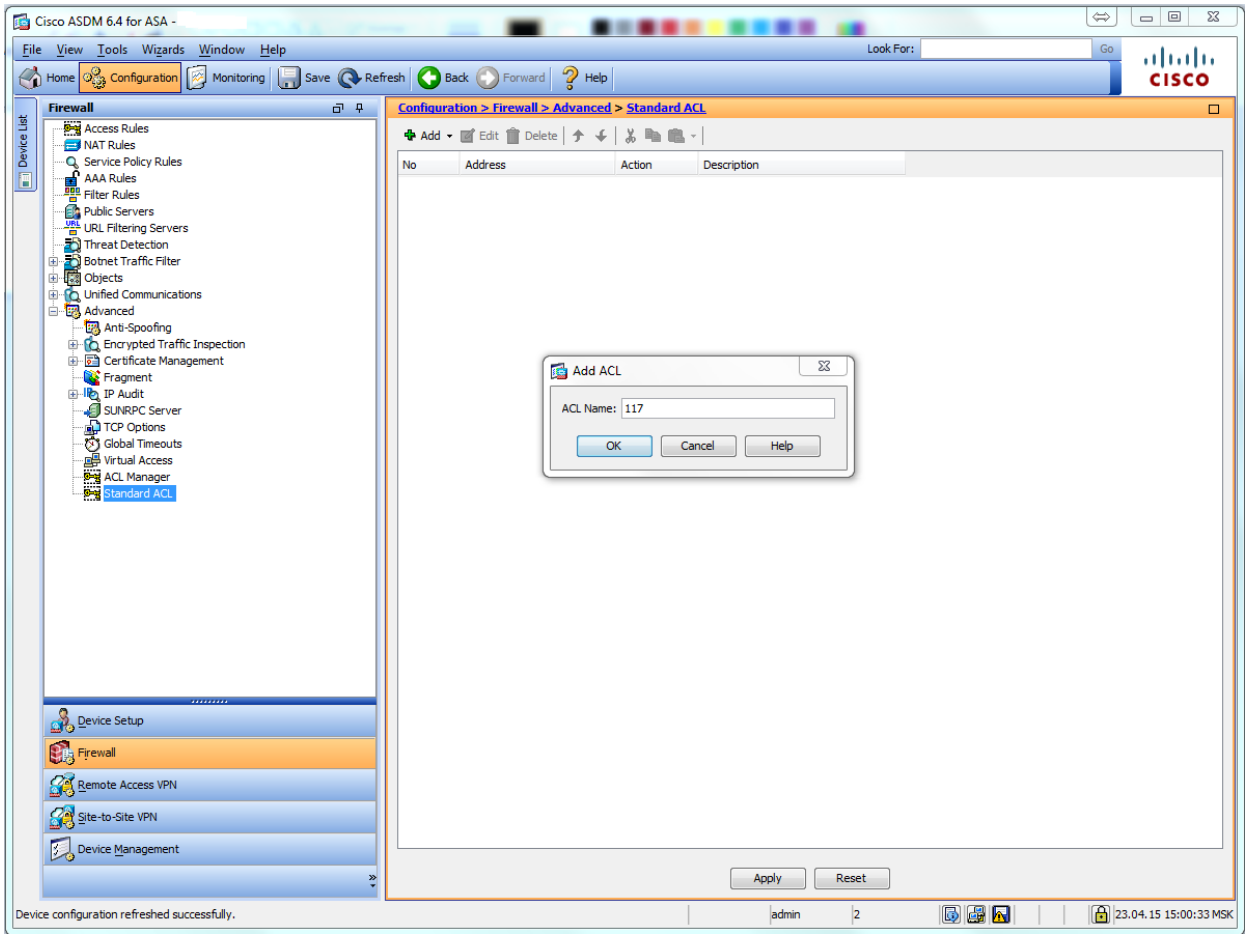
Эта функция называется split tunneling.

Для групповой политики SSL_VPN в туннель будет попадать только трафик, который идет в сеть 192.168.2.0/24.

Сначала создадим access-list, под который будет попадать трафик 192.168.2.0/24.

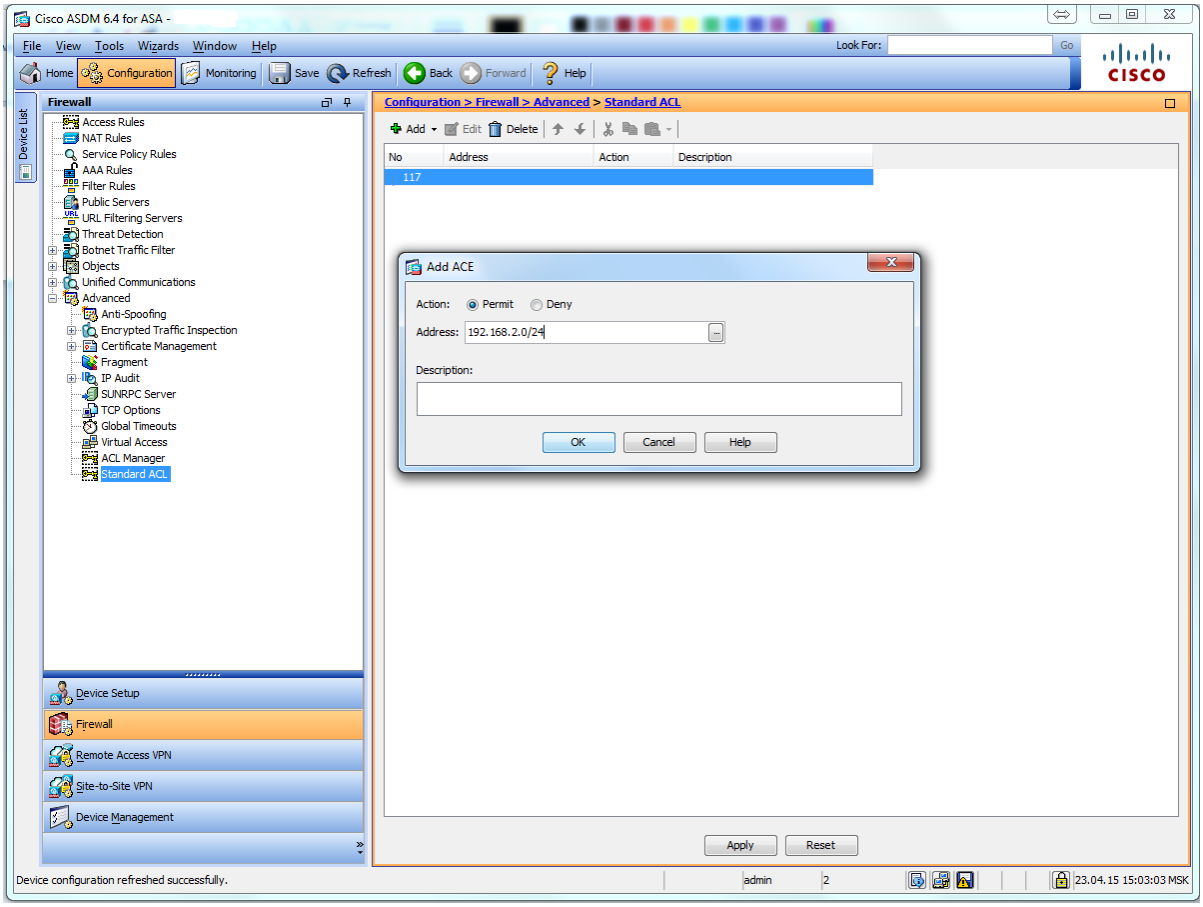
Для этого заходим в раздел Configuration - Firewall - Advanced - Standart ACL, нажимаем кнопку с зеленым плюсиком Add, в выпадающем списке выбираем Add ACL.

В появившемся окне вводим номер ACL и нажимаем OK.



Теперь нужно добавить содержимое для этого листа, это будет одна строка, встаем на наш аксесс лист 117, нажимаем кнопку с зеленым плюсиком Add, в выпадающем списке выбираем Add ACL.
Появится окно для ввода содержимого, Action оставляем Permit, в строку address вводим 192.168.2.0/24. Нажимаем OK и Aplly внизу страницы.

Аксесс-лист готов.



Теперь настраиваем split tunneling. Для этого нужно зайти в настройки самой групповой политики.

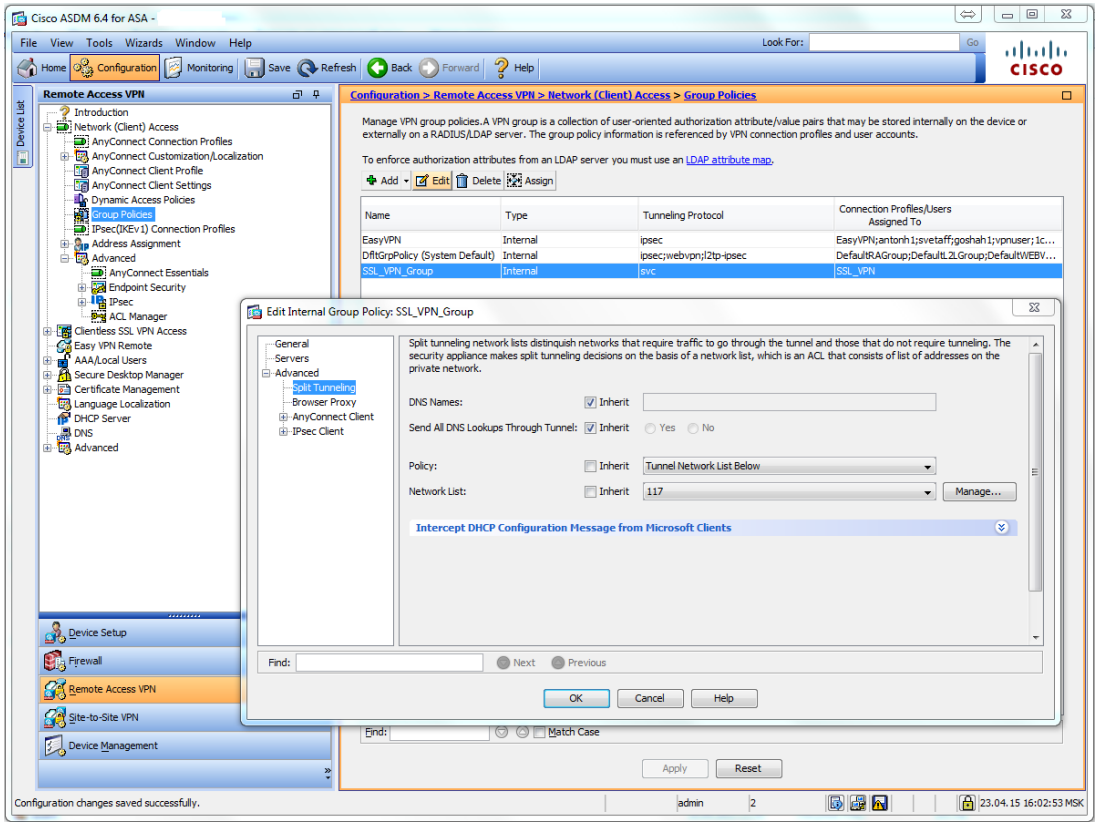
Идем Configuration - Remote Access VPN - Network (Client) Access - Group Policies.

В открывшемся окне в списке политик находим нашу SSL_VPN_Group. Встаем на нее, нажимаем кнопку Edit.

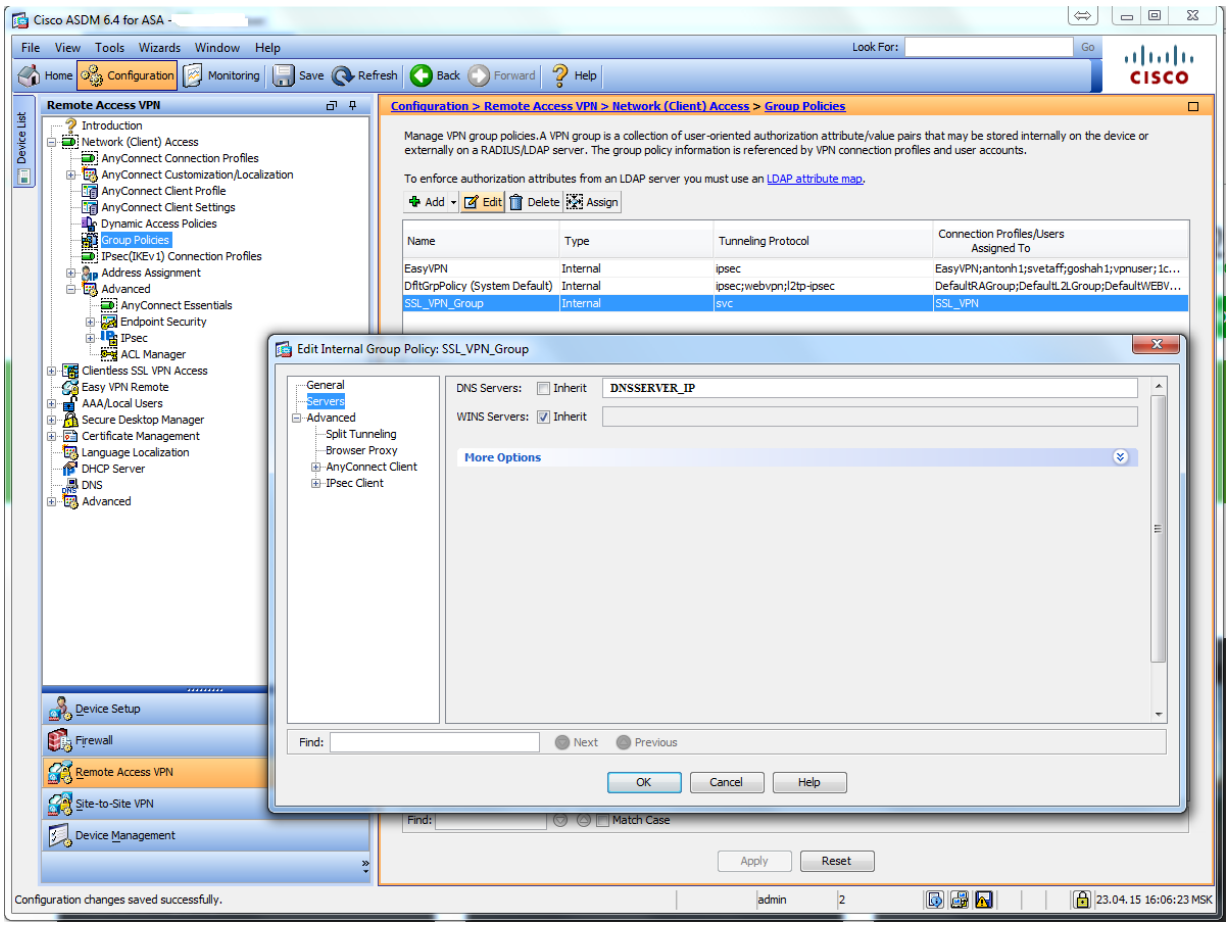
Откроется окно настроек групповой политики. Слева разворачиваем вкладку Advanced, выбираем Split Tunneling.

Напротив записи Policy убираем галку Inherit, и в выпадающем списке выбираем Tunnel Network List Bellow.

Напротив записи Network List убираем галку Inherit, и в выпадающем списке выбираем аксесс-лист 117. Нажимаем OK и Aplly внизу страницы.



Если имеется локальный DNS сервер также нужно прописать его в групповой политике. Идем туда же в настройки групповой политики. Слева выбираем Servers. Напротив строки DNS servers убираем галку Inherit и вписываем адрес локального DNS сервера. Нажимаем OK и Aplly внизу страницы.



Настройка с помощью CLI

Теперь посмотрим какие настройки появились у нас в CLI.

Акксесс-лист для опции Split Tunneling.

access-list 117 standard permit 192.168.2.0 255.255.255.0
Пул для ip адресов

ip local pool vpnusers 192.168.2.245-192.168.2.250 mask 255.255.255.0

Настройки webvpn. Включение svc. Интерфейс Inet. Пути к образам клиентов.
webvpn
 enable Inet
 anyconnect-essentials
 svc image disk0:/anyconnect-win-3.0.5080-k9.pkg 1
 svc image disk0:/anyconnect-linux-3.0.5080-k9.pkg 2
 svc image disk0:/anyconnect-macosx-i386-3.0.5080-k9.pkg 3
 svc enable
 tunnel-group-list enable

Настройки профайла.
tunnel-group SSL_VPN type remote-access
tunnel-group SSL_VPN general-attributes
 address-pool vpnusers
 default-group-policy SSL_VPN_Group

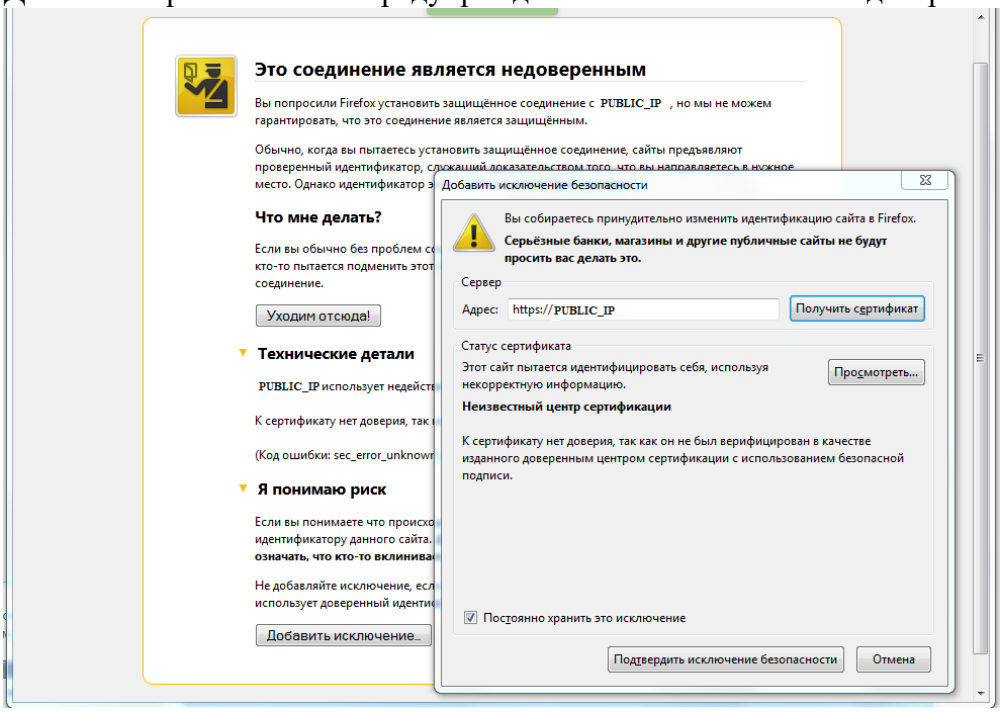
```
tunnel-group SSL_VPN webvpn-attributes
 group-alias SSL_VPN enable
```

Настройки групповой политики. DNS сервер. Опция split-tunnel.

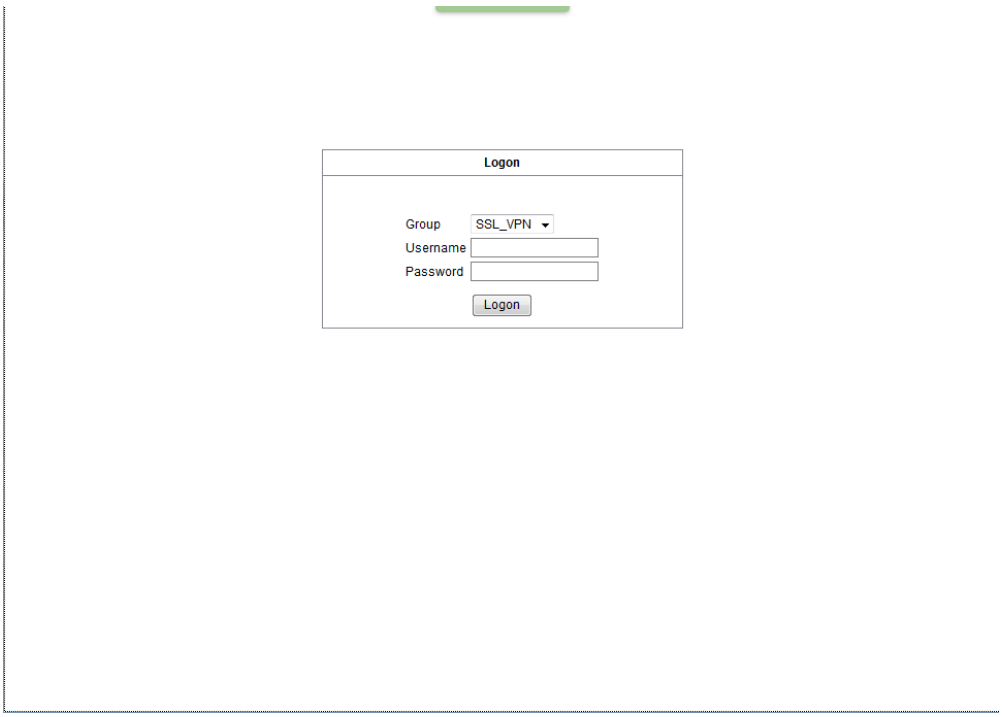
```
group-policy SSL_VPN_Group internal
group-policy SSL_VPN_Group attributes
 dns-server value DNSSERVER_IP
 vpn-tunnel-protocol svc
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value 117
 default-domain none
```

Установка клиента

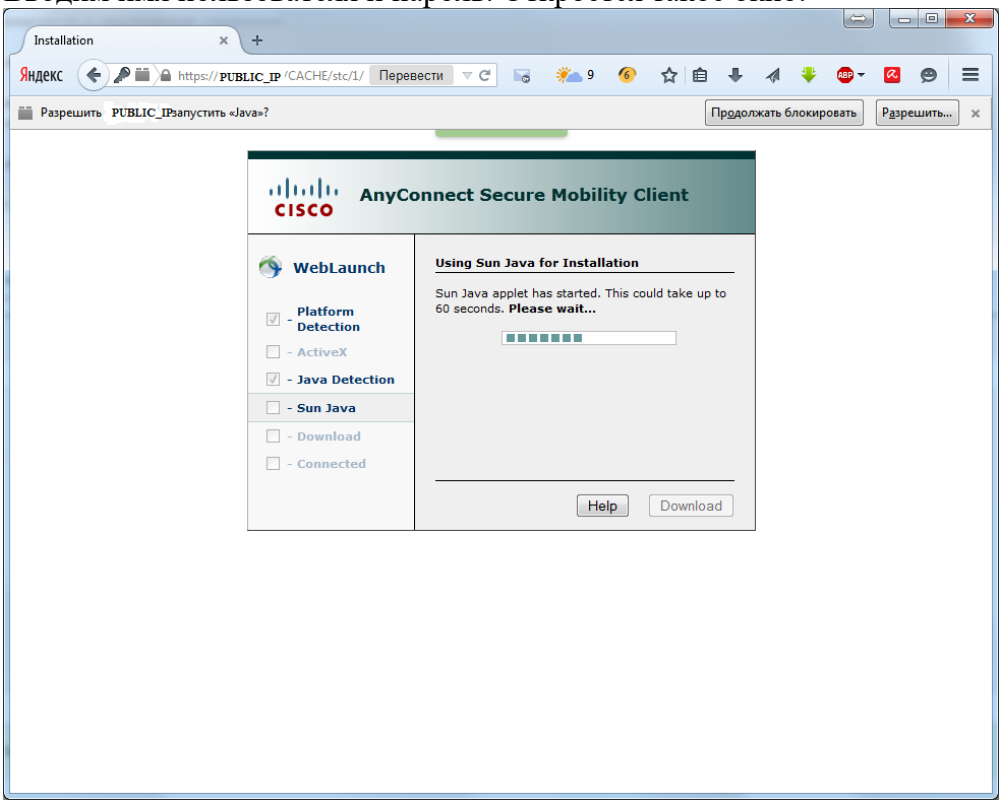
Заходим в браузер. В адресной строке набираем https://PUBLIC_IP
Должно открыться окно с предупреждением безопасности о недоверенном соединении.



Со всем соглашаемся (устанавливаем (получаем) сертификат и добавляем источник в исключения).
Нажимаем на «Подтвердить исключение безопасности» и у вас откроется следующее окно:

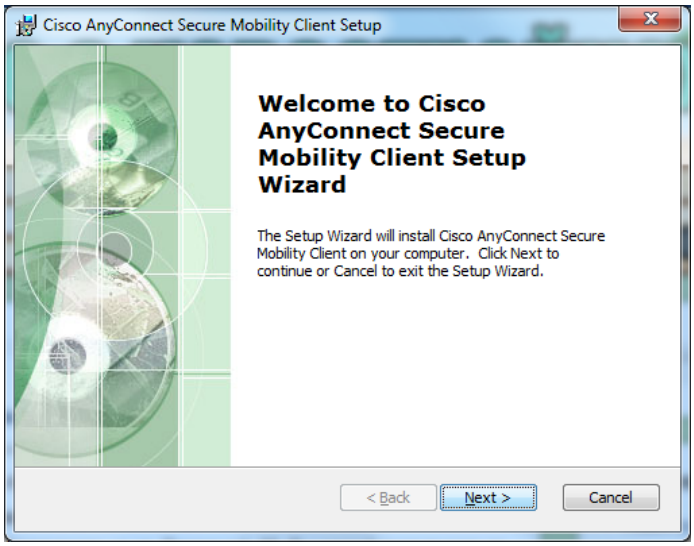


Вводим имя пользователя и пароль. Откроется такое окно:



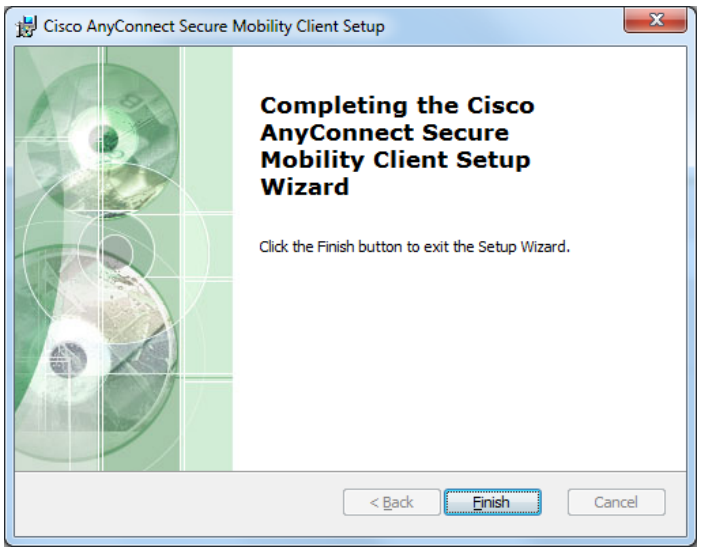
Программа установки пытается определить установленную ОС, для того чтобы запустить установку Cisco AnyConnect Client.
В результате программа предложить скачать подходящий под ОС образ:

Скачиваем образ и запускаем программу установки:

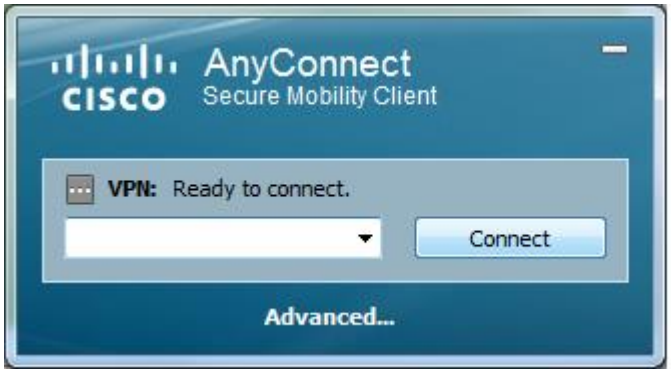


Нажимаем Next, принимаем лицензионное соглашение, Next, Install. Начнется установка.

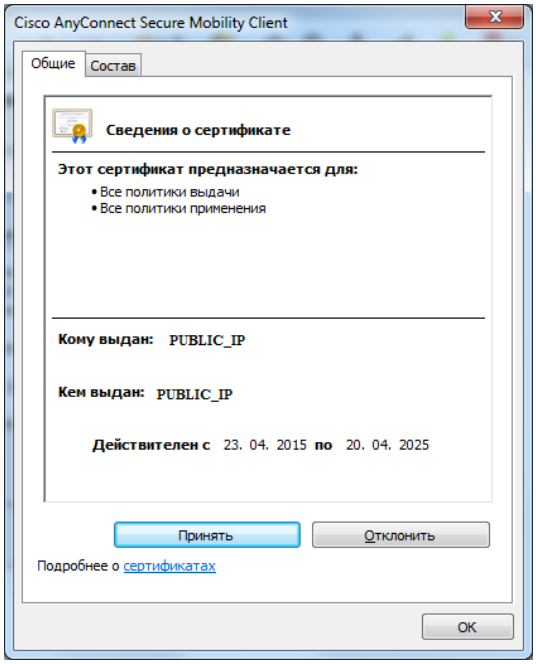
Нажимаем Finish. Установка завершена.



Запускаем программу. Справа внизу появится окошко.

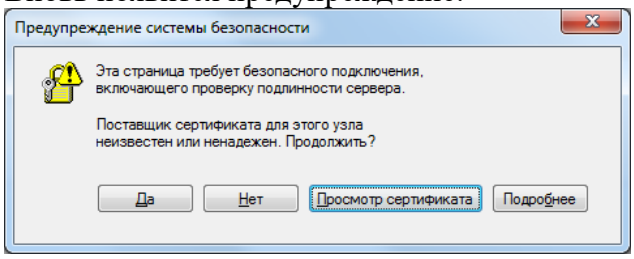


Вводим ip-адрес для подключения, нажимаем Connect.
Появится окно с информацией о сертификате.



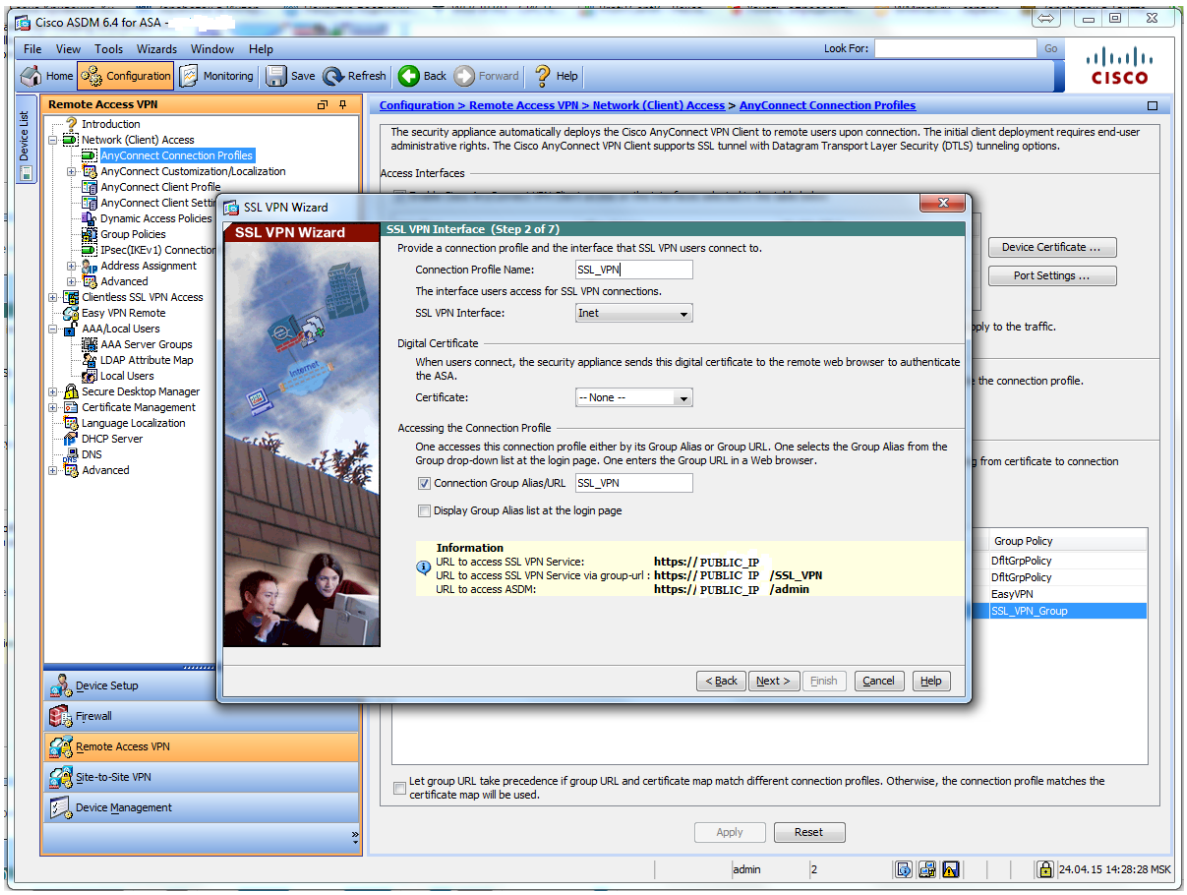
Нажимаем "Принять". Появится окно с запросом логина и пароля.

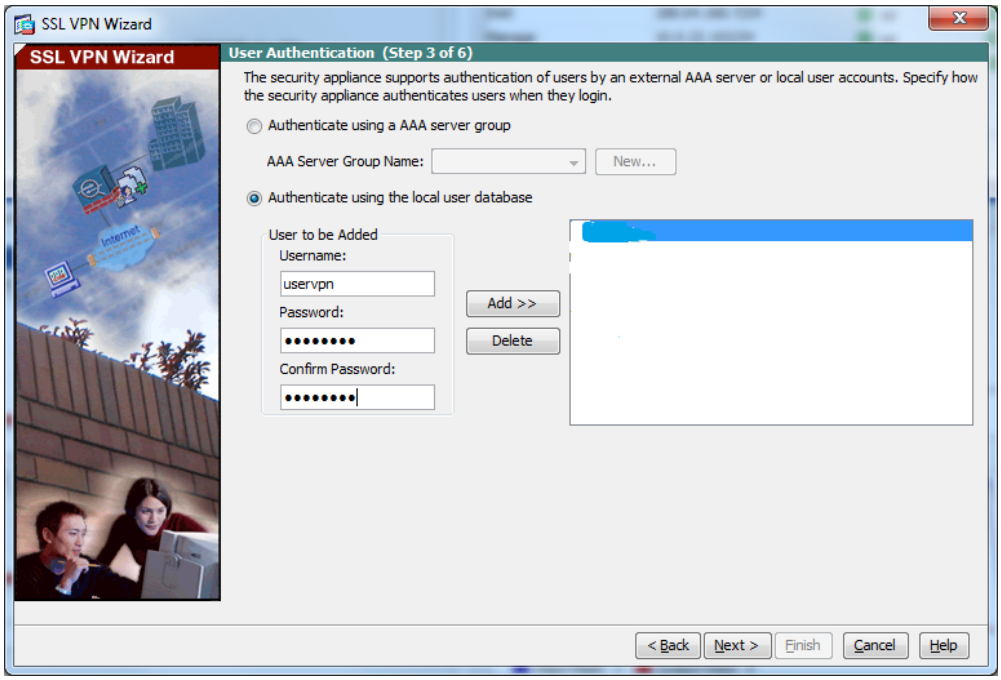
Вновь появится предупреждение:

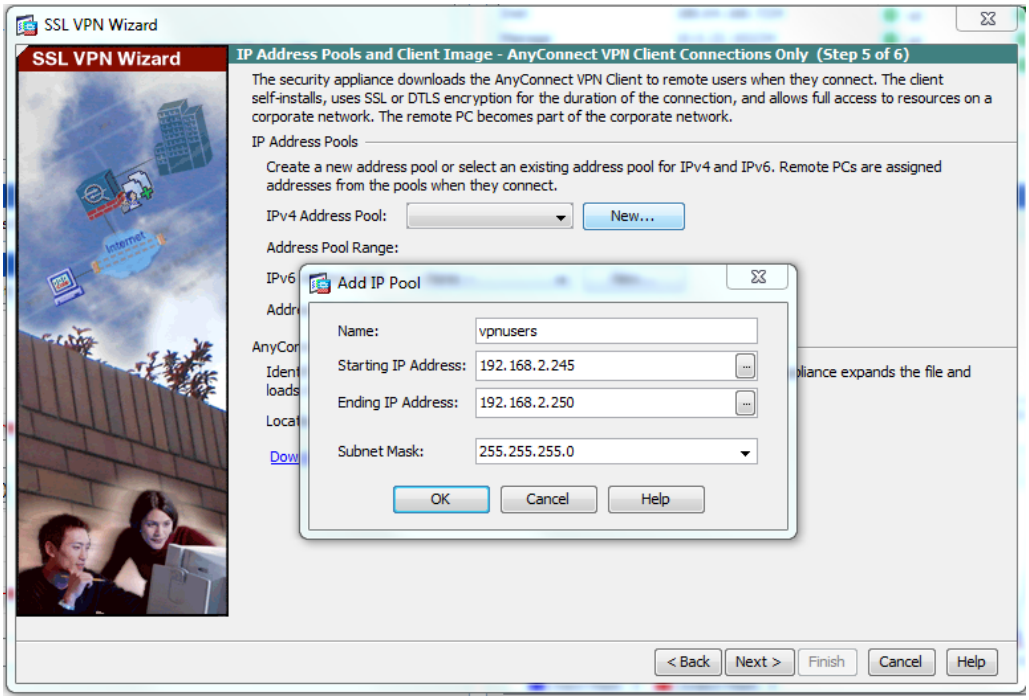


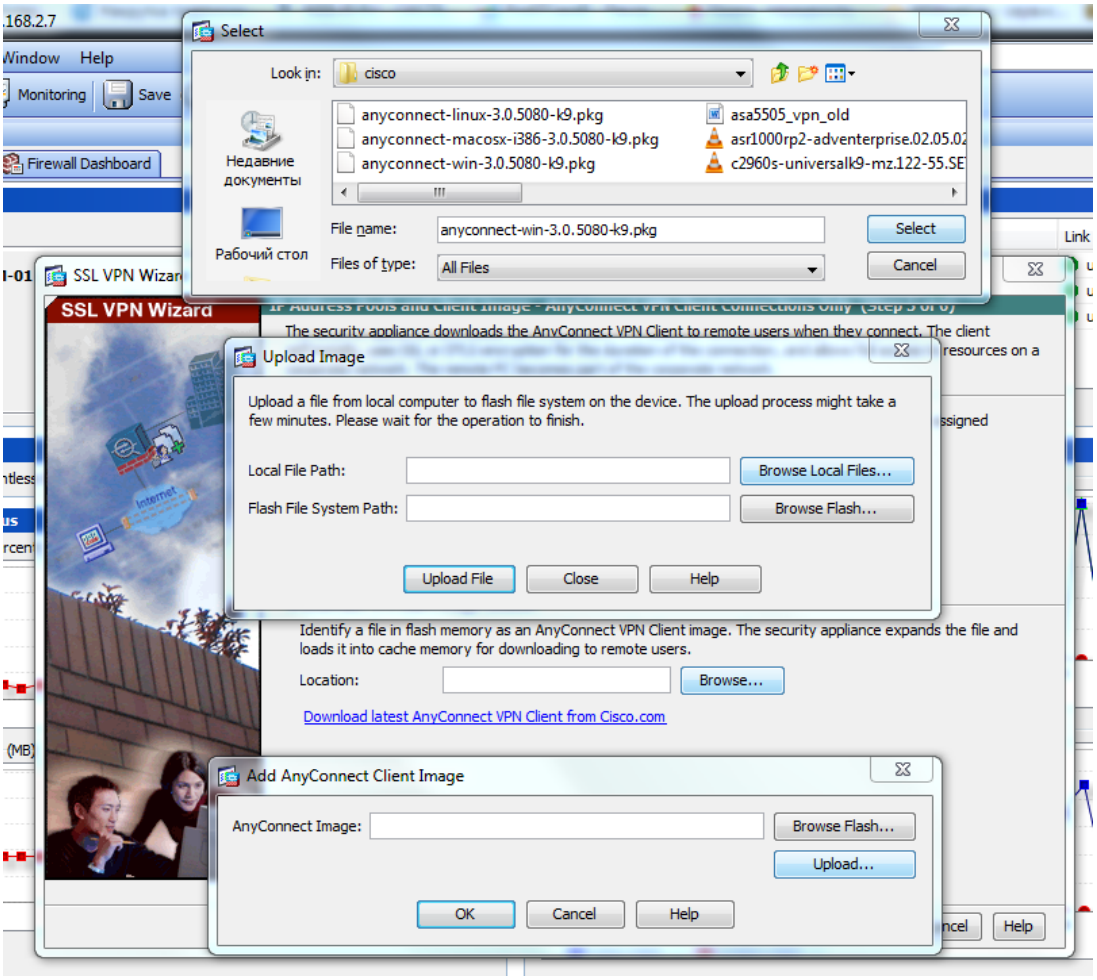
Нажимаем Принять, начнется подключение. В результате окно справа внизу примет вид. VPN подключен.

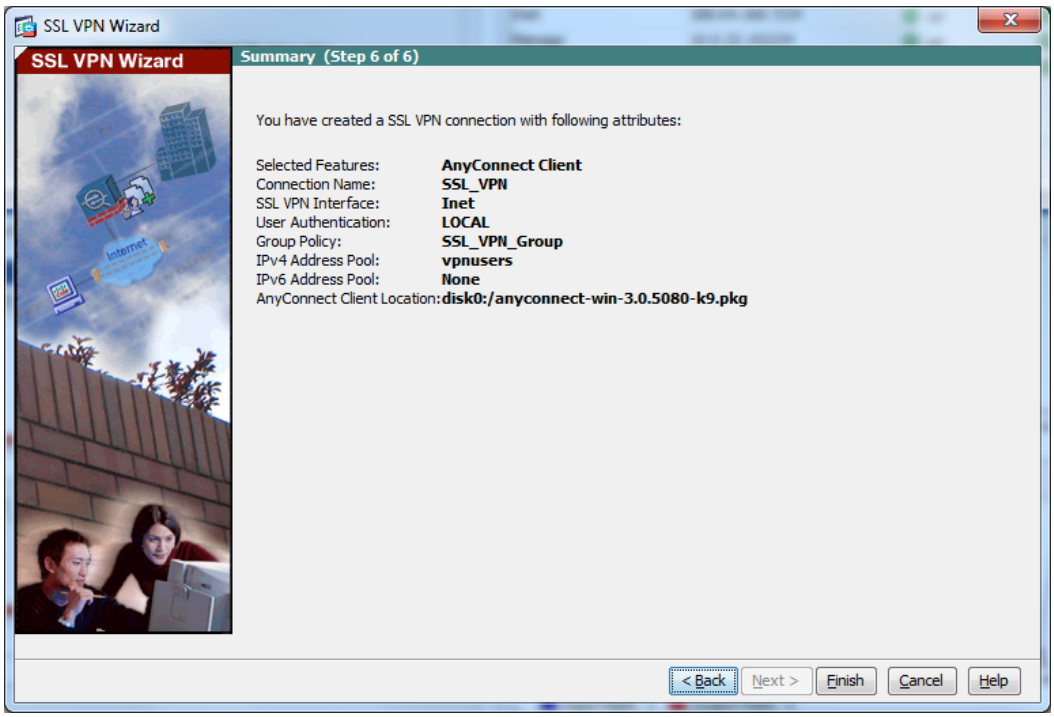
Эталон ответа:

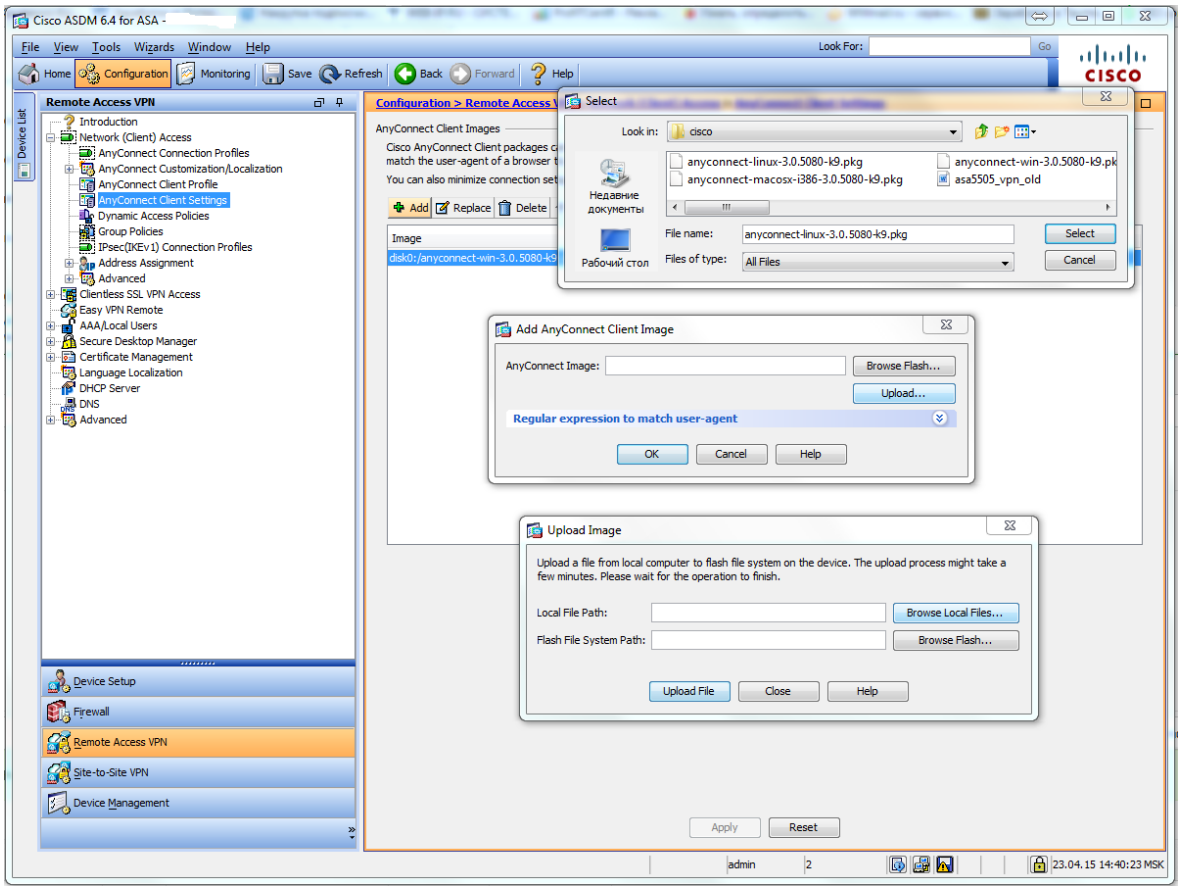

Cisco ASDM 6.4 for ASA -
File View Tools Wizards Window Help
Look For:
Home Configuration Monitoring Save Refresh Back Forward Help
Remote Access VPN
Introduction
Network (Client) Access
AnyConnect Connection Profiles
AnyConnect Customization/Localization
AnyConnect Client Profile
AnyConnect Client Sett
Dynamic Access Policies
Group Policies
IPsec(IKEv1) Connectio
Address Assignment
Advanced
Clientless SSL VPN Access
Easy VPN Remote
AAA/Local Users
AAA Server Groups
LDAP Attribute Map
Local Users
Secure Desktop Manager
Certificate Management
Language Localization
DHCP Server
DNS
Advanced
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles
The security appliance automatically deploys the Cisco AnyConnect VPN Client to remote users upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports SSL tunnel with Datagram Transport Layer Security (DTLS) tunneling options.
Access Interfaces
Device Certificate ...
Port Settings ...
Group Policy
DfltGrpPolicy
DfltGrpPolicy
EasyVPN
SSL_VPN_Group
Let group URL take precedence if group URL and certificate map match different connection profiles. Otherwise, the connection profile matches the certificate map will be used.
Apply
Reset
admin
2
24.04.15 14:28:28 MSK
SSL VPN Wizard
SSL VPN Wizard
SSL VPN Interface (Step 2 of 7)
Provide a connection profile and the interface that SSL VPN users connect to.
Connection Profile Name:
SSL_VPN
The interface users access for SSL VPN connections.
SSL VPN Interface:
Inet
Digital Certificate
When users connect, the security appliance sends this digital certificate to the remote web browser to authenticate the ASA.
Certificate:
-- None --
Accessing the Connection Profile
One accesses this connection profile either by its Group Alias or Group URL. One selects the Group Alias from the Group drop-down list at the login page. One enters the Group URL in a Web browser.
Connection Group Alias/URL
SSL_VPN
Display Group Alias list at the login page
Information
URL to access SSL VPN Service: https:// PUBLIC_IP
URL to access SSL VPN Service via group-url : https:// PUBLIC_IP /SSL_VPN
URL to access ASDM: https:// PUBLIC_IP /admin
< Back
Next >
Finish
Cancel
Help

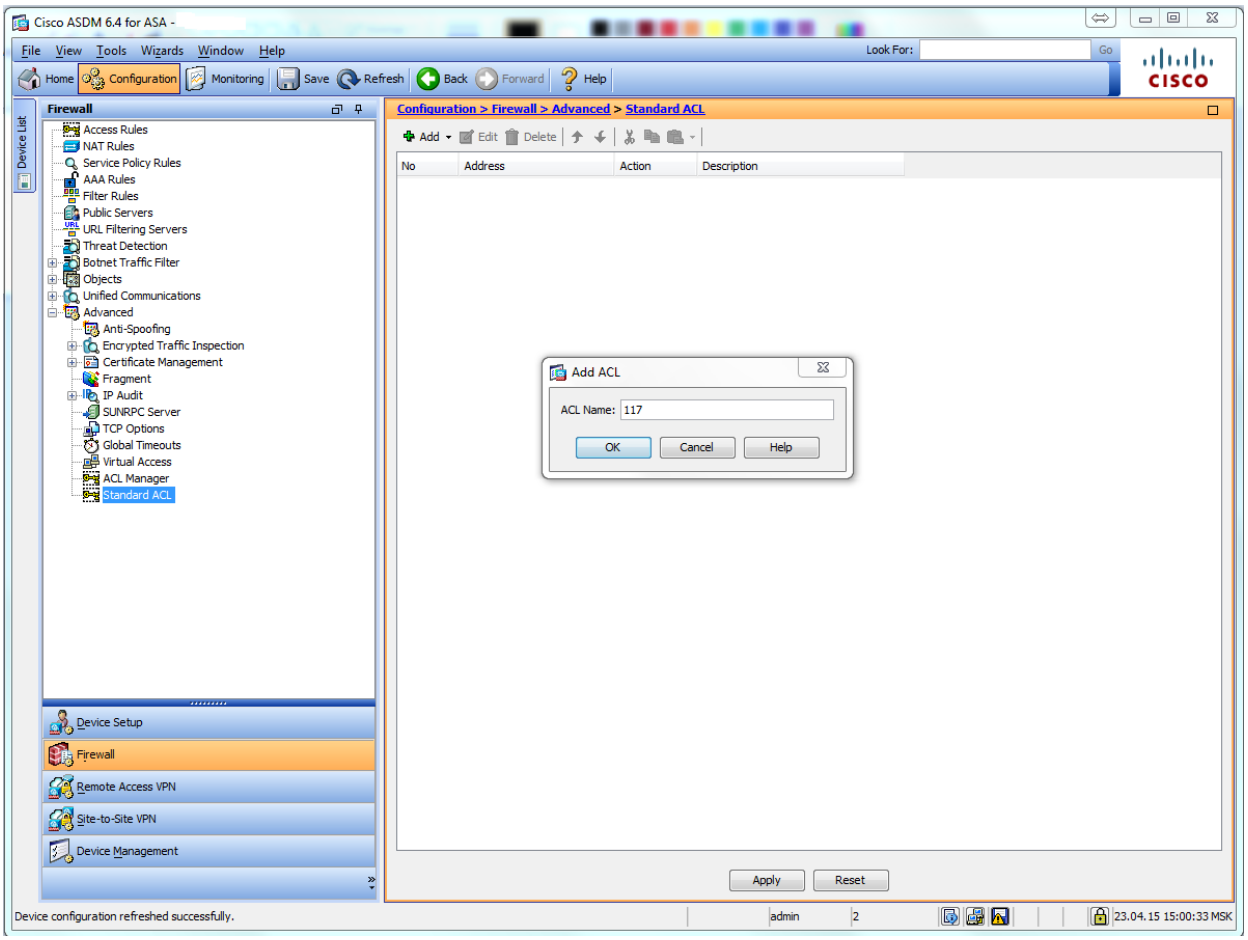

SSL VPN Wizard
SSL VPN Wizard
User Authentication (Step 3 of 6)
The security appliance supports authentication of users by an external AAA server or local user accounts. Specify how the security appliance authenticates users when they login.
Authenticate using a AAA server group
AAA Server Group Name:
New...
Authenticate using the local user database
User to be Added
Username:
uservpn
Password:
Confirm Password:
Add >>
Delete
< Back
Next >
Finish
Cancel
Help

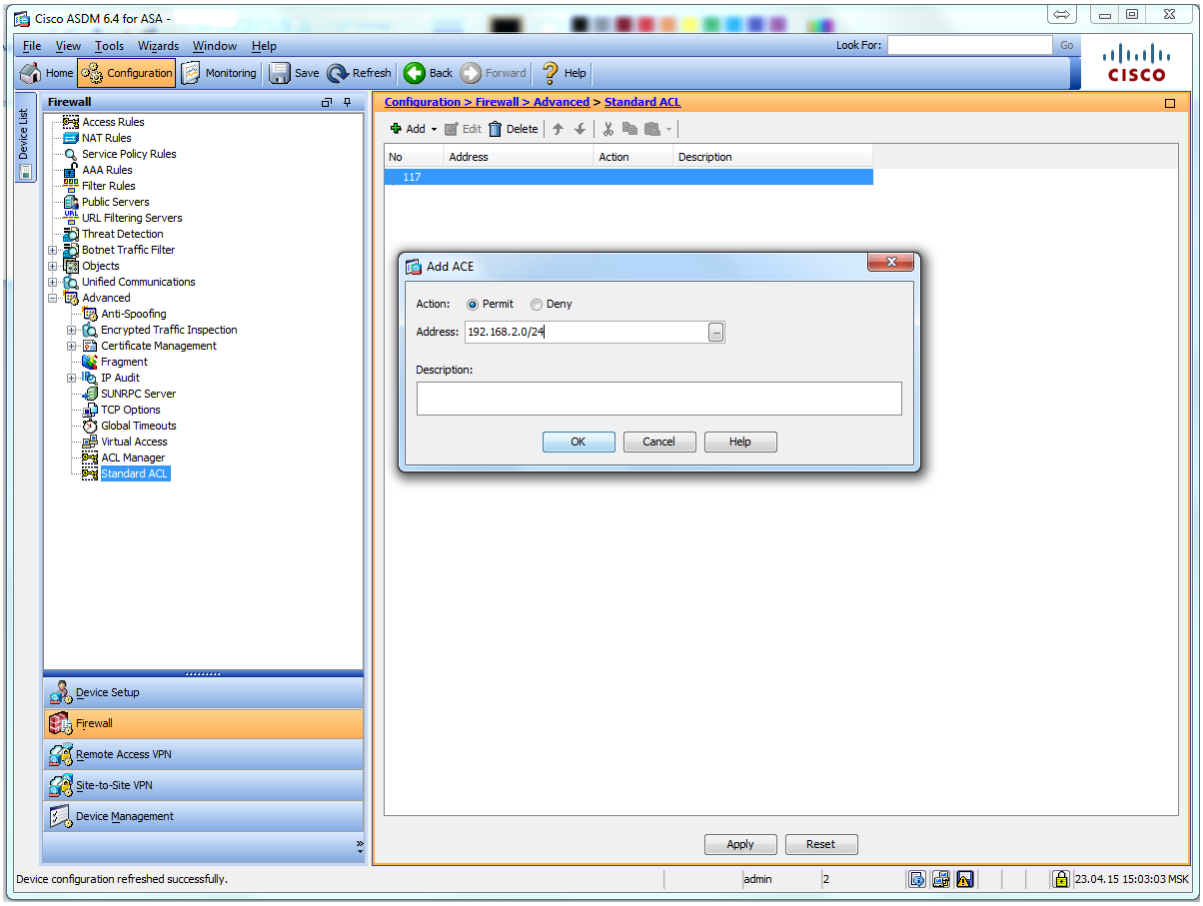

SSL VPN Wizard
SSL VPN Wizard
IP Address Pools and Client Image - AnyConnect VPN Client Connections Only (Step 5 of 6)
The security appliance downloads the AnyConnect VPN Client to remote users when they connect. The client self-installs, uses SSL or DTLS encryption for the duration of the connection, and allows full access to resources on a corporate network. The remote PC becomes part of the corporate network.
IP Address Pools
Create a new address pool or select an existing address pool for IPv4 and IPv6. Remote PCs are assigned addresses from the pools when they connect.
IPv4 Address Pool:
New...
Address Pool Range:
Add IP Pool
Name:
vpnusers
Starting IP Address:
192.168.2.245
Ending IP Address:
192.168.2.250
Subnet Mask:
255.255.255.0
OK
Cancel
Help
< Back
Next >
Finish
Cancel
Help

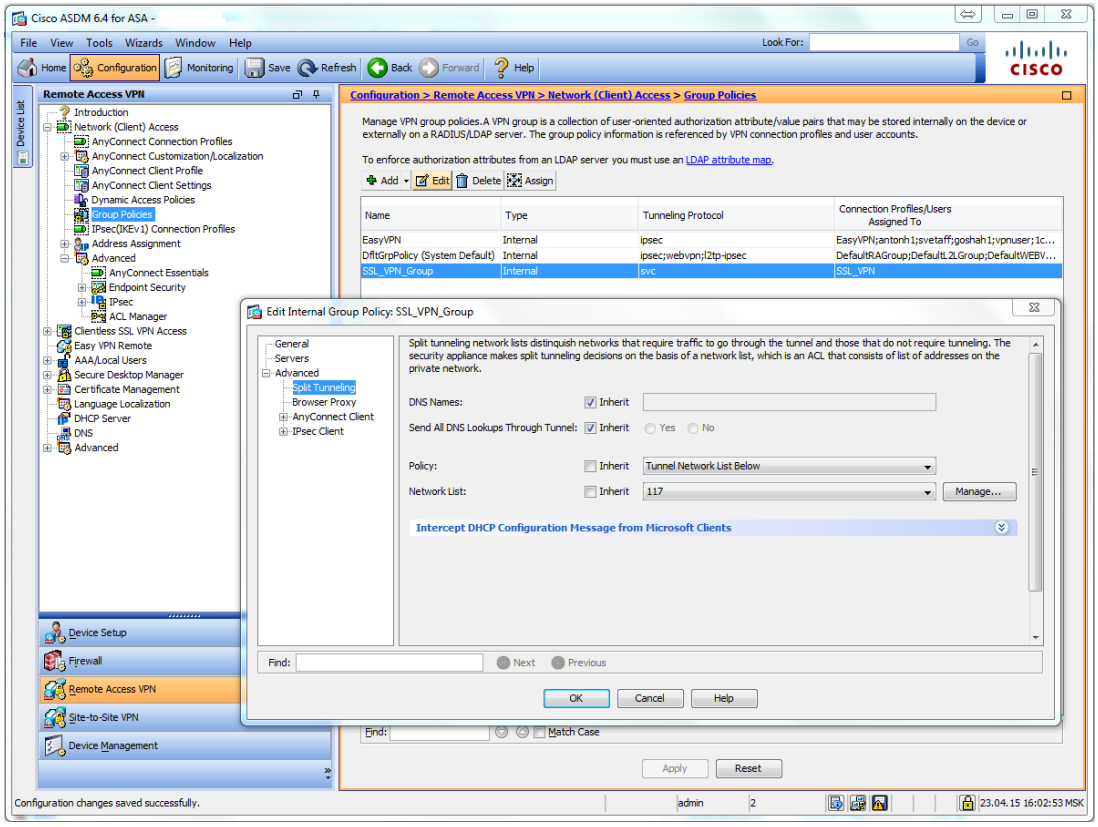

Select
Look in:
cisco
anyconnect-linux-3.0.5080-k9.pkg
anyconnect-macosx-i386-3.0.5080-k9.pkg
anyconnect-win-3.0.5080-k9.pkg
asa5505_vpn_old
asr1000rp2-adventerprise.02.05.02
c2960s-universalk9-mz.122-55.SE
Недавние документы
Рабочий стол
File name:
anyconnect-win-3.0.5080-k9.pkg
Files of type:
All Files
Select
Cancel
Monitoring
Save
Firewall Dashboard
SSL VPN Wizard
Upload Image
Upload a file from local computer to flash file system on the device. The upload process might take a few minutes. Please wait for the operation to finish.
Local File Path:
Browse Local Files...
Flash File System Path:
Browse Flash...
Upload File
Close
Help
Identify a file in flash memory as an AnyConnect VPN Client image. The security appliance expands the file and loads it into cache memory for downloading to remote users.
Location:
Browse...
Download latest AnyConnect VPN Client from Cisco.com
Add AnyConnect Client Image
AnyConnect Image:
Browse Flash...
Upload...
OK
Cancel
Help

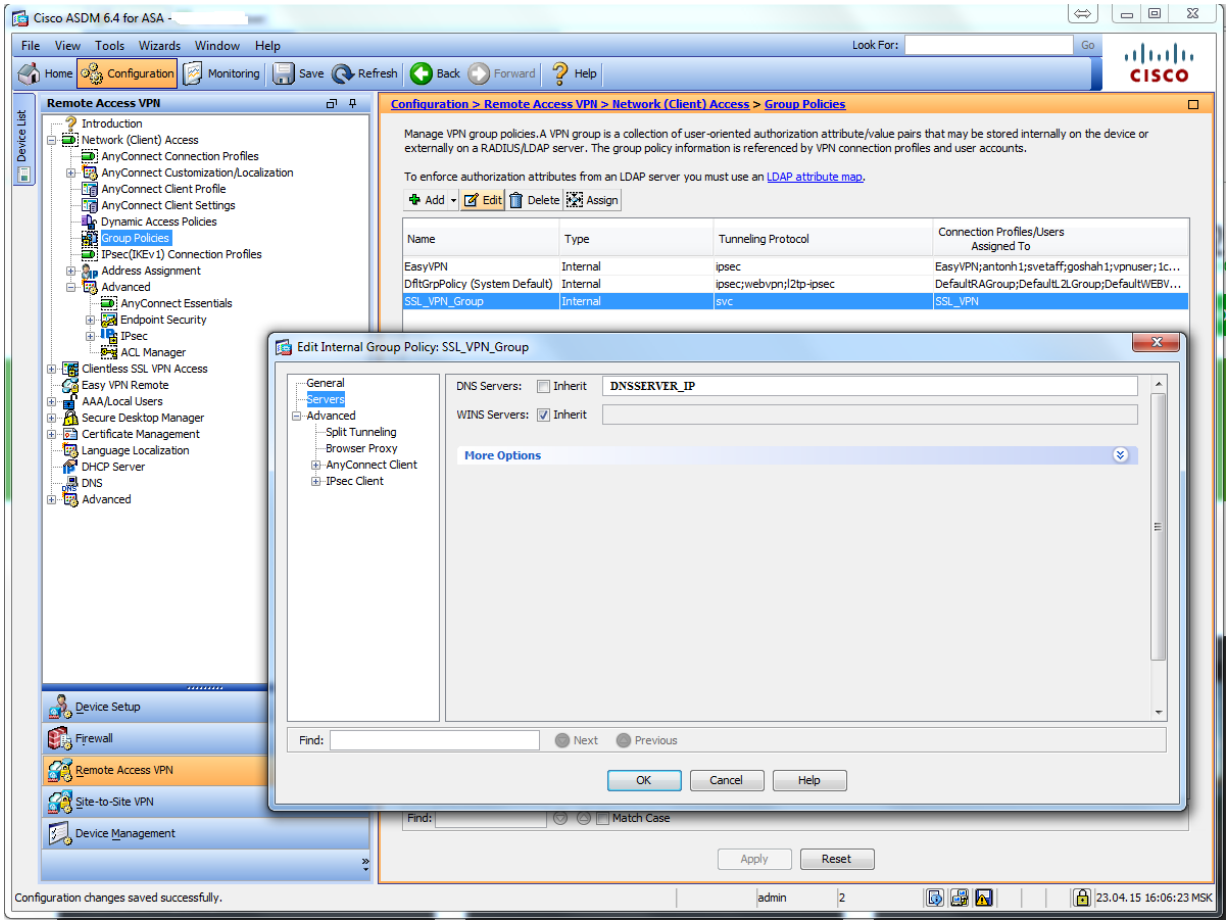

SSL VPN Wizard
SSL VPN Wizard
Summary (Step 6 of 6)
You have created a SSL VPN connection with following attributes:
Selected Features: AnyConnect Client
Connection Name: SSL_VPN
SSL VPN Interface: Inet
User Authentication: LOCAL
Group Policy: SSL_VPN_Group
IPv4 Address Pool: vpnusers
IPv6 Address Pool: None
AnyConnect Client Location: disk0:/anyconnect-win-3.0.5080-k9.pkg
< Back
Next >
Finish
Cancel
Help


Cisco ASDM 6.4 for ASA -
File View Tools Wizards Window Help
Look For:
Home Configuration Monitoring Save Refresh Back Forward Help
Remote Access VPN
Introduction
Network (Client) Access
AnyConnect Connection Profiles
AnyConnect Customization/Localization
AnyConnect Client Profile
AnyConnect Client Settings
Dynamic Access Policies
Group Policies
IPsec(IKEv1) Connection Profiles
Address Assignment
Advanced
Clientless SSL VPN Access
Easy VPN Remote
AAA/Local Users
Secure Desktop Manager
Certificate Management
Language Localization
DHCP Server
DNS
Advanced
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Configuration > Remote Access
AnyConnect Client Images
Add Replace Delete
Image
Select
Look in: cisco
anyconnect-linux-3.0.5080-k9.pkg
anyconnect-macosx-i386-3.0.5080-k9.pkg
anyconnect-win-3.0.5080-k9.pk
asa5505_vpn_old
File name: anyconnect-linux-3.0.5080-k9.pkg
Files of type: All Files
Select
Cancel
Add AnyConnect Client Image
AnyConnect Image:
Browse Flash...
Upload...
Regular expression to match user-agent
OK
Cancel
Help
Upload Image
Upload a file from local computer to flash file system on the device. The upload process might take a few minutes. Please wait for the operation to finish.
Local File Path:
Browse Local Files...
Flash File System Path:
Browse Flash...
Upload File
Close
Help
Apply
Reset
admin
2
23.04.15 14:40:23 MSK

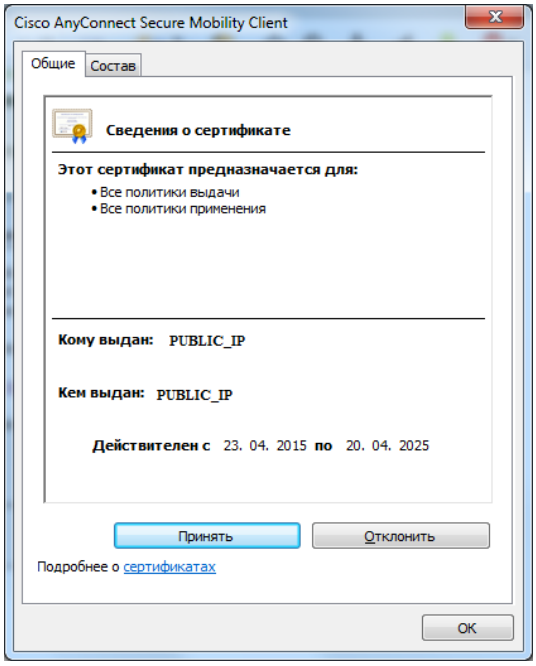

Cisco ASDM 6.4 for ASA -
File View Tools Wizards Window Help
Look For:
Home Configuration Monitoring Save Refresh Back Forward Help
Firewall
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Public Servers
URL Filtering Servers
Threat Detection
Botnet Traffic Filter
Objects
Unified Communications
Advanced
Anti-Spoofing
Encrypted Traffic Inspection
Certificate Management
Fragment
IP Audit
SUNRPC Server
TCP Options
Global Timeouts
Virtual Access
ACL Manager
Standard ACL
Configuration > Firewall > Advanced > Standard ACL
Add Edit Delete
No Address Action Description
Add ACL
ACL Name: 117
OK Cancel Help
Apply Reset
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Device configuration refreshed successfully.
admin 2 23.04.15 15:00:33 MSK


Cisco ASDM 6.4 for ASA -
File View Tools Wizards Window Help
Look For:
Home Configuration Monitoring Save Refresh Back Forward Help
Firewall
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Public Servers
URL Filtering Servers
Threat Detection
Botnet Traffic Filter
Objects
Unified Communications
Advanced
Anti-Spoofing
Encrypted Traffic Inspection
Certificate Management
Fragment
IP Audit
SUNRPC Server
TCP Options
Global Timeouts
Virtual Access
ACL Manager
Standard ACL
Configuration > Firewall > Advanced > Standard ACL
Add Edit Delete
No Address Action Description
117
Add ACE
Action: Permit Deny
Address: 192.168.2.0/24
Description:
OK Cancel Help
Apply Reset
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Device configuration refreshed successfully.
admin 2 23.04.15 15:03:03 MSK


Cisco ASDM 6.4 for ASA -
File View Tools Wizards Window Help
Look For:
Home Configuration Monitoring Save Refresh Back Forward Help
Remote Access VPN
Introduction
Network (Client) Access
AnyConnect Connection Profiles
AnyConnect Customization/Localization
AnyConnect Client Profile
AnyConnect Client Settings
Dynamic Access Policies
Group Policies
IPsec(IKEv1) Connection Profiles
Address Assignment
Advanced
AnyConnect Essentials
Endpoint Security
IPsec
ACL Manager
Clientless SSL VPN Access
Easy VPN Remote
AAA/Local Users
Secure Desktop Manager
Certificate Management
Language Localization
DHCP Server
DNS
Advanced
Configuration > Remote Access VPN > Network (Client) Access > Group Policies
Manage VPN group policies.A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy information is referenced by VPN connection profiles and user accounts.
To enforce authorization attributes from an LDAP server you must use an LDAP attribute map.
Add Edit Delete Assign
Name
Type
Tunneling Protocol
Connection Profiles/Users Assigned To
EasyVPN
Internal
ipsec
EasyVPN;antonh1;svetaff;goshah1;vpnuser;1c...
DfltGrpPolicy (System Default)
Internal
ipsec;webvpn;l2tp-ipsec
DefaultRAGroup;DefaultL2LGroup;DefaultWEBV...
SSL_VPN_Group
Internal
svc
SSL_VPN
Edit Internal Group Policy: SSL_VPN_Group
General
Servers
Advanced
Split Tunneling
Browser Proxy
AnyConnect Client
IPsec Client
Split tunneling network lists distinguish networks that require traffic to go through the tunnel and those that do not require tunneling. The security appliance makes split tunneling decisions on the basis of a network list, which is an ACL that consists of list of addresses on the private network.
DNS Names: Inherit
Send All DNS Lookups Through Tunnel: Inherit Yes No
Policy: Inherit Tunnel Network List Below
Network List: Inherit 117 Manage...
Intercept DHCP Configuration Message from Microsoft Clients
Find: Next Previous
OK Cancel Help
Find: Match Case
Apply Reset
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Configuration changes saved successfully.
admin
2
23.04.15 16:02:53 MSK


Cisco ASDM 6.4 for ASA -
File View Tools Wizards Window Help
Look For:
Home Configuration Monitoring Save Refresh Back Forward Help
Remote Access VPN
Introduction
Network (Client) Access
AnyConnect Connection Profiles
AnyConnect Customization/Localization
AnyConnect Client Profile
AnyConnect Client Settings
Dynamic Access Policies
Group Policies
IPsec(IKEv1) Connection Profiles
Address Assignment
Advanced
AnyConnect Essentials
Endpoint Security
IPsec
ACL Manager
Clientless SSL VPN Access
Easy VPN Remote
AAA/Local Users
Secure Desktop Manager
Certificate Management
Language Localization
DHCP Server
DNS
Advanced
Configuration > Remote Access VPN > Network (Client) Access > Group Policies
Manage VPN group policies.A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy information is referenced by VPN connection profiles and user accounts.
To enforce authorization attributes from an LDAP server you must use an LDAP attribute map.
Add Edit Delete Assign
Name
Type
Tunneling Protocol
Connection Profiles/Users Assigned To
EasyVPN
Internal
ipsec
EasyVPN;antonh1;svetaff;goshah1;vpnuser;1c...
DfltGrpPolicy (System Default)
Internal
ipsec;webvpn;l2tp-ipsec
DefaultRAGroup;DefaultL2LGroup;DefaultWEBV...
SSL_VPN_Group
Internal
svc
SSL_VPN
Edit Internal Group Policy: SSL_VPN_Group
General
Servers
Advanced
Split Tunneling
Browser Proxy
AnyConnect Client
IPsec Client
DNS Servers: Inherit DNSSERVER_IP
WINS Servers: Inherit
More Options
Find: Next Previous
OK Cancel Help
Find: Match Case
Apply Reset
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Configuration changes saved successfully.
admin
2
23.04.15 16:06:23 MSK


AnyConnect Secure Mobility Client
WebLaunch
- Platform Detection
- ActiveX
- Java Detection
- Sun Java
- Download
- Connected
Manual Installation
Web-based installation was unsuccessful. If you wish to install the Cisco AnyConnect Secure Mobility Client, you may download an installer package.
Install using the link below:
Windows 7/Vista/64/XP
Alternatively, retry the automatic installation.
Help
Download


Cisco AnyConnect Secure Mobility Client
Общие
Состав
Сведения о сертификате
Этот сертификат предназначается для:
• Все политики выдачи
• Все политики применения
Кому выдан: PUBLIC_IP
Кем выдан: PUBLIC_IP
Действителен с 23. 04. 2015 по 20. 04. 2025
Принять
Отклонить
Подробнее о сертификатах
OK


Cisco AnyConnect | PUBLIC_IP
Please enter your username and password.
Group:
SSL_VPN
Username:
Password:
OK
Cancel


AnyConnect
Secure Mobility Client
VPN: Connected to PUBLIC_IP
Disconnect
Advanced...

3.2. Оценка сформированности умений и знаний, общих компетенций при выполнении курсовой работы

Основные требования к структуре, содержанию и оформлению курсовой работы представлены в Методических рекомендациях для студентов по выполнению курсовой работы.

Курсовая работа выполняется по единой теме по индивидуальным вариантам: «Проектирование компьютерной сети» и носит практический характер.

Проверяемые результаты обучения:

Показатели оценки работы

Проверяемые освоенные умения и усвоенные знания	Общие и профессиональные компетенции, формируемые в процессе выполнения роботы	Этап выполнения курсовой работы
У1-У2 З1-З5	ОК1-3, ОК9 ПК 1.1., ПК 1.2.	Выдача тем курсовых работ. Знакомство с Методическими указаниями по выполнению и оформлению курсовых работ
У1-У2 З1-З5	ОК1-3, ОК9	Знакомство с источниками информации, подбор информации в соответствии с планом курсовой работы
У1-У2 З1-З5	ОК1-3, ОК9 ПК 1.1., ПК 1.2.	Выполнение Введения к курсовой работе
У1-У2 З1-З5	ОК1-3, ОК9 ПК 1.1., ПК 1.2.	Работа над теоретической частью курсовой работы
У1-У2 З1-З5	ОК1-3, ОК9 ПК 1.1., ПК 1.2.	Работа над практической частью курсовой работы
У1-У2 З1-З5	ОК1-3, ОК9 ПК 1.1., ПК 1.2.	Работа над составлением Заключения к работе
У1-У2 З1-З5	ОК1-3, ОК9 ПК 1.1., ПК 1.2.	Разработка презентации и доклада
У1-У2 З1-З5	ОК1-3, ОК9 ПК 1.1., ПК 1.2.	Подготовка к защите КР

3.3. Контрольно-оценочные материалы для промежуточной аттестации

Формой промежуточной аттестации по МДК.01.01 и МДК.01.03 **является комплексный экзамен.**

Перечень экзаменационных вопросов:

№	Перечень теоретических вопросов
1.	Общие принципы построения сетей. Архитектура, стандартизация и классификация сетей. Оборудование локальных сетей.
2.	Модель OSI. Физический и канальный уровни. Уровни данных: сеансовый, представления, прикладной
3.	Адресация в сети Internet. Типы адресов. Специальные адреса.
4.	Универсальный идентификатор ресурсов (URI). Универсальный указатель ресурса URL. Система DNS. Протокол DHCP
5.	Организация и услуги глобальных сетей. Транспортные технологии глобальных сетей. Технология MPLS.
6.	Ethernet операторского класса. Виртуальные частные сети
7.	Служба Telnet. Протокол Telnet. Служба SSH. Протокол SSH. Регистратуры InterNet. Автономные системы. Протокол SMTP. Протоколы POP3, IMAP 4. Динамическая маршрутизация..
8.	Протоколы RIP, OSPF. Служба FTP. Протокол FTP. Протокол TFTP. Служба WWW. Протокол HTTP.
9.	Фундаментальные принципы безопасной сети
10.	Современные угрозы сетевой безопасности.
11.	Вирусы, черви и троянские кони.
12.	Методы атак на сеть.
13.	Безопасность сетевых устройств OSI
14.	Безопасный доступ к устройствам.
15.	Назначение административных ролей.
16.	Мониторинг и управление устройствами.
17.	Использование функция автоматизированной настройки безопасности.
18.	Авторизация, аутентификация и учет доступа (AAA)
19.	Фундаментальные принципы безопасной сети
20.	Средства защиты сетей

Эталон ответов: приведен в Учебных пособиях МДК.01.01, МДК.01.03.

Условия выполнения

1. Количество билетов для экзаменующегося: 1
2. Время подготовки к ответу: 30 минут
3. Требования к устным ответам:
   Полное овладение содержанием учебного материала, в котором обучающийся легко ориентируется, владение понятийным аппаратом.
4. Оборудование: учебная аудитория, стол, стул, пишущая ручка, бумага.

Результаты промежуточной аттестации фиксируются в протоколе.

Формой промежуточной аттестации по МДК.01.02 дифференцированный зачет

Перечень вопросов:

№	Перечень теоретических вопросов
1.	Спецификации и топологии сети.
2.	Современные сетевые протоколы
3.	Модели межсетевого взаимодействия.
4.	Различные типы Ethernet
5.	Структурированная кабельная система.
6.	Сетевое оборудование для проводной локальной сети.
7.	Беспроводная сеть
8.	Стандартизация сетей.
9.	Проектная документация КС
10.	Эксплуатационная документация КС.
11.	Планирование структуры сети
12.	Требования, предъявляемые к современным ВС
13.	Проектирование локальной сети
14.	Проектирование беспроводной локальной сети.
15.	Ввод в эксплуатацию компьютерных систем
16.	Протокол PPPoE.
17.	Защита межфилиальной связи.
18.	Сети VPN.
19.	Настройка туннелей GRE

Эталон ответов: приведен в Учебном пособии МДК.01.02.

Условия выполнения

5. Количество билетов для экзаменующегося: 1
6. Время подготовки к ответу: 30 минут
7. Требования к устным ответам:
   Полное овладение содержанием учебного материала, в котором обучающийся легко ориентируется, владение понятийным аппаратом.
8. Оборудование: учебная аудитория, стол, стул, пишущая ручка, бумага.

Результаты промежуточной аттестации фиксируются в протоколе.

Критерии оценки устных ответов

(Указываются критерии оценки в зависимости от видов заданий. Оставить только те критерии, которые преподаватель будет использовать))

В системе оценки знаний и умений используются **следующие критерии** (скорректировать в соответствии с особенностями дисциплины):

«Отлично» – за глубокое и полное овладение содержанием учебного материала, в котором обучающийся легко ориентируется, владение понятийным аппаратом за умение связывать теорию с практикой, решать практические задачи, высказывать и обосновывать

свои суждения. Отличная отметка предполагает грамотное, логичное изложение ответа (как в устной, так и в письменной форме), качественное внешнее оформление.

«Хорошо» – если обучающийся полно освоил учебный материал, владеет понятийным аппаратом, ориентируется в изученном материале, осознанно применяет знания для решения практических задач, грамотно излагает ответ, но содержание и форма ответа имеют некоторые неточности.

«Удовлетворительно» – если обучающийся обнаруживает знание и понимание основных положений учебного материала, но излагает его неполно, непоследовательно, допускает неточности в определение понятий, в применении знаний для решения практических задач, не умеет доказательно обосновать свои суждения.

«Неудовлетворительно» – если обучающийся имеет разрозненные, бессистемные знания, не умеет выделять главное и второстепенное, допускает ошибки в определение понятий, искажает их смысл, беспорядочно и неуверенно излагает материал, не может применять знания для решения практических задач; за полное незнание и непонимание учебного материала или отказ отвечать.

.