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

УТВЕРЖДАЮ
Заместитель директора
по учебно-производственной работе
_____ О.В. Фомичева
«26» декабря 2023 г.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
по выполнению практических работ
по МДК.01.05 Эксплуатация компьютерных сетей
ПМ.01 ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ (ИНФОРМАЦИОННЫХ) СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

для специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Санкт-Петербург
2023 г.

Методические рекомендации рассмотрены на заседании методического совета СПб ГБПОУ «АУГСГиП»

Протокол № 2 от «29» ноября 2023 г.

Методические рекомендации одобрены на заседании цикловой комиссии общетехнических дисциплин и компьютерных технологий

Протокол № 4 от «21» ноября 2023 г.

Председатель цикловой комиссии: Караченцева М.С. _____

Разработчики: преподаватели СПб ГБПОУ «АУГСГиП»

С О Д Е Р Ж А Н И Е

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Рабочая тетрадь для выполнения практических работ предназначена для организации работы на практических занятиях по темам 5.1-5.5 МДК.01.05. «Эксплуатация компьютерных сетей» ПМ.01 «Эксплуатация автоматизированных (информационных) систем в защищённом исполнении» являющегося важной составной частью в системе подготовки специалистов среднего профессионального образования по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

Практические занятия являются неотъемлемым этапом изучения тем 5.1-5.5 МДК.01.05. «Эксплуатация компьютерных сетей» и проводятся с целью:

– формирования практических умений в соответствии с требованиями к уровню подготовки обучающихся, установленными рабочей программой учебной дисциплины;

– обобщения, систематизации, углубления, закрепления полученных теоретических знаний;

– готовности использовать теоретические знания на практике.

Практические занятия по темам 5.1-5.5 МДК.01.05. «Эксплуатация компьютерных сетей» способствуют формированию следующих общих и профессиональных компетенций:

- ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
- ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
- ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.
- ОК 09. Использовать информационные технологии в профессиональной деятельности.
- ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.
- ПК 1.2. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
- ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.

В Рабочей тетради предлагаются к выполнению практические работы, предусмотренные рабочей программой ПМ.01 «Эксплуатация автоматизированных (информационных) систем в защищённом исполнении».

При разработке содержания практических работ учитывался уровень сложности освоения студентами соответствующей темы, общих и профессиональных компетенций, на формирование которых направлен ПМ.01.

Выполнение практических работ в рамках тем 5.1-5.5 МДК.01.05. «Эксплуатация компьютерных сетей» ПМ.01 «Эксплуатация автоматизированных (информационных) систем в защищённом исполнении» позволяет освоить комплекс работ по настройке и диагностике сетевого оборудования, построению компьюетрных систем и обеспечению безопасности

Рабочая тетрадь для выполнения практических заданий по темам 5.1-5.5 МДК.01.05. «Эксплуатация компьютерных сетей» ПМ.01 «Эксплуатация автоматизированных (информационных) систем в защищённом исполнении» имеет практическую направленность и значимость. Формируемые в процессе их проведения умения могут быть использованы студентами в будущей профессиональной деятельности.

Рабочая тетрадь предназначена для студентов колледжа, изучающих темы 5.1-5.5 МДК.01.05. «Эксплуатация компьютерных сетей» ПМ.01 «Эксплуатация автоматизированных (информационных) систем в защищённом исполнении» и может использоваться как на учебных занятиях, которые проводятся под руководством преподавателя, так и для самостоятельного выполнения практических работ, предусмотренных рабочей программой во внеаудиторное время.

Практические занятия проводятся в учебном кабинете, не менее двух академических часов, обязательным этапом является самостоятельная деятельность студентов.

Практические занятия в соответствии с требованием ФГОС включают такой обязательный элемент, как использование персонального компьютера.

Оценки за выполнение практических работ выставляются по пятибалльной системе. Оценки за практические работы являются обязательными текущими оценками по темам 5.1-5.5 МДК.01.05. «Эксплуатация компьютерных сетей» ПМ.01 «Эксплуатация автоматизированных (информационных) систем в защищённом исполнении» и выставляются в журнале теоретического обучения.

1 ПЕРЕЧЕНЬ ПРАКТИЧЕСКИХ РАБОТ ПО ТЕМАМ 5.1-5.5 МДК.01.05. «ЭКСПЛУАТАЦИЯ КОМПЬЮТЕРНЫХ СЕТЕЙ» ПМ.01 «ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ (ИНФОРМАЦИОННЫХ) СИСТЕМ В ЗАЩИЩЁННОМ ИСПОЛНЕНИИ»

№ раздела, темы	Освоение умений в процессе занятия	Формируемые ОК и ПК	Тема практического занятия	Кол-во часов
Тема 5.1. Основы сетей передачи данных	применять на практике навыки монтажа кабельных сетей	ОК1-3, 9,10 ПК 1.2 ПК 1.4	**Практическое занятие №1**: Опрессовка кабеля.	2
	работать с сетевым оборудованием и сетевым программным обеспечением		**Практическое занятие №2:** Знакомство со средой моделирования	2
Тема 5.2. Статическая маршрутизация	работать с сетевым оборудованием и сетевым программным обеспечением	ОК1-3, 9,10 ПК 1.2 ПК 1.4	**Практическое занятие №3:** Настройка адресации и маршрутизации	2
			Практическое занятие №4: Настройка маршрутов между различными узлами сети. Документирование сети	2
	конфигурировать оборудование для организации статической маршрутизации в локальных компьютерных сетях	ОК1-3, 9,10 ПК 1.2 ПК 1.4	**Практическое занятие №5:** Настройка интерфейсов IPv4 и IPv6	2
			Практическое занятие №6: Исследование маршрутов с прямым подключением	2
			Практическое занятие №7: Настройка маршрутов IPv4. Настройка маршрутов IPv6.	2
			Практическое занятие №8: Настройка плавающих статических маршрутов. Поиск и устранение неполадок статических маршрутов	2
Тема 5.3. Сетевые информационные службы, сервисы и протоколы	производить настройки соединений на канальном уровне, создание и управление виртуальными локальными сетями. конфигурировать протоколы динамической маршрутизации в локальных компьютерных сетях	ОК1-3, 9,10 ПК 1.2 ПК 1.4	**Практическое занятие №9:** Настройка работы списка контроля доступа	2
			Практическое занятие №10: Настройка сетей VLAN. Построение компьютерной сети, разделенной на VLAN	2
			Практическое занятие №11: Настройка протокола	

№ раздела, темы	Освоение умений в процессе занятия	Формируемые ОК и ПК	Тема практического занятия	Кол-во часов
			SSH. Настройка протоколов Syslog и NTP	
			Практическое занятие №11: Настройка статического NAT	2
			Практическое занятие №12: Настройка протокола RIPv2. Настройка протокола DHCP	2
			Практическое занятие №12: Настройка динамического NAT	2
Тема 5.4. Локальные компьютерные сети	конфигурировать оборудование для организации статической маршрутизации в локальных компьютерных сетях	ОК1-3, 9,10 ПК 1.2 ПК 1.4	**Практическое занятие №15:** Создание топологии сети. Построение компьютерной сети	2
			Практическое занятие №16: Настройка маршрутизации сети. Настройка сетевых протоколов.	2
			Практическое занятие №17: Разбиение сети на подсети	2
Тема 5.5. Безопасность компьютерных сетей	проводить анализ безопасности оборудования в локальной сети	ОК1-3, 9,10 ПК 1.2 ПК 1.4	**Практическое занятие №18:** Анализ уязвимостей сайтов	2
			Практическое занятие №19: Анализ сетевого трафика. Использование Wireshark для анализа сеансов	2
			Практическое занятие №20: Аудит безопасности сетей. Обеспечение безопасности локальной сети	2

2 ОПИСАНИЕ ПОРЯДКА ВЫПОЛНЕНИЯ ПРАКТИЧЕСКИХ РАБОТ

2.1. Практическое занятие №1: Опрессовка кабеля и розеток. Опрессовка перекрестного кабеля (кроссовер)

Задание:

При монтаже локальных сетей сегодня наиболее распространена неэкранированная витая пара 5й категории (CAT-5E) – рис. 1.

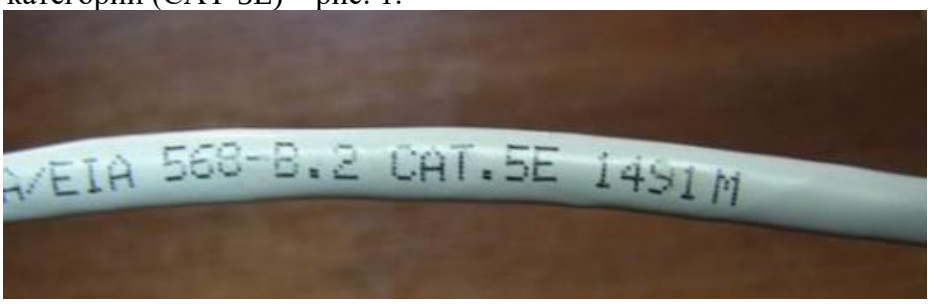


Рис. 1. Так выглядит кабель витая пара

Обжим такого кабеля для соединения ПК (PC)-ХАБ (HUB) по стандарту T568B изображен на рис. 2.

Рис. 2. Прямой обжим для соединения ПК-ХАБ (Одинаковый цвет проводников с обеих сторон кабеля)

Примечание

Обжим (опрессовка) по варианту T568A - стандарт, имеющий хождение в США и Канаде, а в России, в основном, применяется стандарт T568B.

Для обжима (опрессовки) витой пары вам потребуются пара коннекторов RJ-45и специальные клещи (кримпер) - рис 3-5.

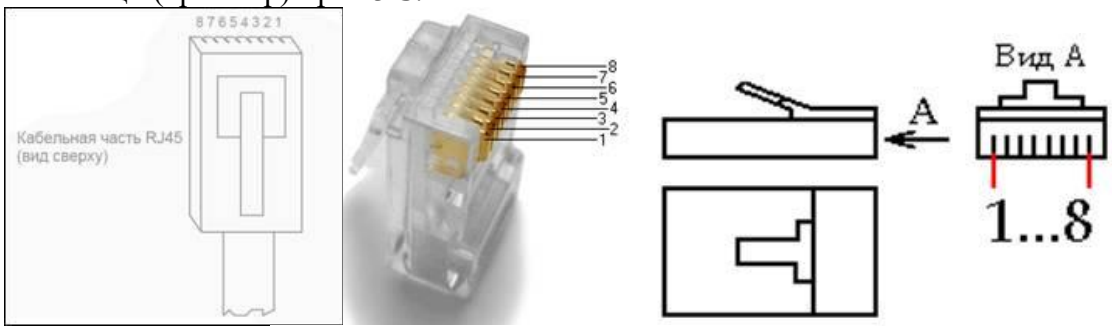


Рис. 3. Нумерация контактов разъема RJ-45

Рис. 4. Кримпер

Рис. 5. Коннектор вставлен в кримпер

Последовательность действий при обжиме:

1. Аккуратно обрежьте конец кабеля резаком, встроенным в обжимной инструмент.
2. Снимите с кабеля изоляцию ножом, встроенным в обжимной инструмент.
3. Разведите и расплетите проводки, выровняйте их в один ряд. Обкусите проводки так, чтобы их осталось чуть больше сантиметра (см. примечание).
4. Вставьте проводники в коннектор RJ-45. Убедитесь, все ли провода полностью вошли в разъем и уперлись в его переднюю стенку.
5. Вставьте коннектор в устройство для обжима коннектора.
6. Надавите на клещи так, чтобы контакты коннектора зажали проводники внутри него.

Примечание

На рис. 6 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. 6. Ошибки обжима кабеля

Контроль результата

Для проверки правильности обжима соедините кабелем сетевую карту и HUB (коммутатор, свич) и убедитесь в правильной работе такого кабеля. Другой вариант – использовать специальный тестер со светодиодной индикацией (рис. 7).

Рис. 7. Внешний вид тестера для проверки витых пар RJ-45 модели FA-7012B

В продаже представлено множество тестеров для проверки витых пар RJ-45 разного уровня сложности и ценового диапазона. Однако, принцип работы их аналогичен. Так, например, кабельный тестер FA-7012B состоит из 2 функциональных блоков - передатчика и приемника, которые подключаются к концам кабельной линии через разъемы RJ-45 или RJ-12. Он позволяет обнаружить оборванные пары, закороченные пары, перепутанные провода в одной паре, перепутанные пары и перепутанные провода между разными парами. Также прибор позволяет проверить целостность экрана кабеля. Блок-передатчик последовательно опрашивает состояние каждого провода в кабеле, а блок-приёмник возвращает ответ по неиспользуемой в конкретный момент паре. Последовательное загорание светодиодов сигнализирует о правильном соединении. Устройство питается от 1 батареи типа "Крона" 9 В.

Обжимаем розетку категории 5 под разъем RJ45

Стандартная схема подключения ПК к локальной или глобальной сети приведена на рис. 8.

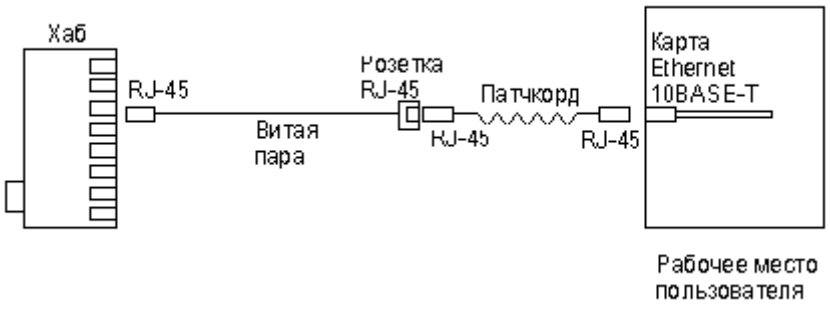


Рис. 8. Обычная схема подключения домашнего или офисного ПК к сети

Так же, как и сам кабель, витая пара, сетевые розетки различаются по категориям. В идеале, для профессионального монтажа вам понадобятся: розетка RJ-45 категории 5e для настенного монтажа, устройство для зачистки и обрезки витой пары, устройство для заделки витой пары, 4-парный кабель UTP, категория 5e и маркеры для нанесения обозначений на кабель (рис. 9).

Рис. 9. Набор для монтажа розетки (слева инструмент для снятия изоляции, сверху – для обрезки концов проводников)

Все контакты в розетках категории 5 пронумерованы, поэтому никаких проблем с разводкой кабеля возникнуть не должно.

Ситуация 1. Розетка с одним гнездом на 8 проводов

Для работы потребуется отвертка с плоским тонким жалом, по толщине, не превышающей диаметр медного проводника витой пары – рис.10. Также заталкивать провода в щели розетки можно ножом с тонким лезвием, например, канцелярским ножом, у которого лезвие выдвигается.

Рис. 10. Нумерация контактов в розетке с одним гнездом по стандарту T568B (для стандарта T568A цвета контактов розетки тоже обозначены)

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 (рис. 11).

Рис. 11. Особый вариант обжима кабеля

Понятно, что скорость информации при таком монтаже будет не 100, а 10 Мбит/сек.

Ситуация 2. Розетка на 2 гнезда по 8 проводов

Для надежной фиксации проводников в контактах розетки существует специальный инструмент, позволяющий поместить провод на максимальную глубину, хотя, можно обойтись обыкновенным пинцетом и отверткой. Провода перед вбиванием в клеммы зачищать не надо - щели оснащены специальной режущей кромкой, которая сама прекрасно снимает с них изоляцию. Заведите кабель на модуль розетки. Подготавливается для разделки кабель, снимается на длину не более 3 см его внешняя оболочка. Расплетаются пары на длину не более 13-15 мм. Закрепите кабель стяжкой на печатной плате розетки. Обрежьте конец стяжки с помощью кусачек или ножниц. На самой розетке всегда есть схема, какой цвет кабеля, в какой контакт должен приходить. На печатной плате наклеена табличка, на которой прорисованы в цветах варианты T568B и T568A разделки проводников витой пары в гребенки – рис. 12.

Рис. 12. Цветовая маркировка проводов розетки стандарта T568B это: 1 бело-ор, 2 ор, 3 бело-зел, 4 син, 5 бело-син 6 зел 7 бело кор, 8 кор (для варианта T568A цвета тоже нарисованы)

7. После выбора места установки розетки нужно ее закрепить на стене с помощью двух шурупов или приклеить двусторонним скотчем (обычно прилагаются в комплекте с розеткой). Для крепления шурупами нужно снять крышку и печатную плату, чтобы добраться до крепежных отверстий в основании розетки. Чтобы снять крышку, нужно двумя пальцами сдавить ее с боков в месте, близком к основанию и потянуть на себя. Защелки выйдут из зацепления, и крышка легко отойдет в сторону. Далее снимается печатная плата отведением в стороны четырех защелок по углам.
8. Результаты занести в отчет.

2.2. Практическая работа № 2 «Знакомство со средой моделирования»

Задание:

1. Запустите среду моделирования Cisco packet tracer. Ознакомьтесь с ещё интерфейсом.

2. Сконфигурируйте в среде моделирования сеть, представленную на рисунке 19. 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).

4. Используя командную строку задайте сетевым узлам:

а. Уникальные сетевые имена;

б. Приветственные приглашения, в которых будет указываться краткая информация о сетевом устройстве;

в. Пароли для прямого подключения к устройствам и режим их проверки;

г. Для устройств, соединяющих главный и дополнительный офисы задайте описания для соответствующих сетевых интерфейсов.

д. Переведите сетевые интерфейсы в состояния, соответствующие рисунку 19.

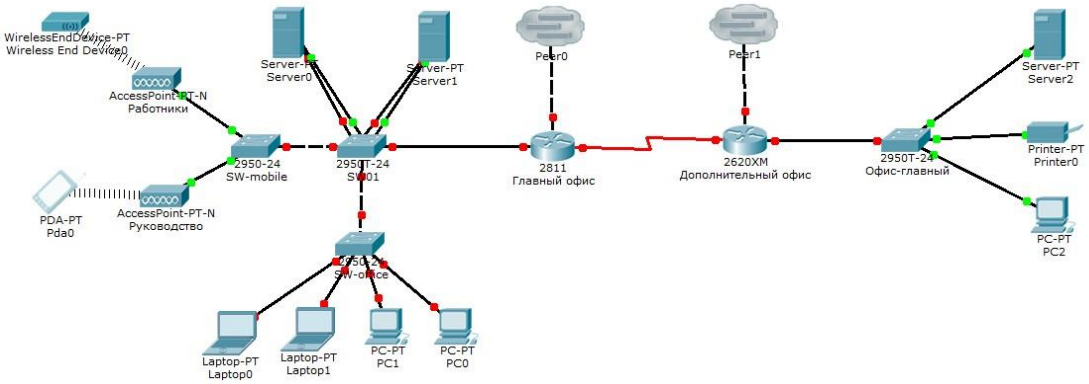


Рисунок 19 – Конфигурируемая сеть

2.3. Практическая работа № 3 «Настройка адресации маршрутизации»

Задание:

1. Измените конфигурацию сети, собранную в п.2 Практической работы № 5 (пример измененной сети представлен на рисунке 13):

a. В маршрутизатор головного офиса добавьте модуль, реализующий 16-ти портовый коммутатор (NM-ESW-161);

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

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);

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

c. Сеть маршрутизаторов (последовательные интерфейса) предприятия;

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

3. Сконфигурируйте ноутбуки, рабочие станции и серверы главного офиса согласно выбранной схеме подсетей. Убедитесь, что настройки верны (компьютеры имею связь друг с другом). Проверьте таблицы физических адресов на коммутаторах и маршрутизаторе офиса. Во всех ли таблицах одинаковые записи? Поясните результат.

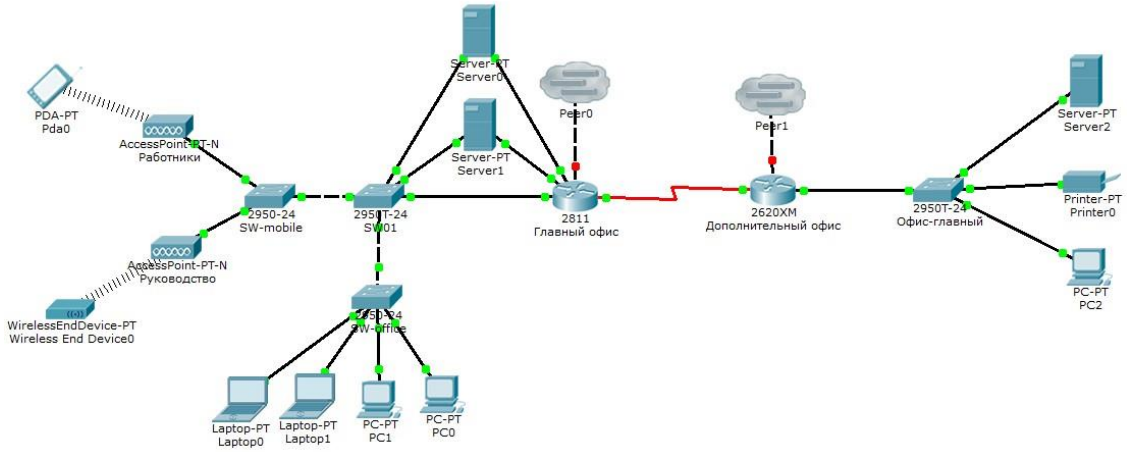


Рисунок 13 – Пример конфигурации модернизированной сети

2.4. Практическая работа № 4 «Настройка маршрутов между различными узлами сети. Документирование сети»

Задание 1:

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

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

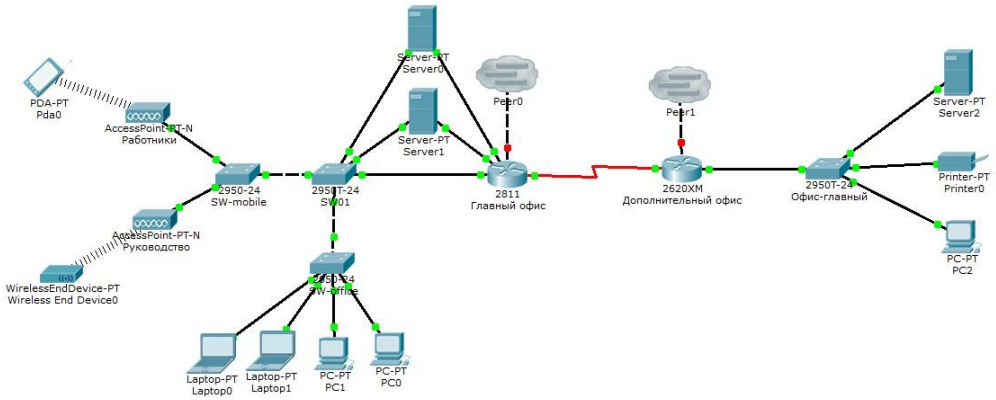


Рисунок 13 – Пример конфигурации модернизированной сети

Задание 2:

1. В этом задании необходимо задокументировать схему адресации и подключения, используемые в центральной области сети (Central). Для сбора необходимой информации необходимо использовать различные команды.

Примечание. Пароль пользовательского режима — cisco. Пароль привилегированного режима EXEC — class., как показано на рисунке 16.

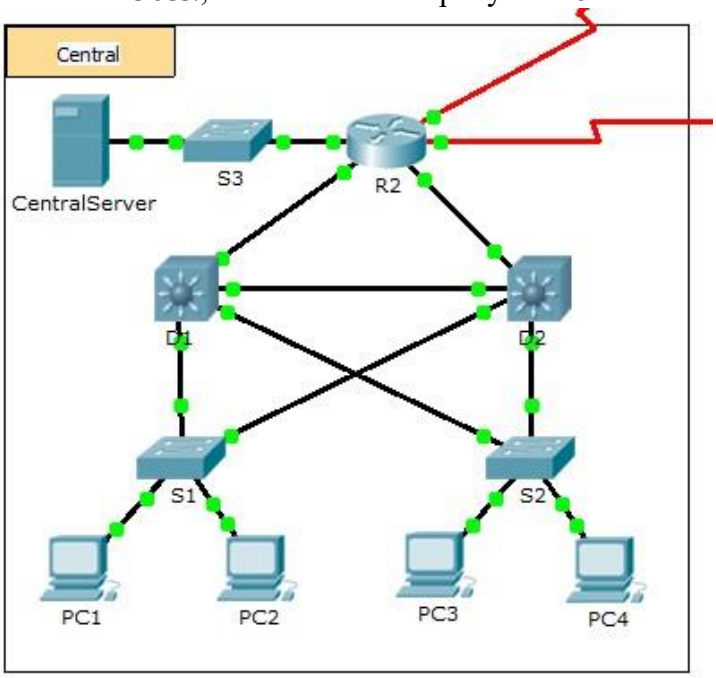


Рисунок 16 – Конфигурация модернизированной сети

2. Перейдите в режим командной строки на различных устройствах области Central.

3. Для сбора необходимой информации для таблицы «Документация схемы адресации и подключений устройств» используйте соответствующие команды.

4. Если вы не помните необходимые команды, можно использовать встроенную справочную систему IOS.

5. Если вам нужна дополнительная помощь, см. страницу Hints (Советы). В программе Packet Tracer нажмите правую стрелку (>) в правой нижней части окна инструкции. Если имеется отпечатанная версия инструкций, страница Советы — это последняя страница.

Таблица 1. Документация схемы адресации и подключений устройств

Имя устройства	Интерфейс	Адрес	Маска подсети	Устройства связи	
				Имя устройства	Интерфейс
R2	G0/0				
	G0/1				
	G0/2				
	S0/0/0	64.100.100.1	255.255.255.252	Internet	Н/Д (недоступно)

	S0/0/1.1	64.100.200.2	255.255.255.252	Intranet	Н/Д (недоступно)
S3	VLAN 1	10.10.10.254	255.255.255.0	—	—
	F0/1	—	—	CentralServer	Сетевой адаптер
	G0/1	—	—		
CentralServer	Сетевой адаптер				
D1	VLAN2	10.2.0.1	255.255.255.0	—	—
	G0/1				
	G0/2				
	F0/23	—	—		
	F0/24	—	—		
S1	VLAN 2	10.2.0.2	255.255.255.0	—	—
	F0/23	—	—		
	G0/1	—	—		
D2	F0/23	—	—	S1	F0/23
	F0/24				
	G0/1				
	G0/2				
S2	VLAN 1	10.3.0.2	255.255.255.0	—	—
	F0/23	—	—		
	G0/1	—	—		

Советы

Для сбора информации, необходимой для документирования сети, используйте следующие команды:

`show ip interface brief show interfaces show running-config ip-config`

2.5. Практическая работа № 5 Настройка интерфейсов IPv4 и IPv6

Задание:

Топология

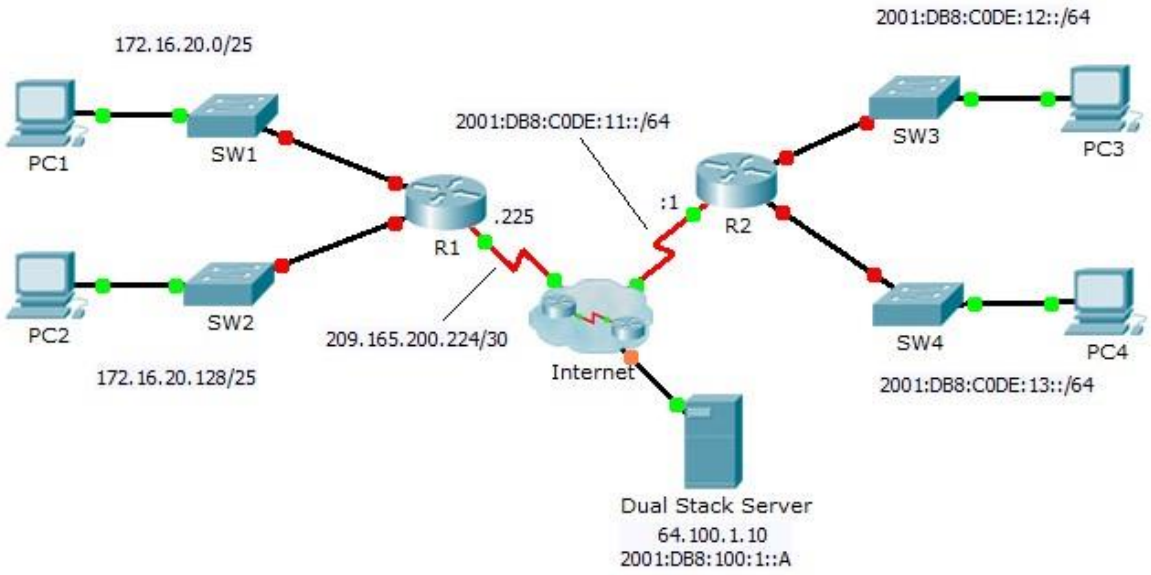


Таблица адресации

Устройство	Интерфейс	IPv4-адрес	Маска подсети	Шлюз по умолчанию
		IPv6-адрес/префикс		
R1	G0/0	172.16.20.1	255.255.255.128	—
	G0/1	172.16.20.129	255.255.255.128	—
	S0/0/0	209.165.200.225	255.255.255.252	—
PC1	NIC	172.16.20.10	255.255.255.128	172.16.20.1
PC2	NIC	172.16.20.138	255.255.255.128	172.16.20.129
R2	G0/0	2001:DB8:C0DE:12::1/64		—
	G0/1	2001:DB8:C0DE:13::1/64		—
	S0/0/1	2001:DB8:C0DE:11::1/64		—
	Link-local	FE80::2		—
PC3	NIC	2001:DB8:C0DE:12::A/64		FE80::2
PC4	NIC	2001:DB8:C0DE:13::A/64		FE80::2

К маршрутизаторам R1 и R2 подключено по две локальных сети. Ваша задача — настроить соответствующую адресацию на каждом устройстве и проверить подключение между локальными сетями.

Примечание. Пароль пользовательского режима — **cisco**. Пароль привилегированного режима EXEC — **class**.

Часть 1: Настройка адресации IPv4 и проверка подключения

Шаг 1: Назначьте IPv4-адреса маршрутизатору R1 и устройствам локальной сети.

Руководствуясь **Таблицей адресации**, настройте IP-адресацию для интерфейсов локальной сети маршрутизатора **R1**, а также для узлов **PC1** и **PC2**. Последовательный интерфейс уже настроен.

Шаг 2: Проверьте подключение.

Компьютеры **PC1** и **PC2** с помощью утилиты ping должны успешно проверять связь между собой и **сервером с двойным стеком**.

Часть 2: Настройка адресации IPv6 и проверка подключения

Шаг 1: Назначьте IPv6-адреса маршрутизатору R2 и устройствам локальной сети.

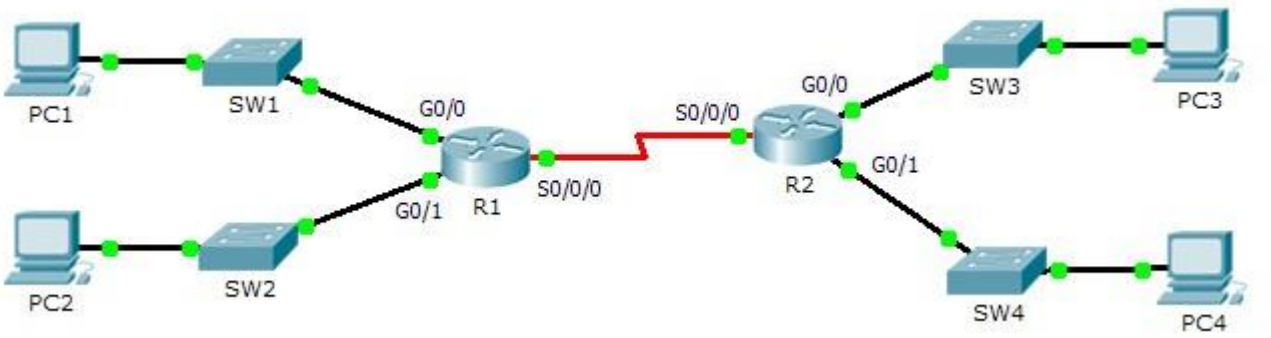
Руководствуясь **Таблицей адресации**, настройте IP-адресацию для интерфейсов локальной сети маршрутизатора **R2**, а также для узлов **PC3** и **PC4**. Последовательный интерфейс уже настроен.

Шаг 2: Проверьте подключение.

Компьютеры **PC3** и **PC4** с помощью утилиты ping должны успешно проверять связь между собой и **сервером с двойным стеком**.

2.6. Практическая работа №6 Исследование маршрутов с прямым подключением

Задание:



Часть 1: Исследование IPv4-маршрутов с прямым подключением

Шаг 1: Используйте команды show для сбора сведений об IPv4-сетях с прямым подключением.

На маршрутизаторе **R1** введите следующую команду:

R1> **show ip route ?**

Какой параметр будет наиболее полезным для определения сетей, назначенных интерфейсам этого маршрутизатора? _____

Какие сети на маршрутизаторе **R1** подключены напрямую? Совет. Используйте параметр, описанный выше.

_____
_____
_____

Какие IP-адреса назначены интерфейсам LAN на маршрутизаторе **R1**?

_____
_____
_____

Исследование маршрутов с прямым подключением

Какие сети на маршрутизаторе R2 подключены напрямую?

_____
_____
_____

Какие IP-адреса назначены интерфейсам LAN на маршрутизаторе **R2**?

_____

_____
_____

Шаг 2: Проверьте адресацию ПК и протестируйте подключение.

Откройте командную строку на **PC1**. Выполните команду для отображения настроек IP. Используя выходные данные, ответьте, сможет ли **PC1** установить подключение с другими интерфейсами маршрутизатора? Дайте короткий ответ с описанием своих предположений.

_____

Откройте командную строку на **PC2**. Выполните команду для отображения настроек IP. Используя выходные данные, ответьте, сможет ли **PC2** установить подключение с **PC1**? Проверьте свои предположения.

_____

Определите IP-адреса узлов **PC3** и **PC4**. Запишите результаты и определите, смогут ли **PC3** и **PC4** установить подключение друг с другом.

_____

Протестируйте подключение от **PC1** к **PC3**. Проверка прошла успешно? _____

Дополнительно. Принимая во внимание выходные данные таблиц маршрутизации на **R1** и **R2**, укажите возможную причину успешного или неудачного подключения между узлами **PC1** и **PC3**.

_____

Часть 2: Исследование IPv6-маршрутов с прямым подключением

Шаг 1: Используйте команды show для сбора сведений об IPv6-сетях с прямым подключением.

Какие сети IPv6 доступны на маршрутизаторе **R1**?

_____
_____
_____
_____
_____
_____

Какие индивидуальные IPv6-адреса назначены интерфейсам локальной сети на маршрутизаторе **R1**?

_____
_____
_____
_____

Исследование маршрутов с прямым подключением

Какие сети IPv6 доступны на маршрутизаторе R2?

_____
_____
_____
_____
_____
_____

Какие IPv6-адреса назначены интерфейсам локальной сети на маршрутизаторе **R2**?

_____
_____

Шаг 2: Проверьте настройки ПК и подключения.

Откройте командную строку на **PC1**. Выполните команду для отображения настроек IPv6. Используя выходные данные, ответьте, сможет ли **PC1** установить подключение с другими интерфейсами маршрутизатора? Дайте короткий ответ с описанием своих предположений.

_____
_____

Откройте командную строку на **PC2**. Выполните команду для отображения настроек IPv6.
Используя выходные данные, ответьте, сможет ли **PC2** установить подключение с **PC1**? Проверьте свои предположения. _____
Определите IPv6-адреса узлов **PC3** и **PC4**. Запишите результаты и определите, смогут ли **PC3** и **PC4** установить подключение друг с другом.

_____

Протестируйте подключение от **PC1** к **PC3**. Проверка прошла успешно? _____

Дополнительно. Принимая во внимание выходные данные таблиц маршрутизации IPv6 на R1 и R2, укажите возможную причину успешного или неудачного подключения между **PC1** и **PC3**.

_____
_____

2.7. Практическая работа № 7 Настройка маршрутов IPv4. Настройка маршрутов IPv6

Задание 1:

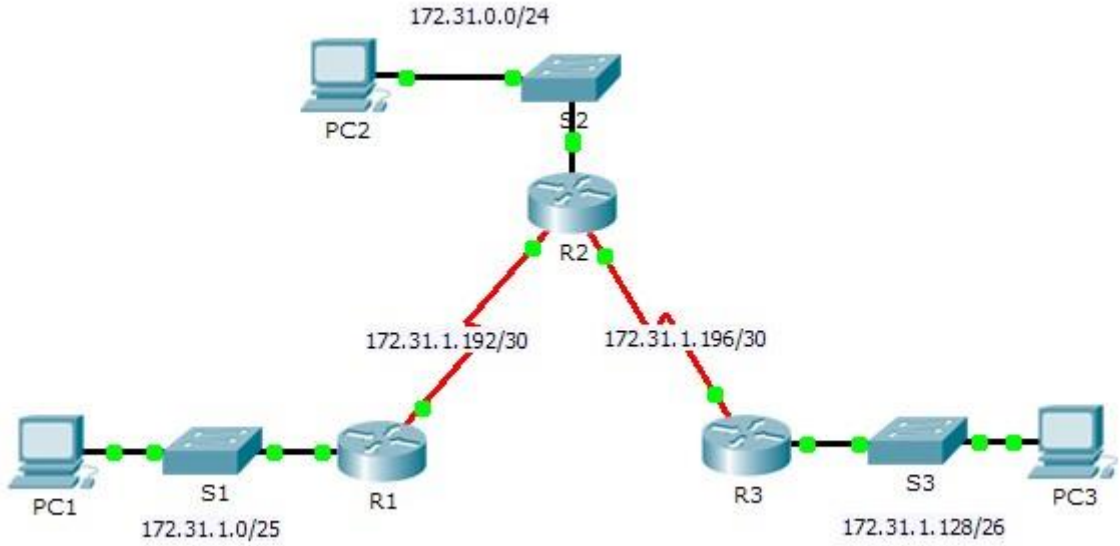


Таблица адресации

Устройство	Интерфейс	IPv4-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/0	172.31.1.1	255.255.255.128	—
	S0/0/0	172.31.1.194	255.255.255.252	—
R2	G0/0	172.31.0.1	255.255.255.0	—
	S0/0/0	172.31.1.193	255.255.255.252	—
	S0/0/1	172.31.1.197	255.255.255.252	—
R3	G0/0	172.31.1.129	255.255.255.192	—
	S0/0/1	172.31.1.198	255.255.255.252	—
PC1	NIC	172.31.1.126	255.255.255.128	172.31.1.1
PC2	NIC	172.31.0.254	255.255.255.0	172.31.0.1
PC3	NIC	172.31.1.190	255.255.255.192	172.31.1.129

В этом задании вам необходимо настроить статические маршруты и маршруты по умолчанию. Статический маршрут — это маршрут, который задается вручную администратором сети для создания надежного и безопасного маршрута. В данном задании используются четыре различных статических маршрута: рекурсивный статический маршрут, статический маршрут с прямым подключением, полностью заданный статический маршрут и маршрут по умолчанию.

Часть 1: Исследование сети и оценка необходимости статической маршрутизации
Используя схему топологии, ответьте, сколько всего имеется сетей? _____
Сколько сетей подключены напрямую к маршрутизаторам R1, R2 и R3? _____
Сколько статических маршрутов требуется каждому маршрутизатору, чтобы достичь сетей, не имеющих с ним прямого подключения?
_____
Проверьте подключение к сетям LAN маршрутизаторов R2 и R3, отправив эхо-запросы на PC2 и PC3 от PC1.
Почему возник сбой? _____
Часть 2: Настройка статических маршрутов и маршрутов по умолчанию
Шаг 1: Настройте рекурсивные статические маршруты на маршрутизаторе R1.
Что такое рекурсивный статический маршрут?
_____
_____
Почему для рекурсивного статического маршрута требуется два поиска в таблице маршрутизации?
_____
_____
Настройте рекурсивный статический маршрут для каждой сети без прямого подключения к маршрутизатору R1, включая канал WAN между R2 и R3.
Проверьте подключение к сети LAN маршрутизатора R2 и отправьте эхо-запросы на IP-адреса компьютеров PC2 и PC3.
Почему возник сбой?
_____
Шаг 2: Настройте на маршрутизаторе R2 статические маршруты с прямым подключением.
Чем отличается статический маршрут с прямым подключением от рекурсивного статического маршрута?
_____
_____
Настройте статический маршрут с прямым подключением от R2 ко всем сетям, не имеющим прямого подключения.
С помощью какой команды отображаются только сети с прямым подключением? _____
С помощью какой команды отображаются только статические маршруты, указанные в таблице маршрутизации? _____
Можете ли вы отличить статический маршрут с прямым подключением от сети с прямым подключением при просмотре таблицы маршрутизации?
_____
Шаг 3: Настройте маршрут по умолчанию для маршрутизатора R3.
Чем отличается маршрут по умолчанию от обычного статического маршрута?
_____
_____
_____
Настройте маршрут по умолчанию на маршрутизаторе R3 таким образом, чтобы была доступна каждая сеть без прямого подключения.
Как статический маршрут отображается в таблице маршрутизации? _____
Шаг 4: Запишите команды для полностью заданных маршрутов.

Примечание. В настоящее время Packet Tracer не поддерживает настройку полностью заданных статических маршрутов. Таким образом, на данном шаге необходимо задокументировать конфигурацию для полностью заданных маршрутов.
Объясните, что означает полностью заданный маршрут.

_____

_____

С помощью какой команды реализуется полностью заданный статический маршрут от R3 к LAN R2?

_____

Запишите полностью заданный маршрут от R3 к сети между маршрутизаторами R2 и R1. Настраивать маршрут не требуется, необходимо просто рассчитать его.

_____

Запишите полностью заданный статический маршрут от R3 к локальной сети R1. Настраивать маршрут не требуется, необходимо просто рассчитать его.

_____

Шаг 5: Проверьте настройки статических маршрутов.
Для проверки настроек используйте соответствующие команды **show**.
Какие команды **show** следует использовать для проверки правильности конфигурации статических маршрутов?

_____

Часть 3: Проверка подключения
Теперь каждое устройство должно успешно отправлять эхо-запрос на любое другое устройство. Если это не так, проверьте конфигурации статических маршрутов и маршрутов по умолчанию.

Задание 2:

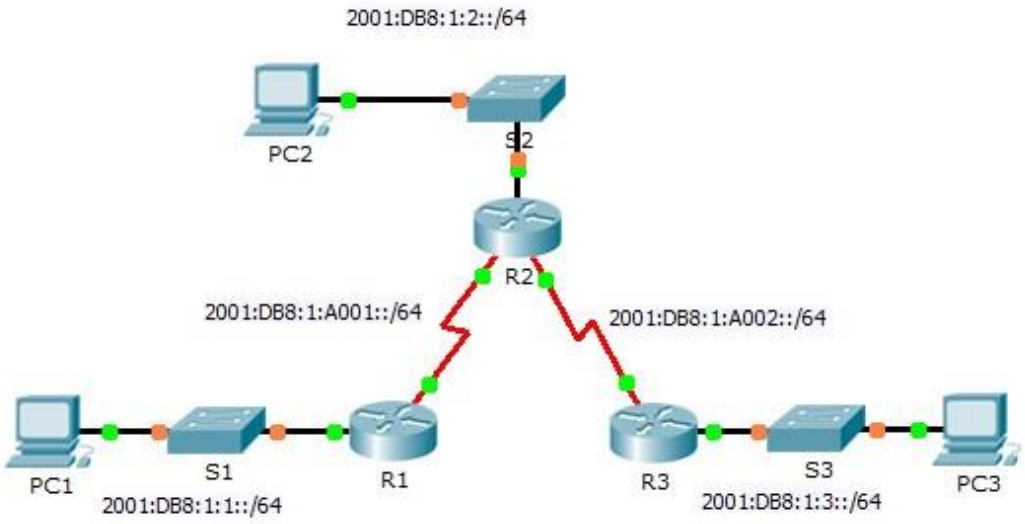


Таблица адресации IPv6

Устройство	Интерфейс	IPv6-адрес/префикс	Шлюз по умолчанию
R1	G0/0	2001:DB8:1:1::1/64	—
	S0/0/0	2001:DB8:1:A001::1/64	—
R2	G0/0	2001:DB8:1:2::1/64	—

	S0/0/0	2001:DB8:1:A001::2/64	—
	S0/0/1	2001:DB8:1:A002::1/64	—
R3	G0/0	2001:DB8:1:3::1/64	—
	S0/0/1	2001:DB8:1:A002::2/64	—
PC1	NIC	2001:DB8:1:1::F/64	FE80::1
PC2	NIC	2001:DB8:1:2::F/64	FE80::2
PC3	NIC	2001:DB8:1:3::F/64	FE80::3

Общие сведения

В этом задании вам необходимо настроить статические маршруты и маршруты по умолчанию для IPv6. Статический маршрут — это маршрут, который задается вручную администратором сети для создания надежного и безопасного маршрута. В данном задании используются четыре различных статических маршрута: рекурсивный статический маршрут, статический маршрут с прямым подключением, полностью заданный статический маршрут и маршрут по умолчанию.

Часть 1: Исследование сети и оценка необходимости статической маршрутизации

Используя схему топологии, ответьте, сколько всего имеется сетей? _____

Сколько сетей подключены напрямую к маршрутизаторам R1, R2 и R3? _____

Сколько статических маршрутов требуется каждому маршрутизатору, чтобы достичь сетей, не имеющих с ним прямого подключения?

_____

_____

Какая команда используется для настройки статических маршрутов IPv6?

_____

Часть 2: Настройка статических IPv6-маршрутов и маршрутов IPv6 по умолчанию

Шаг 1: Включите IPv6-маршрутизацию на всех маршрутизаторах.

Перед настройкой статических маршрутов необходимо сначала настроить маршрутизатор для пересылки пакетов IPv6.

С помощью какой команды выполняется данная операция? _____ Выполните эту команду на каждом маршрутизаторе.

Шаг 2: Настройте рекурсивные статические маршруты на маршрутизаторе R1.

Настройте рекурсивный маршрут IPv6 для каждой сети, не имеющей прямого подключения к маршрутизатору R1.

Шаг 3: На маршрутизаторе R2 настройте прямое подключение и полностью заданный статический маршрут.

Настройте статический маршрут с прямым подключением между R2 и локальной сетью R1.

Настройте полностью заданный маршрут между R2 и LAN R3.

Примечание. Программа Packet Tracer v6.0.1 позволяет проверять только маршруты с прямым подключением и рекурсивные статические маршруты. Инструктор может попросить проверить вашу конфигурацию полностью заданного статического маршрута IPv6.

Шаг 4: Настройте маршрут по умолчанию для маршрутизатора R3.

Настройте рекурсивный маршрут по умолчанию на маршрутизаторе R3, чтобы получить доступ ко всем сетям, не имеющим прямого подключения.

Packet Tracer. Настройка статических маршрутов IPv6 и маршрутов IPv6 по умолчанию

Шаг 5: Проверьте настройки статических маршрутов.

С помощью какой команды командной строки Packet Tracer выполняется проверка конфигурации IPv6 на компьютере?

_____

С помощью какой команды отображаются IPv6-адреса, настроенные на интерфейсе маршрутизатора?

_____

С помощью какой команды отображается содержимое таблицы IPv6-маршрутизации

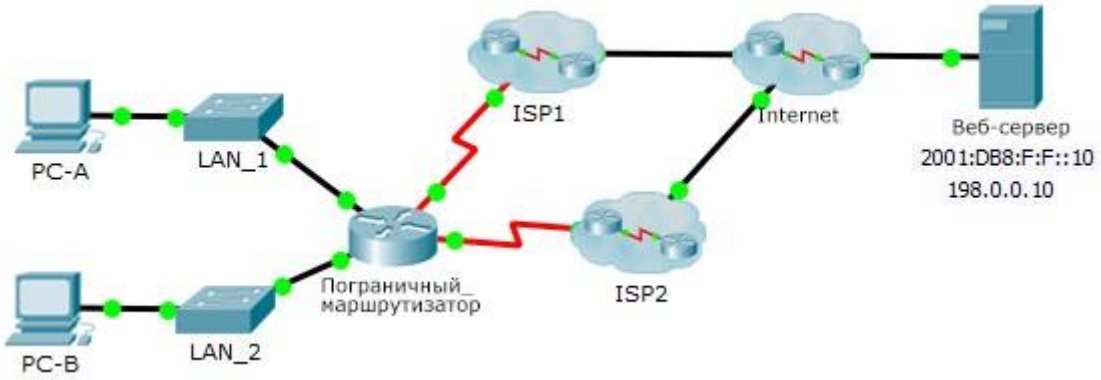
_____

Часть 3: Проверка подключения

Теперь каждое устройство должно успешно отправлять эхо-запрос на любое другое устройство. Если это не так, проверьте конфигурации статических маршрутов и маршрутов по умолчанию.

2.8 Практическая работа № 8 Настройка плавающих статических маршрутов. Поиск и устранение неполадок статических маршрутов

Задание 1:



Общие сведения

В этом задании необходимо настроить плавающие статические маршруты IPv4 и IPv6. Эти маршруты настраиваются вручную так, чтобы значение административного расстояния превышало аналогичное значение для основного маршрута, поэтому данный маршрут не добавляется в таблицу маршрутизации до тех пор, пока не произойдет сбой основного маршрута. Необходимо будет проверить переключение при отказе на резервные маршруты, а затем восстановить подключение к основному маршруту.

Часть 1: Настройка плавающего статического маршрута IPv4

Шаг 1: Настройте статический маршрут IPv4 по умолчанию.

a. Настройте напрямую подключенный статический маршрут по умолчанию от **Edge_Router** (Пограничный_маршрутизатор) к Интернету. Основной маршрут по умолчанию должен проходить через **ISP1**.

b. Отобразите содержимое таблицы маршрутизации. Убедитесь в том, что маршрут по умолчанию виден в таблице маршрутизации.

c. Какая команда используется для трассировки пути от компьютера к узлу назначения?

_____

От узла **PC-A** выполните трассировку маршрута к **веб-серверу**. Маршрут должен начинаться от шлюза по умолчанию 192.168.10.1 и проходить через адрес 10.10.10.1. В противном случае проверьте настройки статического маршрута по умолчанию.

Шаг 2: Настройте плавающий статический маршрут IPv4.

a. Какое значение административной дистанции имеет статический маршрут?

_____

b. Настройте плавающий статический маршрут по умолчанию с прямым подключением, административное расстояние которого равно 5. Маршрут должен иметь направление к **ISP2**.

c. Просмотрите текущую конфигурацию и убедитесь, что в этой конфигурации содержится плавающий статический маршрут IPv4 по умолчанию, а также статический маршрут IPv4 по умолчанию.

d. Отобразите содержимое таблицы маршрутизации. Содержится ли плавающий статический маршрут IPv4 в таблице маршрутизации? Поясните ответ

_____
_____
_____

Часть 2: Проверка переключения при отказе на плавающий статический маршрут IPv4

a. На устройстве **Пограничный_маршрутизатор (Edge_Router**) от имени администратора отключите выходной интерфейс основного маршрута.

b. Убедитесь, что плавающий статический маршрут IPv4 теперь содержится в таблице маршрутизации.

c. Выполните трассировку маршрута от **PC-A** к **веб-серверу**.

Был ли выполнен переход на резервный маршрут? Если нет, подождите несколько секунд для завершения сходимости и проверьте еще раз. Если резервный маршрут по-прежнему не работает, проверьте конфигурацию плавающего статического маршрута.

d. Восстановите подключение к основному маршруту.

e. Выполните трассировку маршрута от **PC-A** к **веб-серверу**, чтобы убедиться в успешном восстановлении основного маршрута.

Часть 3: Настройка и проверка переключения при отказе на плавающий статический маршрут IPv6

Шаг 1: Настройте плавающий статический маршрут IPv6.

a. Статический маршрут IPv6 по умолчанию до **ISP1** уже настроен. Настройте плавающий статический маршрут IPv6 по умолчанию, административное расстояние которого равно 5. Маршрут должен вести к IPv6-адресу **ISP2** (**2001:DB8:A:2::1**).

b. Просмотрите текущую конфигурацию и убедитесь, что плавающий статический маршрут IPv6 по умолчанию теперь указан в списке ниже статического маршрута IPv6 по умолчанию.

Шаг 2: Проверка переключения при отказе на плавающий статический маршрут IPv6

a. На устройстве **Пограничный_маршрутизатор (Edge_Router)** от имени администратора отключите выходной интерфейс основного маршрута.

b. Убедитесь, что плавающий статический маршрут IPv6 теперь содержится в таблице маршрутизации.

c. Выполните трассировку маршрута от **PC-A** к **веб-серверу**.

Был ли выполнен переход на резервный маршрут? Если нет, подождите несколько секунд для завершения сходимости и проверьте еще раз. Если резервный маршрут по-прежнему не работает, проверьте конфигурацию плавающего статического маршрута.

d. Восстановите подключение к основному маршруту.

e. Выполните трассировку маршрута от **PC-A** к **веб-серверу**, чтобы убедиться в успешном восстановлении основного маршрута.

Задание 2:

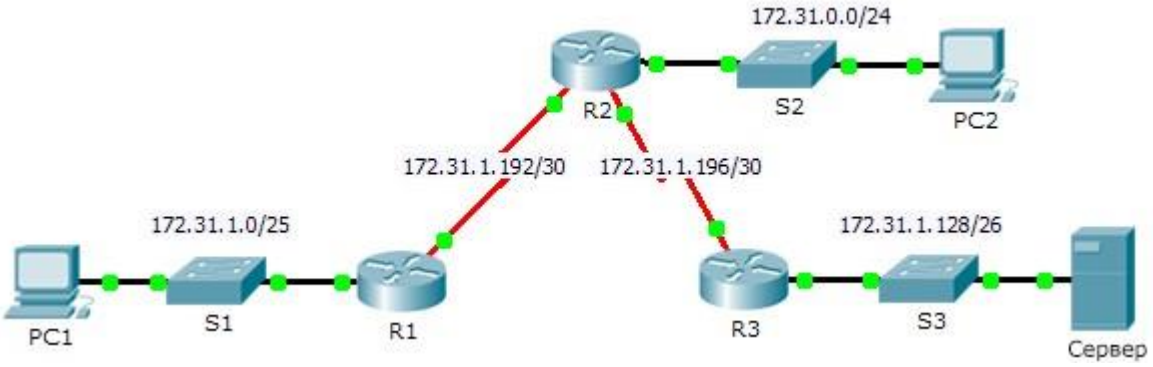


Таблица адресации

Устройство	Интерфейс	IPv4-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/0	172.31.1.1	255.255.255.128	—
	S0/0/0	172.31.1.194	255.255.255.252	—
R2	G0/0	172.31.0.1	255.255.255.0	—
	S0/0/0	172.31.1.193	255.255.255.252	—
	S0/0/1	172.31.1.197	255.255.255.252	—
R3	G0/0	172.31.1.129	255.255.255.192	—
	S0/0/1	172.31.1.198	255.255.255.252	—
PC1	NIC	172.31.1.126	255.255.255.128	172.31.1.1
PC2	NIC	172.31.0.254	255.255.255.0	172.31.0.1

Сервер	NIC	172.31.1.190	255.255.255.192	172.31.1.129

Общие сведения

В этом задании компьютер PC1 сообщает о невозможности доступа к ресурсам сервера. Найдите неполадку, выберите подходящее решение и устраните проблему.

Часть 1: Выявление неполадки

У PC1 нет доступа к файлам на сервере. Выявите неполадку, используя соответствующие команды **show** на всех маршрутизаторах, и выполните на компьютерах все необходимые команды для устранения неполадок, которые вы узнали из предыдущих глав.

Назовите несколько команд поиска и устранения неполадок на маршрутизаторах и компьютерах, которые можно использовать для выявления причин неполадки.

_____

Часть 2: Выбор решения

После выявления неполадки, не позволяющей PC1 получить доступ к файлам сервера, заполните таблицу, приведенную ниже.

Проблема	**Решение**

Часть 3: Реализация решения

a. Если обнаружены статические маршруты с неправильными настройками, их следует удалить перед добавлением в конфигурацию корректно настроенных маршрутов.

b. Добавьте любые недостающие маршруты, настроив маршруты с прямым подключением.

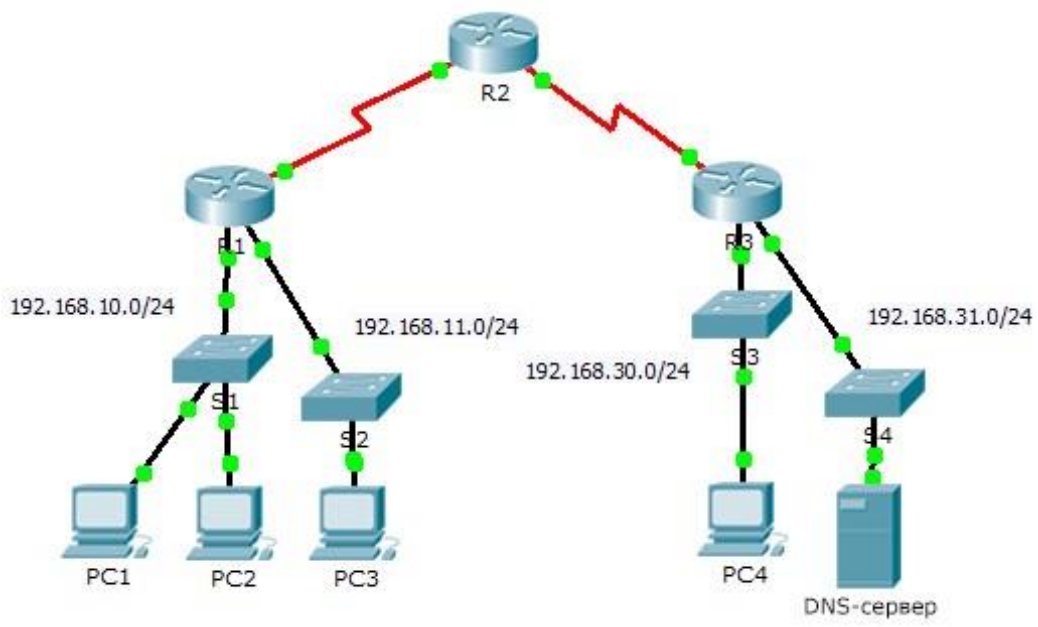
Часть 4: Проверка успешного устранения неполадки

a. Отправьте эхо-запрос из PC1 на сервер.

Откройте веб-соединение с сервером. После выявления и реализации правильного решения по устранению неполадки при подключении к серверу в веб-обозревателе появится сообщение.

2.9 Практическая работа № 9 Настройка работы списка контроля доступа

Задание:



Общие сведения

В рамках этого задания вы получите представление о том, как можно использовать список контроля доступа (ACL) для запрещения эхо-запросов, отправленных на узлы удаленных сетей. После удаления ACL-списка из конфигурации эхо-запросы будут успешными.

Часть 1: Проверка локального подключения и тестирование списка контроля доступа

Шаг 1: Отправьте эхо-запросы по локальной сети, чтобы проверить подключение.

a. Из командной строки узла **PC1** отправьте эхо-запрос на **PC2**.

b. Из командной строки узла **PC1** отправьте эхо-запрос на **PC3**.

Почему ping-запросы прошли успешно?

_____

Шаг 2: Отправьте эхо-запросы в удаленные сети, чтобы протестировать работу ACLсписка.

a. Из командной строки узла **PC1** отправьте эхо-запрос на **PC4**.

b. Из командной строки узла **PC1** отправьте эхо-запрос на **DNS-сервер**.

Почему возникает сбой при отправке ping-запросов? (Подсказка. Для анализа используйте режим моделирования или просмотрите конфигурации маршрутизатора.)

_____

Часть 2: Удаление ACL-списка и повторное тестирование

Шаг 1: Используйте команды show, чтобы проверить конфигурацию ACL-списка.

a. Используйте команды **show run** и **show access-lists**, чтобы просмотреть текущие ACL-списки. Для быстрого просмотра текущих ACL-списков используйте команду **show access-lists**. Введите команду **show access-lists**, после которой

нажмите ПРОБЕЛ и поставьте вопросительный знак (?), чтобы просмотреть доступные параметры:

R1#**show access-lists ?**

<1-199> ACL number

Имя ACL-списка СЛОВО

<cr>

Если вы знаете номер или имя ACL-списка, вы можете дополнительно отфильтровать выходные данные команды **show**. Однако на маршрутизаторе **R1** применен только один ACL-список, поэтому будет достаточно команды **show access-lists**.
R1#**show access-lists**

Standard IP access list 11

10 deny 192.168.10.0 0.0.0.255

20 permit any

Первая строка списка контроля доступа запрещает все пакеты из сети **192.168.10.0/24**, в том числе эхо-запросы по протоколу ICMP (ping-запросы). Вторая строка списка контроля доступа разрешает прохождение через маршрутизатор всего остального трафика по протоколу IP (**ip)** от любого источника (**any**) источника.

b. Чтобы список контроля доступа влиял на работу маршрутизатора, он должен быть применен к интерфейсу в определенном направлении. В этом сценарии список контроля доступа используется для фильтрации исходящего трафика на интерфейсе. Поэтому весь трафик, покидающий указанный интерфейс на маршрутизаторе R1, будет проверяться на соответствие списку ACL 11.

Несмотря на возможность просмотра сведений об IP с помощью команды **show ip interface**, в некоторых случаях эффективнее использовать команду **show run**.
С помощью обеих или одной из этих команд определите, к какому интерфейсу и в каком направлении применяется список контроля доступа?

_____

Шаг 2: Удаление списка доступа 11 из конфигурации

ACL-списки можно удалить из конфигурации, применив команду **no access list** [*номер ACL-списка*].
Команда **no access-list** удаляет все списки контроля доступа, настроенные на маршрутизаторе.
Команда **no access-list** [*номер ACL-списка*] удаляет только указанный список контроля доступа.

a. Для интерфейса Serial0/0/0 удалите список контроля доступа 11, который был применен к интерфейсу в качестве **исходящего** фильтра:

R1(config)# **int se0/0/0**

R1(config-if)#**no ip access-group 11 out**

b. В режиме глобальной конфигурации удалите ACL-список, применив следующую команду:

R1(config)# **no access-list 11**

Убедитесь, что теперь ping-запросы с компьютера **PC1** успешно достигают **DNS-сервера** и **PC4**.

2.10 Практическая работа № 10 Настройка сетей VLAN. Построение компьютерной сети, разделенной на VLAN

Задание 1:

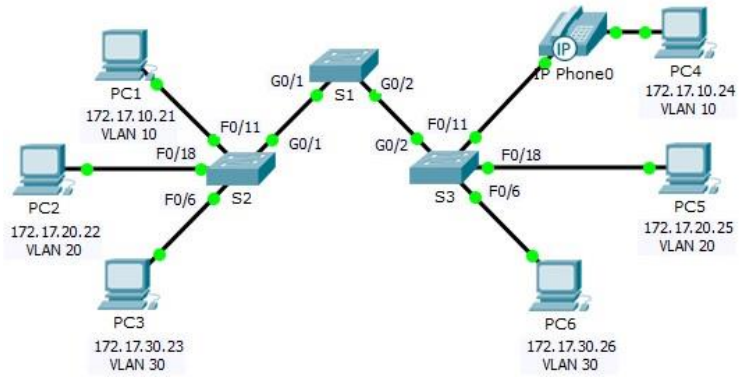


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	VLAN
PC1	NIC	172.17.10.21	255.255.255.0	10
PC2	NIC	172.17.20.22	255.255.255.0	20
PC3	NIC	172.17.30.23	255.255.255.0	30
PC4	NIC	172.17.10.24	255.255.255.0	10
PC5	NIC	172.17.20.25	255.255.255.0	20
PC6	NIC	172.17.30.26	255.255.255.0	30

Общие сведения

Сети VLAN удобны в администрировании логических групп, поскольку позволяют легко перемещать, изменять или добавлять участников группы. Главная цель этого задания — создать сети VLAN, присвоить им имена и назначить порты доступа конкретным сетям VLAN.

Часть 1: Проверка конфигурации VLAN, установленной по умолчанию

Шаг 1: Отобразите текущие сети VLAN.

На коммутаторе S1 выполните команду, с помощью которой отображаются все настроенные сети VLAN. По умолчанию все интерфейсы назначены сети VLAN 1.

Шаг 2: Проверьте подключение между компьютерами в одной и той же сети.

Обратите внимание, что с каждого компьютера можно отправлять эхо-запрос на другой компьютер, подключенный к той же сети.

- Проверка связи с помощью утилиты ping компьютера PC1 с PC4 выполняется успешно.
- Узел PC2 может получить ответ на ping-запрос узлу PC5.
- Узел PC3 может получить ответ на ping-запрос узлу PC6.

Эхо-запросы к узлам из других сетей выполнены неудачно.
Какое преимущество для текущей конфигурации обеспечивает настройка сетей VLAN?

_____

_____

_____

Часть 2: Настройка сетей VLAN

Шаг 1: Создайте сети VLAN на коммутаторе S1 и присвойте им имена.

Создайте следующие сети VLAN. Имена чувствительны к регистру.

- VLAN 10: Faculty/Staff
- VLAN 20: Students
- VLAN 30: Guest (по умолчанию)
- VLAN 99: Management&Native
- VLAN 150: VOICE

Шаг 2: Проверьте конфигурацию сети VLAN.

С помощью какой команды отображается только имя сети VLAN, состояние сети и связанные с ней порты коммутатора?

_____

Шаг 3: Создайте сети VLAN на коммутаторах S2 и S3.

С помощью тех же команд, что и в шаге 1, создайте такие же сети VLAN и присвойте им имена на коммутаторах S2 и S3.

Шаг 4: Проверьте конфигурацию сети VLAN.

Часть 3: Назначение сетей VLAN портам

Шаг 1: Назначьте сети VLAN активным портам на коммутаторе S2.

Настройте интерфейсы в качестве портов доступа и назначьте сети VLAN следующим образом.

- VLAN 10: FastEthernet 0/11
- VLAN 20: FastEthernet 0/18
- VLAN 30: FastEthernet 0/6

Шаг 2: Назначьте сети VLAN активным портам на коммутаторе S3.

На коммутаторе S3 используются те же назначения портов доступа к сети VLAN, что и на коммутаторе S2. Настройте интерфейсы в качестве портов доступа и назначьте сети VLAN следующим образом.

- VLAN 10: FastEthernet 0/11
- VLAN 20: FastEthernet 0/18
- VLAN 30: FastEthernet 0/6

Шаг 3: Назначьте сеть VOICE VLAN интерфейсу FastEthernet 0/11 на коммутаторе S3.

Как показано в топологии, интерфейс FastEthernet 0/11 коммутатора S3 подключен к IP-телефону Cisco и компьютеру PC4. IP-телефон содержит встроенный 3-портовый коммутатор 10/100. Один порт на телефоне имеет обозначение Switch (Коммутатор) и подключается к интерфейсу F0/4. Другой порт на телефоне обозначен PC (ПК) и подключается к компьютеру PC4. IP-телефон также имеет внутренний порт, который подключается к функциям IP-телефона.
Интерфейс F0/11 на коммутаторе S3 должен быть настроен для поддержки пользовательского трафика, направленного к компьютеру PC4, с использованием сети VLAN 10 и трафика голосовых данных, направленного на IP-телефон, с использованием сети VLAN 150. На интерфейсе также необходимо включить QoS и поддержку значений класса обслуживания (CoS), назначенных IPтелефоном.

Шаг 4: Проверьте подключение.

Ранее PC, находящиеся в одной общей сети, могли успешно отправлять эхо-запросы друг другу.
Попытайтесь отправить эхо-запросы между компьютерами PC1 и PC4. Успешно ли выполняются эхозапросы при назначении портов доступа в соответствующие сети VLAN? Почему?

_____

_____

_____

Что можно сделать для разрешения этой проблемы?

_____

_____

_____

Задание 2:

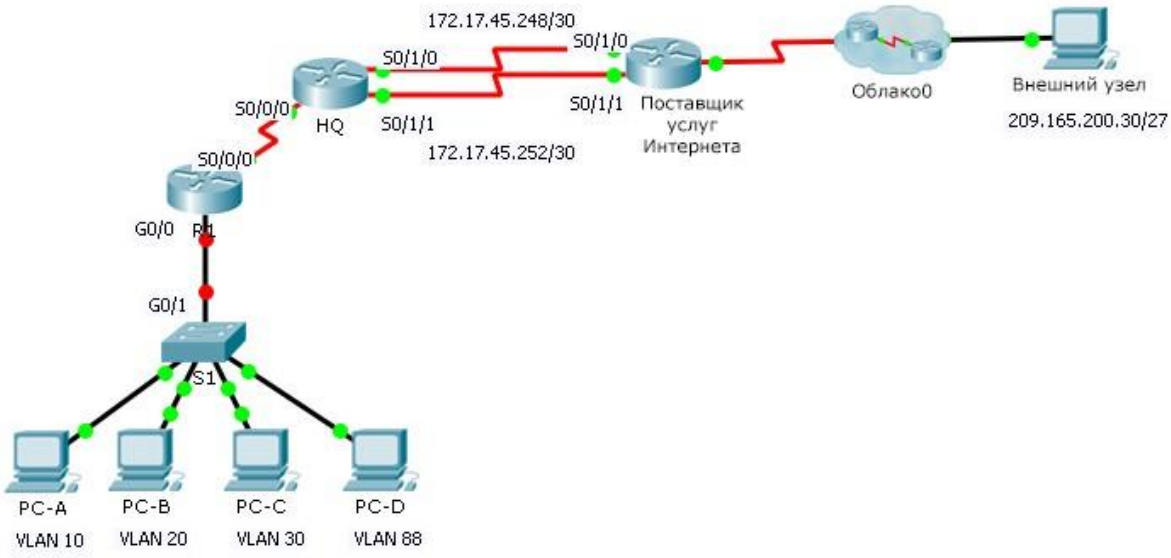


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию	VLAN
R1	S0/0/0	172.31.1.2	255.255.255.0	—	—
	G0/0,10	172.31.10.1	255.255.255.0	—	10
	G0/0,20	172.31.20.1	255.255.255.0	—	В данном примере — 20.
	G0/0,30	172.31.30.1	255.255.255.0	—	30
	G0/0,88	172.31.88.1	255.255.255.0	—	88
	G0/0,99	172.31.99.1	255.255.255.0	—	99
S1	VLAN 88	172.31.88.33	255.255.255.0	172.31.88.1	88
PC-A	NIC	172.31.10.21	255.255.255.0	172.31.10.1	10
PC-B	NIC	172.31.20.22	255.255.255.0	172.31.20.1	В данном примере — 20.
PC-C	NIC	172.31.30.23	255.255.255.0	172.31.30.1	30
PC-D	NIC	172.31.88.24	255.255.255.0	172.31.88.1	88

Таблица VLAN

VLAN	Имя	Интерфейсы
10	Отдел продаж	F0/11-15
В данном примере — 20.	Производство	F0/16-20
30	Marketing	F0/5-10
88	Управление	F0/21-24
99	Собственная	G0/1

Сценарий

В этом задании вам предстоит продемонстрировать и закрепить свои навыки настройки маршрутов для связи между сетями VLAN, а также потребуется выполнить настройку статических маршрутов для обеспечения доступа к узлам назначения за пределами вашей сети. Вы также продемонстрируете умение настраивать маршрутизацию между VLAN, статические маршруты и маршруты по умолчанию.

- Настройте маршрутизацию между VLAN на **R1** в соответствии с **Таблицей адресации**.

- Настройте транковый канал на коммутаторе **S1**.
- На маршрутизаторе **HQ** настройте четыре статических маршрута с прямым подключением к каждой сети VLAN: 10, 20, 30 и 88.
- На маршрутизаторе **HQ** настройте статические маршруты с прямым подключением к **внешнему узлу (Outside Host)**.
  - Настройте основной путь через последовательный интерфейс 0/1/0.
  - Настройте резервный маршрут через последовательный интерфейс 0/1/1 с административной дистанцией, равной 10.
- На маршрутизаторе **R1** настройте маршрут по умолчанию с прямым подключением.
- Проверьте подключение, убедившись, что все ПК могут отправлять эхо-запросы на **внешний узел (Outside Host)**.

2.11 Практическая работа № 11 Настройка протокола SSH. Настройка протоколов Syslog и NTP

Задание 1:

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети
S1	VLAN 1	10.10.10.2	255.255.255.0
PC1	NIC	10.10.10.10	255.255.255.0

Общие сведения

Для безопасного управления удаленными подключениями Cisco рекомендует заменить протокол Telnet протоколом SSH. В Telnet используется открытый незашифрованный текстовый обмен. Протокол SSH обеспечивает безопасность удаленных соединений, предоставляя надежное шифрование всех данных, передаваемых между устройствами. В этом упражнении необходимо обеспечить безопасность удаленного коммутатора с использованием зашифрованного пароля и протокола SSH.

Часть 1: Безопасные пароли

a. С помощью командной строки на узле **PC1**, подключитесь к коммутатору **S1** через Telnet. Пароль для пользовательского и привилегированного доступа — **cisco**.

b. Сохраните текущую конфигурацию, чтобы любые допущенные вами ошибки можно было отменить, отключив питание коммутатора **S1**.

c. Отобразите текущую конфигурацию и обратите внимание на то, что пароли написаны в виде открытого текста. Введите команду, которая шифрует текстовые пароли.

_____

d. Убедитесь, что пароли зашифрованы.

Часть 2: Обеспечение защищенной коммуникации

Шаг 1: Настройте имя домена IP и создайте ключи шифрования.

В принципе, использование Telnet небезопасно, поскольку текстовые данные передаются в незашифрованном виде. Поэтому рекомендуется по возможности использовать протокол SSH.

a. Присвойте домену имя **netacad.pka.**

_____

b. Для шифрования данных требуются ключи шифрования. Создайте RSA ключи длиной 1024 бит.

_____

Шаг 2: Создайте пользователя SSH и перенастройте линии VTY на доступ только по протоколу SSH.

a. Создайте пользователя **administrator** с секретным паролем **cisco**.

_____

b. Настройте линии VTY для проверки регистрационных данных на основе локальной базы данных имен пользователей, а также для разрешения удаленного доступа только по протоколу SSH. Удалите существующий пароль линии VTY.

_____

_____

_____

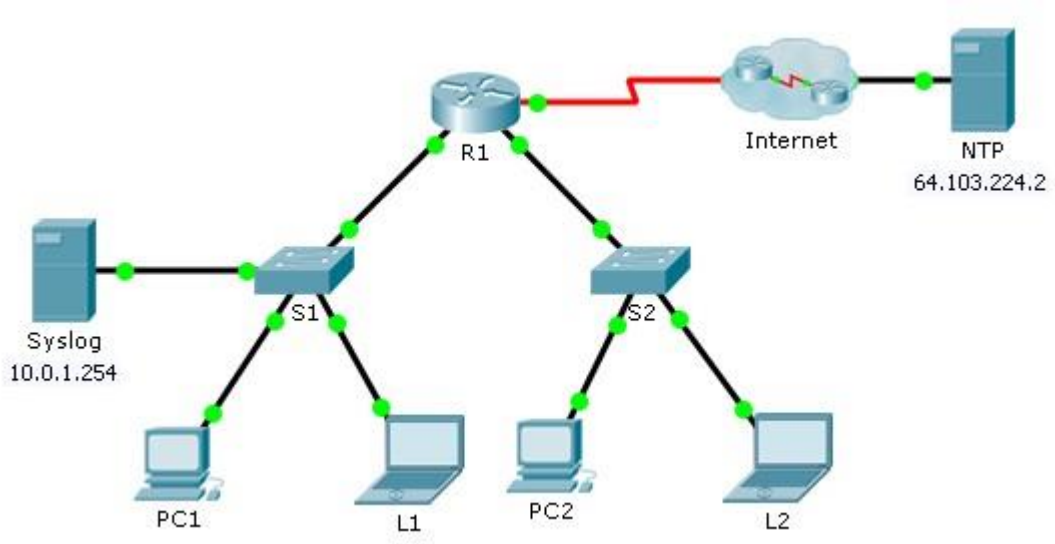
Часть 3: Проверка реализации протокола SSH

a. Завершите сеанс Telnet и попробуйте заново войти в систему, используя Telnet. Попытка должна завершиться неудачей.

b. Попробуйте войти в систему через протокол SSH. Введите **ssh** и нажмите **ВВОД**, не добавляя какие-либо параметры, чтобы отобразить инструкции использования команды. Указание. Параметр **-l** — это буква «L», а не цифра 1.

c. После успешного входа перейдите в режим привилегированного доступа EXEC и сохраните конфигурацию. Если вам не удалось получить доступ к коммутатору **S1**, отключите питание и повторите шаги, описанные в части 1.

Задание 2:



Сценарий

В этом упражнении необходимо включить и использовать Syslog и NTP, чтобы сетевой администратор мог более эффективно вести мониторинг сети.

Часть 1: Настройка службы Syslog

Шаг 1: Включите службу Syslog.

a. Щелкните **Syslog** и выберите вкладку **Services** (Сервисы).

b. Включите **Syslog** и разместите окно таким образом, чтобы вести мониторинг активности.

Шаг 2: Настройте промежуточные устройства для использования службы Syslog.

a. Настройте маршрутизатор **R1** для отправки событий журнала на сервер **Syslog**.

```
R1(config)# logging 10.0.1.254
```

b. Настройте коммутатор **S1** для отправки событий журнала на сервер **Syslog**.

c. Настройте коммутатор **S2** для отправки событий журнала на сервер **Syslog**.

Часть 2: Создание регистрируемых событий

Шаг 1: Измените состояние интерфейсов для создания записей журнала событий.

a. Настройте интерфейс Loopback 0 маршрутизатора **R1**, а затем выключите его.

b. Выключите компьютеры **ПК 1** и **ПК 2**. Включите их снова.

Шаг 2: Изучите события системного журнала Syslog.

a. Посмотрите события системного журнала Syslog. **Примечание.** Все события были записаны, но метки времени оказались неправильными.

b. Перед переходом к следующей части очистите журнал.

Часть 3: Настройка часов на коммутаторе вручную

Шаг 1: Вручную настройте часы на коммутаторах.

Вручную настройте часы на коммутаторах **S1** и **S2**, установив текущую дату и примерное время.

Пример.

```
S1# clock set 11:47:00 July 10 2013
```

Шаг 2: Включите службу меток времени для журналирования на коммутаторах.

Настройте коммутаторы **S1** и **S2** для отправки соответствующих меток времени вместе с записями событий, передаваемыми на сервер **Syslog**.

```
S1(config)# service timestamps log datetime msec
```

Часть 4: Настройка службы NTP

Шаг 1: Включите службу NTP.

В этом задании предположим, что служба NTP находится на общедоступном интернет-сервере. Аутентификация может использоваться в случае использования частного сервера NTP.

c. Откройте вкладку **Services** (Сервисы) сервера **NTP**.

d. Включите службу NTP и запишите отображаемые дату и время.

Шаг 2: Автоматически настройте время на маршрутизаторе.

Установите на часах маршрутизатора **R1** дату и время согласно серверу NTP.

```
R1(config)# ntp server 64.103.224.2
```

Шаг 3: Включите службу меток времени для журналирования на маршрутизаторе.

Настройте маршрутизатор **R1** для отправки соответствующих меток времени вместе с записями событий, передаваемыми на сервер **Syslog**.

Часть 5: Проверка записей с метками времени

Шаг 1: Измените состояние интерфейсов для создания записей журнала событий.

a. Снова включите, а затем выключите интерфейс Loopback 0 маршрутизатора R1.

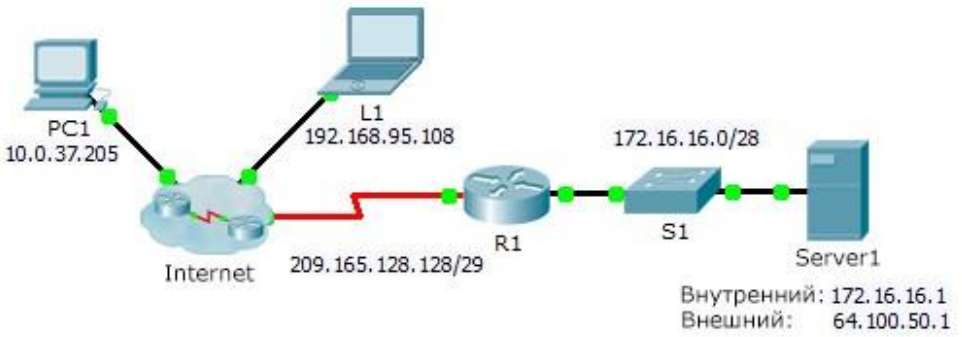
b. Выключите ноутбуки **L1** и **L2**. Включите их снова.

Шаг 2: Изучите события системного журнала Syslog.

Посмотрите события системного журнала Syslog. **Примечание**. Все события были записаны, и метки времени соответствуют настройкам. **Примечание**. Маршрутизатор **R1** использует настройки времени, полученные с сервера NTP, а коммутаторы **S1** и **S2** используют настройки времени, определенные вами в части 3.

2.12 *Практическая работа № 17 Настройка статического NAT*

Задание:



Сценарий

В сетях, настроенных по протоколу IPv4, для клиентов и серверов используется частная адресация. Перед выходом из сети в Интернет пакеты с частной адресацией должны быть преобразованы в пакеты с публичной адресацией. Серверам, доступным извне сети компании, обычно назначают как публичный, так и частный статические IP-адреса. В рамках задания необходимо настроить статический NAT таким образом, чтобы внешние устройства могли получать доступ к внутреннему серверу по публичному адресу.

Часть 1: Проверка доступа без использования NAT

Шаг 1: Попытайтесь подключиться к серверу Сервер 1 в режиме симуляции.

a. С **ПК 1** или **L1** попытайтесь подключиться к веб-странице сервера **Сервер 1** по адресу 172.16.16.1. Используйте веб-браузер для входа на **Сервер 1** 172.16.16.1. Попытки должны завершиться неудачей.

b. С **ПК 1** отправьте эхо-запрос на интерфейс S0/0/0 маршрутизатора **R1**. Выполнение команды ping должно быть успешным.

Шаг 2: Просмотрите таблицы маршрутизации и текущую настройку маршрутизатора R1.

a. Просмотрите текущую конфигурацию маршрутизатора **R1**. Обратите внимание на отсутствие команд, относящихся к NAT.

b. Убедитесь, что в таблице маршрутизации нет записей, ссылающихся на IP-адреса, используемые **ПК 1** и **L1**.

c. Убедитесь, что NAT не используется маршрутизатором **R1**.

R1# **show ip nat translations**

Часть 2: Настройка статического NAT

Шаг 1: Настройка команд статического NAT.

См. топологию. Создайте статическое преобразование NAT для сопоставления внутреннего адреса **Сервер 1** его внешнему адресу.

Шаг 2: Настройте интерфейсы.

Правильно настройте внутренний и внешний интерфейсы.

Часть 3: Проверка доступа с использованием NAT

Шаг 1: Проверьте связь с веб-страницей сервера Сервер 1.

a. Откройте командную строку на **ПК 1** или **L1**, попытайтесь отправить эхо-запрос, используя публичный адрес сервера **Сервер 1**. Эхо-запросы должны быть успешными.

b. Убедитесь, что и **ПК 1**, и **L1** теперь могут осуществить доступ к веб-странице сервера **Сервер 1**.

Шаг 2: Просмотрите преобразования NAT.

Для проверки настройки статического преобразования NAT используйте следующие команды:

show running-config

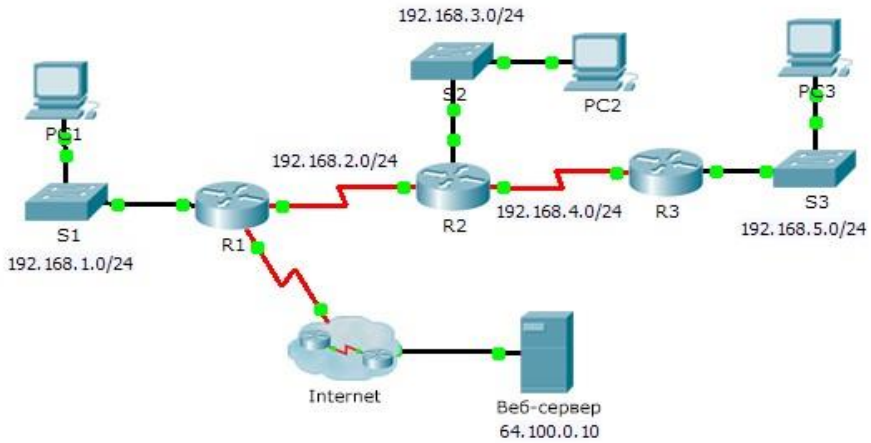
show ip nat transla-

tions show ip nat

statistics

2.13 Практическая работа № 13 Настройка протокола RIPv2. Настройка протокола DHCP

Задание 1:



Общие сведения

Несмотря на то, что RIP редко используется в современных сетях, он может послужить основой для понимания принципов маршрутизации сети. В этом задании необходимо настроить маршрут по умолчанию (на базе протокола RIP версии 2) с соответствующими выражениями network и пассивными интерфейсами, а также проверить наличие полного подключения.

Часть 1: Настройка RIPv2

Шаг 1: Настройте протокол RIPv2 на маршрутизаторе R1.

a. Используйте соответствующую команду, чтобы создать на маршрутизаторе **R1** маршрут по умолчанию, по которому весь интернет-трафик покинет сеть через интерфейс S0/0/1.

b. Войдите в режим настройки протокола RIP.

c. Используйте версию 2 протокола RIP, отключите объединение сетей.

d. Настройте протокол RIP для сетей, которые подключены к маршрутизатору **R1**.

e. Настройте порт LAN таким образом, чтобы он не отправлял маршрутизирующую информацию в виде анонсов маршрутов.

f. Объявите маршрут по умолчанию, настроенный на шаге 1a для других маршрутизаторов RIP. g. Сохраните конфигурацию.

Шаг 2: Настройте протокол RIPv2 на маршрутизаторе R2.

a. Войдите в режим настройки протокола RIP.

b. Используйте версию 2 протокола RIP, отключите объединение сетей.

c. Настройте протокол RIP для сетей с прямым подключением к маршрутизатору **R2**.

d. Настройте интерфейс, к которому не подключены маршрутизаторы таким образом, чтобы через него не отправлялась никакая информация маршрутизации.

e. Сохраните конфигурацию.

Шаг 3: Настройте протокол RIPv2 на маршрутизаторе R3

Повторите действия шага 2 на маршрутизаторе **R3**.

Часть 2: Проверка конфигураций

Шаг 1: Просмотрите таблицы маршрутизации на маршрутизаторах R1, R2 и R3.

a. Используйте соответствующие команды, чтобы посмотреть таблицу маршрутизации **R1**. Теперь RIP (R) появляется в таблице маршрутизации вместе с подключёнными (C) и локальными (L) маршрутами. Для каждой сети существует запись. В списке также отображается маршрут по умолчанию.

b. Просмотрите таблицы маршрутизации на маршрутизаторах **R2** и **R3**. Обратите внимание, что у каждого маршрутизатора есть полный список всех сетей 192.168.x.0 и маршрут по умолчанию.

Шаг 2: Убедитесь в наличии полного подключения ко всем местам назначения.

Теперь каждое устройство должно успешно отправлять эхо-запрос на любое другой устройство внутри сети. Кроме того, все устройства должны успешно отправлять эхо-запросы на **веб-сервер**.

Задание 2:

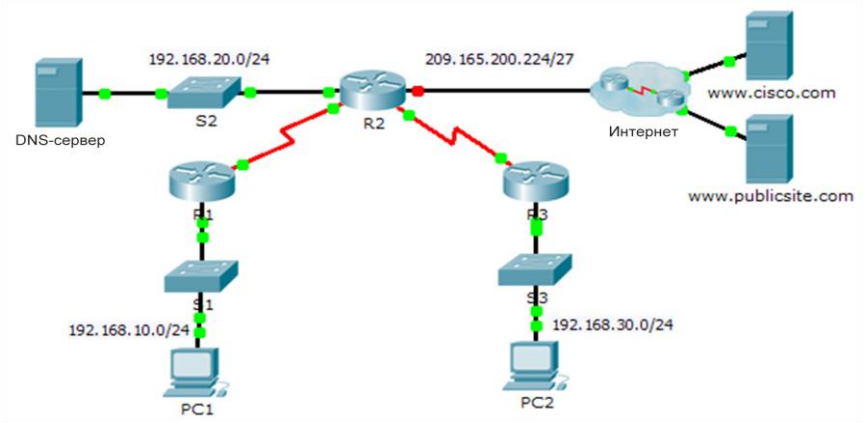


Таблица адресации

Устройство	Интерфейс	IPv4-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/0	192.168.10.1	255.255.255.0	—
	S0/0/0	10.1.1.1	255.255.255.252	—
R2	G0/0	192.168.20.1	255.255.255.0	—
	G0/1	Назначенный DHCP	Назначенный DHCP	—
	S0/0/0	10.1.1.2	255.255.255.252	—
	S0/0/1	10.2.2.2	255.255.255.252	—
R3	G0/0	192.168.30.1	255.255.255.0	—
	S0/0/1	10.2.2.1	255.255.255.0	—
PC1	NIC	Назначенный DHCP	Назначенный DHCP	Назначенный DHCP
PC2	NIC	Назначенный DHCP	Назначенный DHCP	Назначенный DHCP
DNS Server	NIC	192.168.20.254	255.255.255.0	192.168.20.1

Сценарий

Выделенный сервер DHCP хорошо масштабируется и им относительно легко управлять, однако использование подобного сервера в каждой точке сети может оказаться слишком затратным. Вместе с тем маршрутизатор Cisco можно настроить для обеспечения DHCP-служб без необходимости в выделенном сервере. Как специалисту по обслуживанию сетей, вам необходимо настроить маршрутизатор Cisco в качестве сервера DHCP, чтобы обеспечить динамическое распределение адресов для клиентов внутри сети. Также необходимо настроить пограничный маршрутизатор в качестве

DHCP-клиента таким образом, чтобы он получал IP-адрес от сети Интернет-провайдера.

Часть 1: Настройка маршрутизатора в роли DHCP-сервера

Шаг 1: Исключите зарезервированные IPv4-адреса из пула DHCP.

Настройте маршрутизатор **R2** таким образом, чтобы исключить первые 10 адресов из локальных сетей маршрутизаторов R1 и R3. Все другие адреса должны быть доступны в пуле адресов DHCP.

Шаг 2: На маршрутизаторе R2 создайте пул DHCP для локальной сети маршрутизатора R1.

a. Создайте пул DHCP под названием **R1-LAN** (с учетом регистра).

b. Настройте пул DHCP с учетом сетевого адреса, шлюза по умолчанию и IP-адреса сервера DNS.

Шаг 3: На маршрутизаторе R2 создайте пул DHCP для локальной сети маршрутизатора R3.

a. Создайте пул DHCP под названием **R3-LAN** (с чувствительным регистром).

b. Настройте пул DHCP с учетом сетевого адреса, шлюза по умолчанию и IP-адреса сервера DNS.

Часть 2: Настройка DHCP-ретрансляции

Шаг 1: Настройте маршрутизаторы R1 и R3 в качестве агентов-ретрансляторов.

Шаг 2: Настройте узлы PC1 и PC2 таким образом, чтобы они получали IP-адреса через DHCP.

Часть 3: Настройте коммутатор S2 в качестве клиента DHCP.

a. Настройте интерфейс Gigabit Ethernet 0/1 на маршрутизаторе R2 для получения информации об IP-адресации через DHCP и включения интерфейса.

Примечание. В программе Packet Tracer используйте функцию **Fast Forward Time** (Ускорить время), чтобы ускорить процесс, или подождите, пока между маршрутизаторами R2 и ISP установятся отношения смежности EIGRP.

b. Используйте команду **show ip interface brief**, чтобы убедиться, что маршрутизатор R2 получил IPадрес от DHCP-сервера.

Часть 4: Проверка DHCP и связности

Шаг 1: Проверьте ассоциации MAC- и IP-адресов в DHCP.

R2# **show ip dhcp binding**

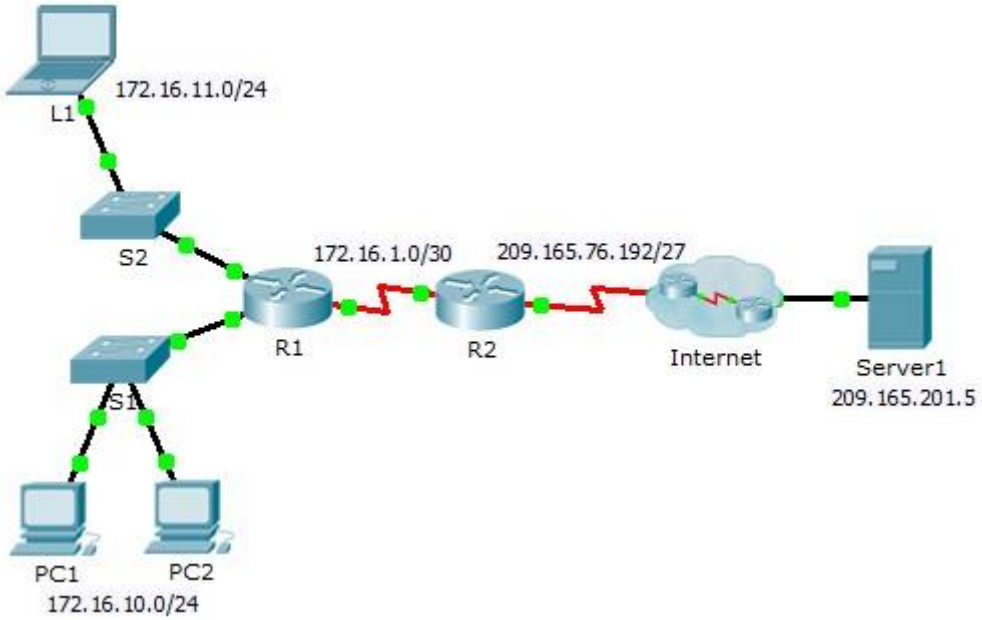
IP address	Client-ID/ Hardware address	Lease expiration	Type
192.168.10.11	0002.4AA5.1470	--	Automatic
192.168.30.11	0004.9A97.2535	--	Automatic

Шаг 2: Проверьте конфигурации.

Убедитесь в том, что **PC1** и **PC2** теперь могут отправлять эхо-запросы друг другу и другим устройствам.

2.14 Практическая работа № 14. Настройка динамического NAT

Задание:



Часть 1: Настройка динамического NAT

Шаг 1: Настройте трафик, который будет разрешен.

На маршрутизаторе **R2** настройте одно правило для ACL-списка 1, разрешающее любой адрес, принадлежащий подсети 172.16.0.0/16.

Шаг 2: Настройте пул адресов для NAT.

Настройте **R2**, определяя пул NAT, использующий все четыре адреса из адресного пространства 209.165.76.196/30.

Обратите внимание, что в топологии имеется 3 сетевых диапазона, которые должны преобразовываться согласно созданному ACL-списку. Что произойдёт, если более 2 устройств попытаются осуществить доступ к Интернету?

_____

_____

Шаг 3: Соотнесите ACL-список 1 и пул NAT.

Шаг 4: Настройте интерфейсы NAT.

Настройте интерфейсы маршрутизатора **R2** с помощью соответствующих внутренних и внешних команд NAT.

Часть 2: Проверьте реализацию NAT

Шаг 1: Осуществите доступ к сервисам через Интернет.

Из веб-браузера узла **L1**, **ПК 1** или **ПК 2** осуществите доступ к веб-странице сервера **Сервер 1**.

Шаг 2: Просмотрите преобразования NAT.

Просмотрите преобразования NAT на маршрутизаторе **R2**.

R2# **show ip nat translations**

2.15 Практическая работа №15. Создание топологии сети. Построение компьютерной сети

Задание 1: создайте топологию сети, согласно заданным требованиям.

Требования:

1. Не менее 3 офисов, связанных общим интернетом. (центрального, рабочего и домашнего)
2. Наличие хотя бы одного сервера
3. Не менее 3 коммутаторов
4. Не менее 5 ПК
5. Не менее 2 периферийных устройств
6. Наличие подключений мобильных устройств

Ответ:

Задание 2: постройте сеть по топологии, созданной в Практической работе №21.
В Cisco Packet Tracer постройте сети по созданной топологии. Добавьте все устройства, продумайте логическую топологию.
Заполните таблицу:

Устройство	Название устройства	Интерфейсы	Офис

Ответ:

2.16 Практическая работа №16. Настройка маршрутизации сети. Настройка сетевых протоколов.

Задание 1: постройте таблицу маршрутизации для устройств и их интерфейсов из таблицы, созданной в Практической работе №22.

Заполните таблицу маршрутизации:

Устройство	Интерфейс	**IPv4-адрес** Маска подсети	Шлюз по умолчанию

В Cisco Packet Tracer проставьте IP-адреса всем устройствам по созданной таблице.
Ответ:

Задание 2: настройте сетевые параметры устройств построенной сети.

- Необходимо использовать протоколы: RIPv2, SSH, Syslog и NTP.
- Настроить DHCP в рабочем офисе.

- Настроить NAT

Ответ:

2.17 Практическая работа №17. Разбиение сети на подсети

Задание: разбить сеть на подсети

- Добавить в сеть рабочего офиса 10 компьютеров: 3 рабочих, 3 для студента, 1 для администратора, 3 для гостей.
- Разбить сеть рабочего офиса на подсети для новых добавленных компьютеров.
- Обеспечить подключение к каждой подсети с получением IP по DHCP.

Ответ:

2.18 Практическая работа № 16 Анализ уязвимостей сайтов

Задание:

Краткие теоретические сведения
Одним из первых этапов анализа защищенности любой компьютерной системы является сбор информации. В зависимости от используемой методологии анализа защищенности вебприложения могут применяться различные методы и средства сбора информации. Стоит отметить, что сбор информации, как правило, не характерен для методологии инструментального анализа защищенности (сканирования), а характерен для методологии тестирования на возможность проникновения.
Методы сбора информации делятся на активные и пассивные. Активные методы требуют непосредственного взаимодействия с исследуемым приложением путем отправки ему запросов и анализа соответствующих ответов, а пассивные методы используют информацию, отправляемую сервером веб-приложения его клиентам (например, HTTP-заголовки X-Frame-Options, Strict-TransportSecurity и т.д.) без отправки запросов. При анализе вебприложений, как правило, используются только активные методы.
Активные методы делятся на методы с подключением к приложению (например, идентификация веб-сервера с помощью сканера Httprint) и методы без подключения (например, сбор информации о приложении поисковыми роботами, сканерами Интернет, и т.д.).
В результате проведения сбора информации о веб-приложении могут быть получены:

- имена и IP-адреса сетевых узлов, на которых размещены вебприложение и его компоненты;
- логины и пароли технологических учетных записей;
- комментарии разработчиков;
- данные о системном и прикладном ПО, применяемых средствах защиты и конфигурации веб-приложения;
- адреса электронной почты разработчиков приложения; исходный код серверной части веб-приложения; конфиденциальные файлы.

Программными средствами получения необходимой информации являются:

- поисковые системы (например, Google, Shodan, Bing);
- специализированные сканеры уязвимостей Интернет (например, http://un1c0rn.net/);

- инструментальные средства анализа защищенности сетей общего назначения (Nmap, Xprobe2, XSpider);
- инструментальные средства анализа защищенности сетей вебприложений (AppScan, Acunetix, Burp Suite, ZAP, W3AF и т.д.).

Постановка задачи

Выполнить сбор информации об анализируемом вебприложении `www.test.app.com`.

Последовательность действий

Будем рассматривать сбор информации на примере вебприложения с условным именем `www.test.app.com`.

Шаг 1. В адресной строке браузера перейти по адресу `www.test.app.com/robots.txt`. Проанализировать содержимое файла. Сделать выводы о наличии «скрытых» директорий.

Шаг 2. В адресной строке браузера перейти по адресу `http://www.test.app.com/crossdomain.xml` и, затем, по адресу `http://www.test.app.com/clientaccesspolicy.xml`. Проанализировать содержимое файлов. Сделать выводы о корректности конфигурации политики междоменного взаимодействия RIA [3].

Шаг 3. Перейти по адресу `http://www.google.com`. Задать поисковые запросы, определяемые анализируемым приложением, например:

- `site:www.test.app.com filetype:docx confidential`
- `site:www.test.app.com filetype:doc secret`
- `site:www.test.app.com inurl:admin`
- `site:www.test.app.com filetype:sql`
- `site:www.test.app.com intext: "Access denied"`

Проанализировать логику запросов и полученные данные. Построить свои запросы, используя примеры из базы запросов [4].

Шаг 4. Перейти по адресу `http://www.shodanhq.com`. Задать следующий поисковый запрос:

- `hostname:www.test.app.com`

Построить свои запросы для приложения `www.test.app.com`. Шаг 5. Данный тест выполняется только для приложений, размещенных в лабораторной сети. С помощью сетевых сканеров Nmap и Xprobe выполнить идентификацию ОС веб-сервера:

```
# nmap –O www.test.app.com –vv
# xprobe2 www.test.app.com
```

Шаг 6. Подключиться к веб-серверу, используя утилиту Netcat:

```
# nc www.test.app.com 80
```

Отправить следующий GET запрос

```
GET / HTTP/1.1
Host: www.test.app.com
\r\n
```

По заголовкам `Server` и `X-Powered-By` определить программное обеспечение, реализующее веб-сервер и фрэймворк вебприложения.

В браузере установить расширение Wappalyzer, перейти по адресу веб-приложения и проанализировать информацию о компонентах веб-приложения полученное через Wappalyzer.
Шаг 7. С помощью сканера веб-серверов Httprint (дистрибутив Backtrack) или Httprecon (ОС Windows) выполнить идентификацию веб-сервера:

```
# cd /pentest/enumeration/web/httprint/linux
# ./httprint –h www.test.app.com –s signatures.txt
```

С помощью сканера Wafw00f проверить наличие у вебприложения подсистемы WAF:

```
# cd /pentest/web/waffit
# python ./wafw00f.py http://www.test.app.com
# python ./wafw00f.py https://www.test.app.com
```

Шаг 8. Выполнить тесты по идентификации поддерживаемых веб-сервером HTTP-методов. Для этого необходимо отправить с помощью Burp Suite или Netcat запрос следующего вида:

```
OPTIONS / HTTP/1.1 Host: www.test.app.com
\r\n
```

Проверить, поддерживает ли сервер обработку запросов с произвольными методами:

```
DOGS / HTTP/1.1
Host: www.test.app.com
\r\n
```

Если веб-сервер поддерживает метод TRACE, то это может привести к уязвимости к атаке Cross-Site Tracing (XST). Для проверки поддержки веб-сервером методы TRACE отправить запрос

```
TRACE / HTTP/1.1
Host: www.test.app.com
\r\n
```

Веб-сервер поддерживает метод TRACE и потенциально уязвим к атаке XST, если получен ответа вида

```
HTTP/1.1 200 OK
Connection: close
Content-Length: 39
TRACE / HTTP/1.1 Host: www.test.app.com
```

Задание:

1. Найти административные интерфейсы коммуникационного и сетевого оборудования (видеокамеры, коммутаторы ЛВС, домашние Wi-Fi маршрутизаторы, и т.д.), подключенные к сети Интернет.
2. Известно, что адрес веб-интерфейса системы VMWare Horizon View HTML Access содержит строку `portal/webclient/views/mainUI.html`. Найти такие системы, доступные из сети Интернет.

3. Оценить количество коммутаторов Cisco Catalyst с административным веб-интерфейсом, подключенным к сети Интернет.

2.19 Практическая работа №19. Анализ сетевого трафика. Использование Wireshark для анализа сеансов

Задание 1:

1. Загрузка и установка программы Wireshark (необязательно)

2. Сбор и анализ данных протокола ICMP по локальным узлам в программе Wireshark

- Начните и остановите сбор данных трафика эхо-запросов с помощью команды ping к локальным узлам.
- Найдите данные об IP- и MAC-адресах в полученных PDU.

3. Сбор и анализ данных протокола ICMP по удалённым узлам в программе Wireshark

- Начните и остановите сбор данных трафика эхо-запросов с помощью команды ping к удалённым узлам.
- Найдите данные об IP- и MAC-адресах в полученных PDU.
- Поясните, почему MAC-адреса удалённых узлов отличаются от MAC-адресов локальных узлов.

Задание 2:

Исходные данные/сценарий

На транспортном уровне TCP/IP используются два протокола — TCP, описанный в документе RFC 761, и UDP, описанный в документе RFC 768. Оба протокола поддерживают обмен данными по протоколу верхнего уровня. Например, TCP используется для поддержки транспортного уровня, в том числе и протоколов HTTP и FTP. Протокол UDP обеспечивает поддержку транспортного уровня DNS (службы доменных имён), TFTP и других протоколов.

Примечание. Сетевые инженеры обязаны знать компоненты заголовков и принцип работы протоколов TCP и UDP.

В части 1 лабораторной работы вам необходимо с помощью бесплатной программы Wireshark собрать и проанализировать поля заголовков протокола TCP для передачи файлов по протоколу FTP между главным компьютером и анонимным FTP-сервером. Подключение к анонимному FTP-серверу и загрузка файла выполняются с помощью утилиты командной строки Windows. В части 2 лабораторной работы вам необходимо с помощью бесплатной программы Wireshark собрать и проанализировать поля заголовков протокола UDP для передачи файлов по протоколу TFTP между главным компьютером и коммутатором S1.

Примечание. В задании используется коммутатор Cisco Catalyst 2960s с операционной системой Cisco

IOS версии 15.0(2) (образ lanbasek9). Можно использовать другие коммутаторы и версии ПО Cisco IOS. В зависимости от модели и версии Cisco IOS доступные команды и результаты их выполнения могут отличаться от представленных в лабораторных работах.

Примечание. Коммутатор необходимо очистить от данных и загрузочной конфигурации. Если вы не уверены, что сможете это сделать, обратитесь к инструктору.

Примечание. Часть 1 предполагает наличие компьютера с доступом в Интернет; Netlab для её

выполнения не подходит. Задания в части 2 могут выполняться с использованием Netlab.

Необходимые ресурсы — часть 1 (FTP)

Один ПК (Windows 7, Vista или XP с доступом к командной строке, выходом в Интернет и установленной программой Wireshark).

Необходимые ресурсы — часть 2 (TFTP)

- 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 установленными программой Wireshark и TFTP-сервером, например Tftpd32)
- Кабель для настройки устройств с операционной системой Cisco IOS через консольный порт.
- Кабель Ethernet, как показано в схеме топологии.

Часть 1: Определение полей и принципа работы заголовков TCP с помощью функции захвата сеанса FTP программы Wireshark

В части 1 вам необходимо с помощью программы Wireshark получить данные о сеансе FTP и изучить поля заголовков TCP.

Шаг 1: Начните захват данных программой Wireshark.

a. Закройте все ненужные сетевые приложения, например браузер, чтобы ограничить количество трафика во время захвата данных программой Wireshark.

b. Начните захват данных программой Wireshark.

Шаг 2: Загрузите файл справки Readme.

a. В окне командной строки введите **ftp ftp.cdc.gov**.

b. Подключитесь к FTP-узлу Центра по контролю и профилактике заболеваний (CDC), указав в качестве имени пользователя **anonymous** (пароль вводить не нужно).

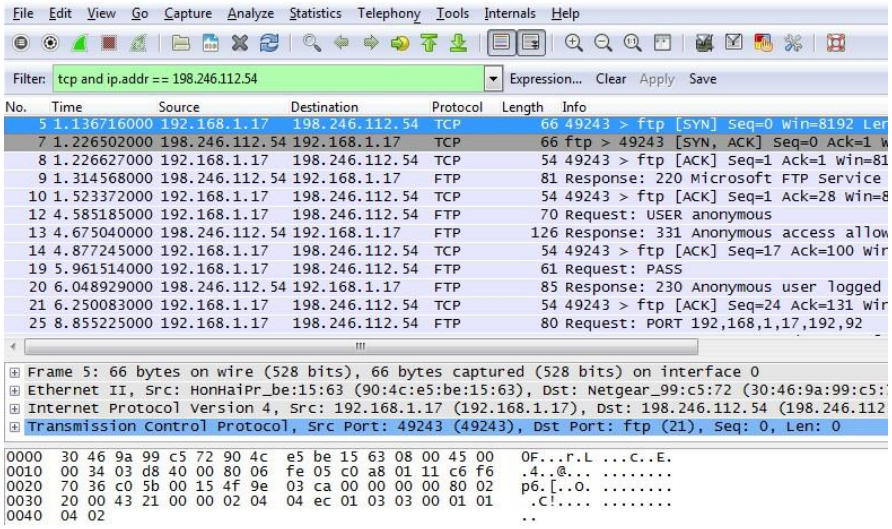
c. Найдите и загрузите файл справки Readme.

```
C:\Users\user1>ftp ftp.cdc.gov
Connected to ftp.cdc.gov.
220 Microsoft FTP Service
User (ftp.cdc.gov:(none)): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 Anonymous user logged in.
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection for file list.
aspnet_client
pub
Readme
Siteinfo
up.htm
w3c
web.config
welcome.msg
226 Transfer complete.
ftp: 76 bytes received in 0.00Seconds 19.00Kbytes/sec.
ftp> get Readme
200 PORT command successful.
150 Opening ASCII mode data connection for Readme(1428 bytes).
226 Transfer complete.
ftp: 1428 bytes received in 0.01Seconds 204.00Kbytes/sec.
ftp> quit
221
```

Шаг 3: Остановите сбор данных программой Wireshark.

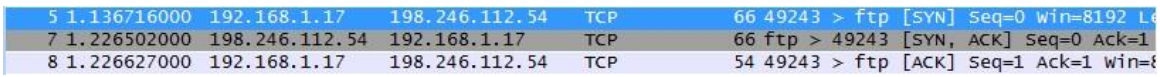
Шаг 4: Откройте главное окно программы Wireshark.

Во время сеанса FTP-подключения к сайту ftp.cdc.gov программа Wireshark захватила большое число пакетов. Чтобы ограничить количество полученных данных для дальнейшего анализа, введите критерий **tcp and ip.addr == 198.246.112.54** в поле **Filter:** (Фильтр) и нажмите **Apply** (Применить) Введённый IP-адрес 198.246.112.54 — это адрес сайта ftp.cdc.gov.



Шаг 5: Проанализируйте поля TCP.

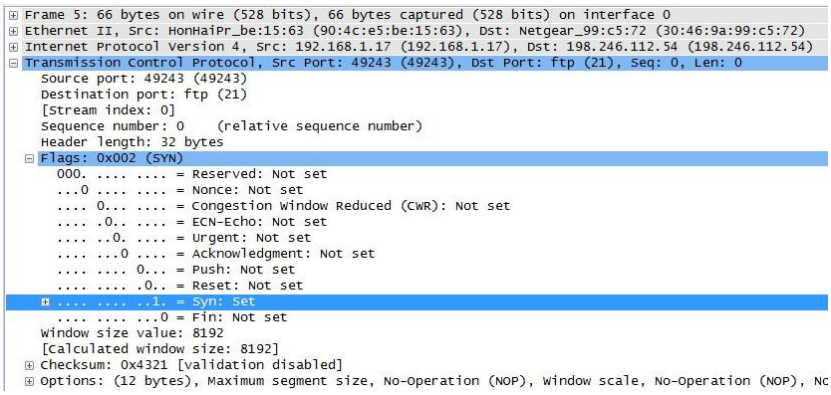
После применения фильтра TCP первые три кадра на панели списка пакетов (верхний раздел) отображают протокол транспортного уровня TCP, создающий надёжный сеанс связи. Последовательность [SYN], [SYN, ACK] и [ACK] иллюстрирует трёхстороннее рукопожатие.



Протокол TCP регулярно используется во время сеанса связи для контроля доставки датаграмм, проверки их поступления и управления размером окна. Для каждого обмена данными между FTPклиентом и FTP-сервером запускается новый сеанс TCP. По

завершении передачи данных сеанс TCP закрывается. По завершении сеанса FTP протокол TCP выполняет плановое отключение и прекращение работы.

Программа Wireshark отображает подробные данные TCP на панели сведений о пакетах (средний раздел). Выделите первую датаграмму TCP с главного компьютера и разверните строку TCP. Откроется показанная ниже расширенная датаграмма TCP, подобная панели сведений о пакетах.



На приведённом выше изображении показана схема TCP-датаграммы. Для большей ясности к каждому полю приводится пояснение.

- Поле **Номер источника TCP** (TCP source port number) относится к узлу сеанса TCP, который установил подключение. Обычно используется произвольное значение больше 1023.

- Поле **TCP destination port number** (Номер порта назначения TCP) используется для идентификации протокола верхнего уровня или приложения на удалённом сайте. Значения в диапазоне от 0 до 1023 соответствуют «хорошо известным портам» и связаны с популярными сервисами и приложениями (как описано в документе RFC 1700, такими как Telnet, FTP, HTTP и т. д.). Комбинация IP-адреса и порта источника и IP-адреса и порта назначения однозначно определяет сеанс как для отправителя, так и для получателя.

Примечание. В приведённых ниже данных, захваченных программой Wireshark, указан порт назначения 21, который используется для FTP. Через порт 21 FTP-серверы принимают пакеты, предназначенные для подключений FTP-клиента.

- В поле **Sequence number** (Порядковый номер) указывается номер последнего октета в сегменте.

- В поле **Acknowledgment number** (Номер подтверждения) указывается следующий октет, который ожидается получателем.

• Значение в поле **Code bits** (Кодовые биты) играет особую роль в управлении сеансами и обработке сегментов. Среди интересных значений можно привести следующие:

- ACK — подтверждение получения сегмента.

- SYN — синхронизация, устанавливается только в том случае, если новый сеанс TCP согласовывается в процессе трёхстороннего рукопожатия TCP.

- FIN — завершение, запрос о прекращении сеанса TCP.

• В поле **Window size** (Размер окна) отображается значение скользящего окна, которое определяет, сколько октетов могут быть отправлены до ожидания подтверждения.

• Поле **Urgent pointer** (Указатель важности) используется только с флагом срочности Urgent (URG), когда отправителю необходимо переслать важные данные на узел получателя.

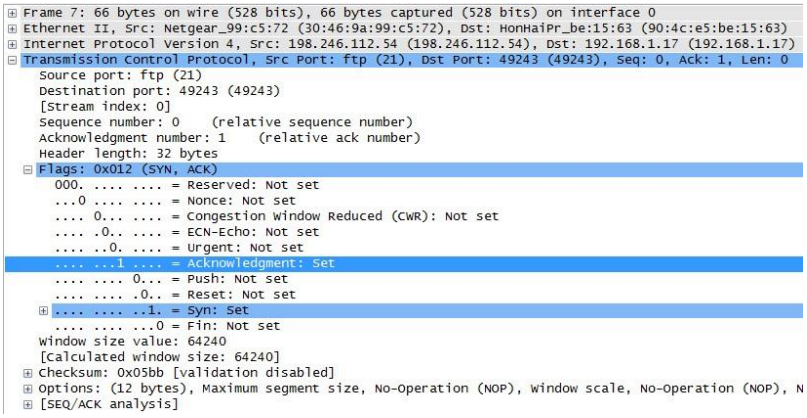
• Для поля **Options** (Параметры) в настоящее время используется только один параметр, определяемый как максимальный размер TCP-сегмента (дополнительное значение).

Используя данные, захваченные программой Wireshark для запуска первого сеанса TCP (бит SYN установлен как 1), заполните информацию о заголовке TCP.

От ПК к серверу CDC (только бит SYN установлен как 1):

IP-адрес источника:	
IP-адрес назначения:	
Номер порта источника:	
Номер порта назначения:	
Порядковый номер:	
Номер подтверждения:	
Длина заголовка:	
Размер окна:	

Во втором окне отфильтрованных данных, захваченных программой Wireshark, FTP-сервер CDC подтверждает запрос, отправленный компьютером. Обратите внимание на значения битов для SYN и ACK.

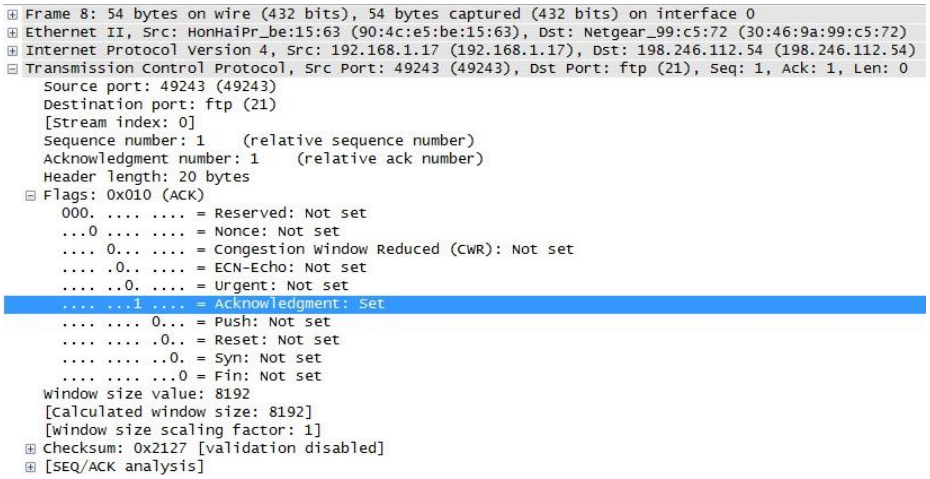


Заполните приведённую ниже таблицу данными сообщения SYN-ACK.

IP-адрес источника:	

IP-адрес назначения:	
Номер порта источника:	
Номер порта назначения:	
Порядковый номер:	
Номер подтверждения:	
Длина заголовка:	
Размер окна:	

На последнем этапе согласования для установления связи компьютер отправляет серверу сообщение подтверждения. Обратите внимание на то, что только бит ACK имеет значение 1, в то время как значение Sequence number (Порядковый номер) увеличено до 1.



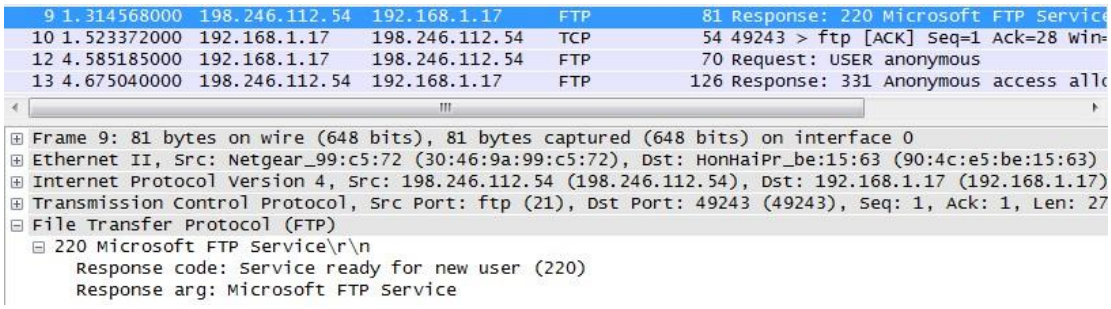
Заполните приведённую ниже таблицу данными сообщения ACK.

IP-адрес источника:	
IP-адрес назначения:	
Номер порта источника:	
Номер порта назначения:	
Порядковый номер:	
Номер подтверждения:	
Длина заголовка:	
Размер окна:	

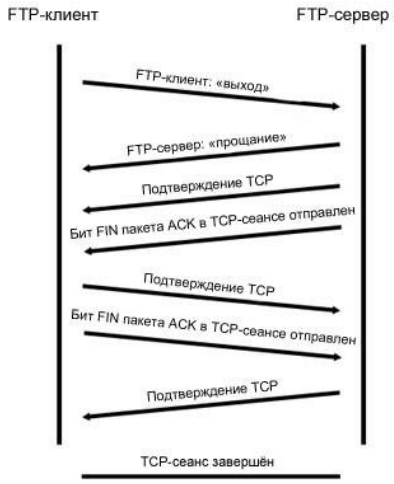
Сколько других датаграмм TCP содержали бит SYN?

Как только сеанс TCP установлен, появляется возможность для передачи FTP-трафика между компьютером и FTP-сервером. FTP-клиент и сервер взаимодействуют

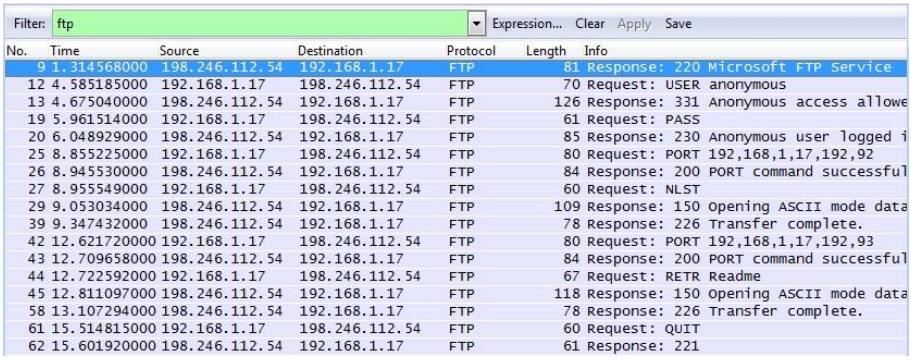
друг с другом, не зная о том, что TCP контролирует сеанс и может им управлять. Когда FTP-сервер отправляет FTP-клиенту сообщение Response: 220, сеанс TCP на FTP-клиенте отправляет подтверждение сеансу TCP на сервере. Эту последовательность можно увидеть в приведенном ниже окне захвата данных программой Wireshark.



Когда сеанс FTP завершается, FTP-клиент отправляет команду quit (завершить). FTP-сервер подтверждает прекращение сеанса FTP, отправляя ответ Response: 221 Goodbye. В этот раз сеанс TCP FTP-сервера отправляет датаграмму TCP FTP-клиенту, сообщая о прекращении сеанса TCP. Сеанс TCP FTP-клиента подтверждает получение датаграммы прекращения, после чего отправляет собственное сообщение о прекращении сеанса TCP. Получив копию сообщения о прекращении, FTPсервер, инициировавший прекращение сеанса TCP, отправляет датаграмму ACK с подтверждением прекращения, и сеанс TCP завершается. Эту последовательность можно увидеть в приведённой ниже схеме и результатах захвата данных.



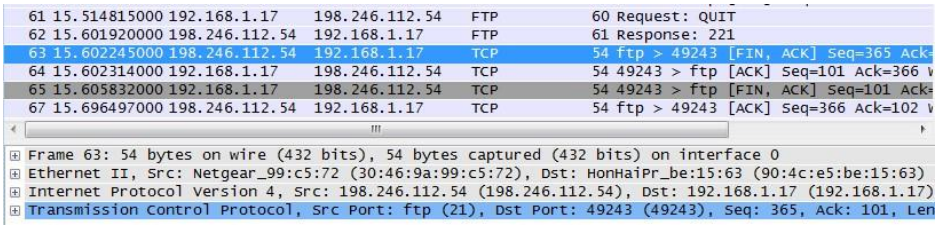
Применение фильтра **ftp** позволяет изучить всю последовательность трафика FTP с помощью программы Wireshark. Обратите внимание на последовательность событий во время этого сеанса FTP. Для загрузки файла справки Readme было использовано имя пользователя anonymous. По окончании передачи файлов пользователь завершил сеанс FTP.



Ещё раз примените фильтр TCP программы Wireshark, чтобы изучить процесс прекращения сеанса TCP. Для завершения сеанса TCP передаются четыре пакета. Поскольку подключение TCP является полнодуплексным, для каждого направления требуется отдельное прекращение сеанса. Изучите адреса источника и назначения.

В этом примере у FTP-сервера больше нет данных для отправки в потоке; он отправляет сегмент с флагом завершения FIN, установленным в кадре 63. Компьютер отправляет ACK, чтобы подтвердить получение FIN для завершения сеанса связи между сервером и клиентом в кадре 64.

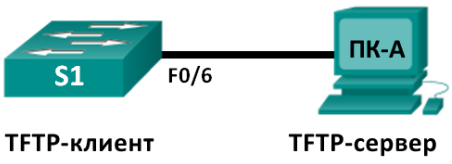
В кадре 65 компьютер посылает FIN FTP-серверу, чтобы завершить сеанс TCP. FTP-сервер отправляет ответ, содержащий ACK в кадре 67, чтобы подтвердить получение FIN от компьютера. После этого сеанс TCP между FTP-сервером и компьютером завершается.



Часть 2: Определение полей и принципа работы заголовков UDP с помощью функции захвата сеанса TFTP программы Wireshark

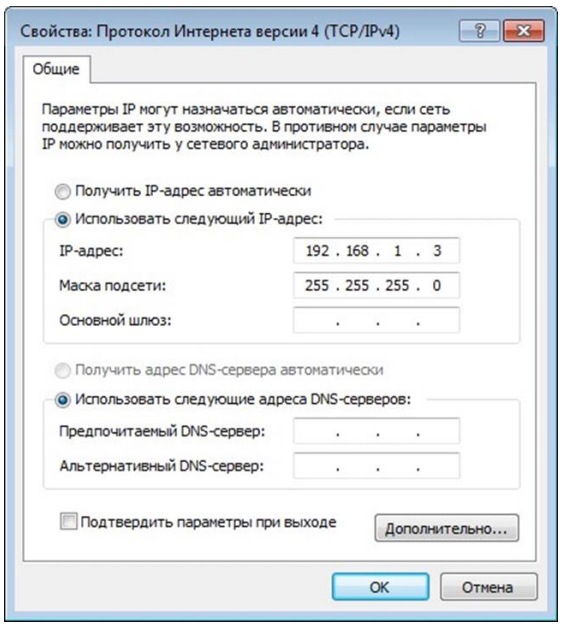
В части 2 вам необходимо с помощью программы Wireshark получить данные о сеансе TFTP и изучить поля заголовков UDP.

Шаг 1: Постройте физическую топологию сети и подготовьте всё необходимое для захвата данных о сеансе TFTP.



a. Установите между компьютером ПК-А и коммутатором S1 Ethernet-подключение и подключение через консоль.

b. Если это ещё не сделано, укажите IP-адрес компьютера (192.168.1.3) вручную. Для настройки шлюза по умолчанию это не требуется.



a. Настройте коммутатор. Для сети VLAN 1 укажите IP-адрес 192.168.1.1. Проверьте подключение к компьютеру, отправив эхо-запрос с помощью команды ping на адрес 192.168.1.3. При необходимости устраните неполадки.

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#host S1
S1(config)#interface vlan 1
S1(config-if)#ip address 192.168.1.1 255.255.255.0
S1(config-if)#no shut
*Mar    1  00:37:50.166:  %LINK-3-UPDOWN:  Interface  Vlan1, changed state to up
*Mar  1 00:37:50.175: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up S1(config-if)# end
S1# ping 192.168.1.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/203/1007 ms
```

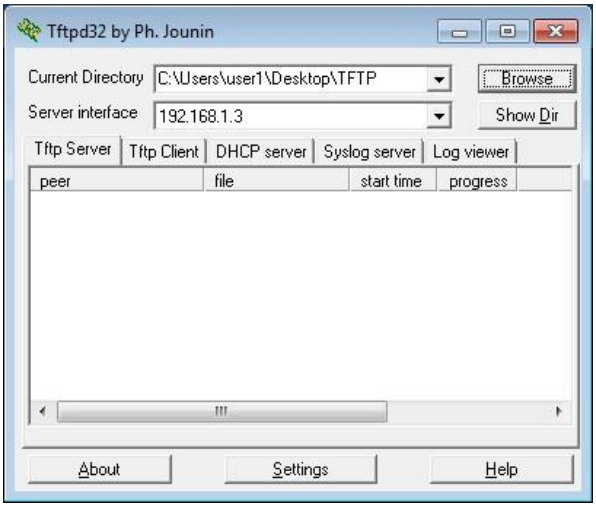
Шаг 2: Подготовьте TFTP-сервер на компьютере.

a. На рабочем столе создайте папку **TFTP**, если такой ещё нет. В неё будут скопированы файлы с коммутатора.

b. На компьютере запустите программу **Tftpd32**.

c. Нажмите кнопку **Browse** (Обзор) и вместо выбранной папки укажите **C:\Users\user1\Desktop\TFTP**, заменив user1 на своё имя пользователя.

TFTP-сервер должен иметь следующий вид:



Обратите внимание на то, что в поле Current Directory (Текущий каталог) указаны пользователь и интерфейс сервера Server (ПК-A) в виде IP-адреса **192.168.1.3**.

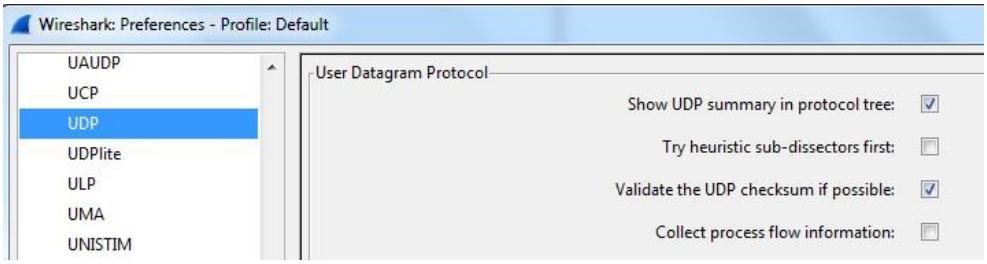
d. Проверьте возможность копирования файлов с коммутатора на компьютер с помощью TFTP. При необходимости устраните неполадки.

```
S1# copy start tftp
Address or name of remote host []?
192.168.1.3 Destination filename [s1-confg]?
!!
1638 bytes copied in 0.026 secs (63000 bytes/sec)
```

Если вы видите, что файл скопирован (как в приведённом выше примере), переходите к следующему шагу. В противном случае устраните неполадки. Если появится сообщение об ошибке `%Error opening tftp (Permission denied)` (%Невозможно открыть tftp (нет прав доступа)), проверьте, не блокирует ли ваш межсетевой экран протокол TFTP, и убедитесь в том, что копирование выполняется в папку с правами доступа для вашего имени пользователя, например, в папку на рабочем столе.

Шаг 3: Захватите данные о сеансе TFTP с помощью программы Wireshark.

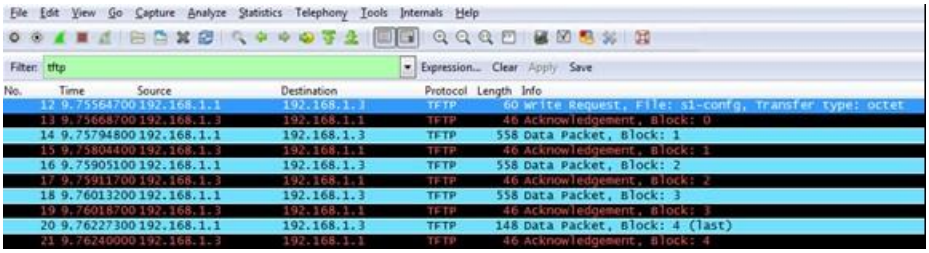
a. Откройте Wireshark. В меню **Edit** (Правка) выберите пункт **Preferences** (Установки) и нажмите на значок «плюс» (+), чтобы раскрыть меню **Protocols** (Протоколы). Прокрутите экран вниз и выберите **UDP**. Установите флажок **Validate the UDP checksum if possible** (Проверять контрольную сумму UDP, если возможно) и нажмите **Apply** (Применить). Затем нажмите кнопку **OK**.



b. Начните захват данных программой Wireshark.

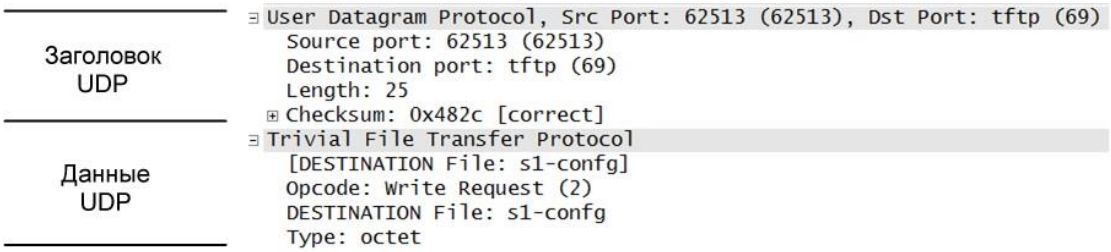
c. На коммутаторе введите команду **`copy start tftp`**.

d. Остановите сбор данных программой Wireshark.



e. Для фильтра выберите значение **tftp**. Полученные результаты должны выглядеть примерно так, как показано выше. Эта передача TFTP используется для анализа работы UDP транспортного уровня.

Программа Wireshark отображает подробные данные UDP на панели сведений о пакетах. Выделите первую датаграмму UDP, полученную с главного компьютера, и наведите указатель мыши на панель сведений о пакетах. При необходимости скорректируйте эту панель и разверните строку UDP, нажав на соответствующее поле. Расширенная датаграмма UDP должна выглядеть подобно приведённой ниже схеме.



На приведённом выше изображении показана схема UDP-датаграммы. По сравнению с датаграммой TCP информация в заголовке не такая подробная. Как и в случае с TCP, каждая датаграмма UDP обозначается портом источника UDP и портом назначения UDP.

Используя данные, захваченные программой Wireshark для первой датаграммы UDP, заполните информацию о заголовке UDP. Значение контрольной суммы имеет формат шестнадцатеричного числа (основание 16) с предшествующим кодом 0x.

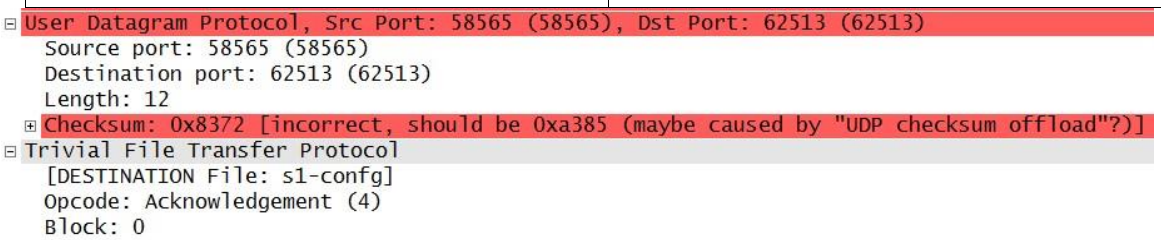
IP-адрес источника:	
IP-адрес назначения:	
Номер порта источника:	
Номер порта назначения:	
Длина сообщения UDP:	
Контрольная сумма UDP:	

Как протокол UDP проверяет правильность датаграммы?

_____

Изучите первый кадр, возвращённый TFTPD-сервером. Заполните приведённую ниже таблицу данными заголовка UDP.

IP-адрес источника:	
IP-адрес назначения:	
Номер порта источника:	
Номер порта назначения:	
Длина сообщения UDP:	
Контрольная сумма UDP:	



Обратите внимание на то, что в возвращённой датаграмме UDP указывается другой порт источника UDP, который, однако, используется до конца пересылки данных по TFTP. Поскольку надёжное соединение отсутствует, для пересылки данных по TFTP используется только исходный порт источника, предназначенный для начала сеанса TFTP.

- Кроме того, необходимо учитывать, что значение в поле UDP Checksum (Контрольная сумма UDP) указано неверно. Скорее всего, это вызвано выгрузкой контрольной суммы UDP (UDP checksum offload). Дополнительную информацию о причинах этого явления можно найти в Интернете, выполнив поиск по словам «UDP checksum offload» или «выгрузка контрольной суммы UDP».

2.20 Практическая работа № 20 Аудит безопасности сетей. Аудит безопасности сетей. Обеспечение безопасности локальной сети

Задание 1:

1. Соберите сеть, состоящую из двух коммутаторов 2960.
   1.1. На каждом коммутаторе отключите использование протокола SPT в VLAN 1.
   1.2. На одном из коммутаторов сконфигурируйте layer 3 для VLAN 1 (например, IP адрес 1.1.1.1).
   1.3. Административно включите интерфейс VLAN 1.
   1.4. Соедините коммутаторы двумя каналами (интерфейсы fastEthernet 0/1 и 0/2).
   1.5. На коммутаторе, на котором настроен VLAN, попробуйте выполнить запрос ARP несуществующего адреса (например, 2.2.2.2, можно сделать команду ping).
   1.6. В режиме моделирования убедитесь, что даже после завершения запроса в сети бесконечно присутствует широковещательные запросы ARP и получился цифровой шторм.
2. В моделируемую сеть предприятия в главном офисе добавьте коммутатор и соедините его так, как показано на рисунке 1.

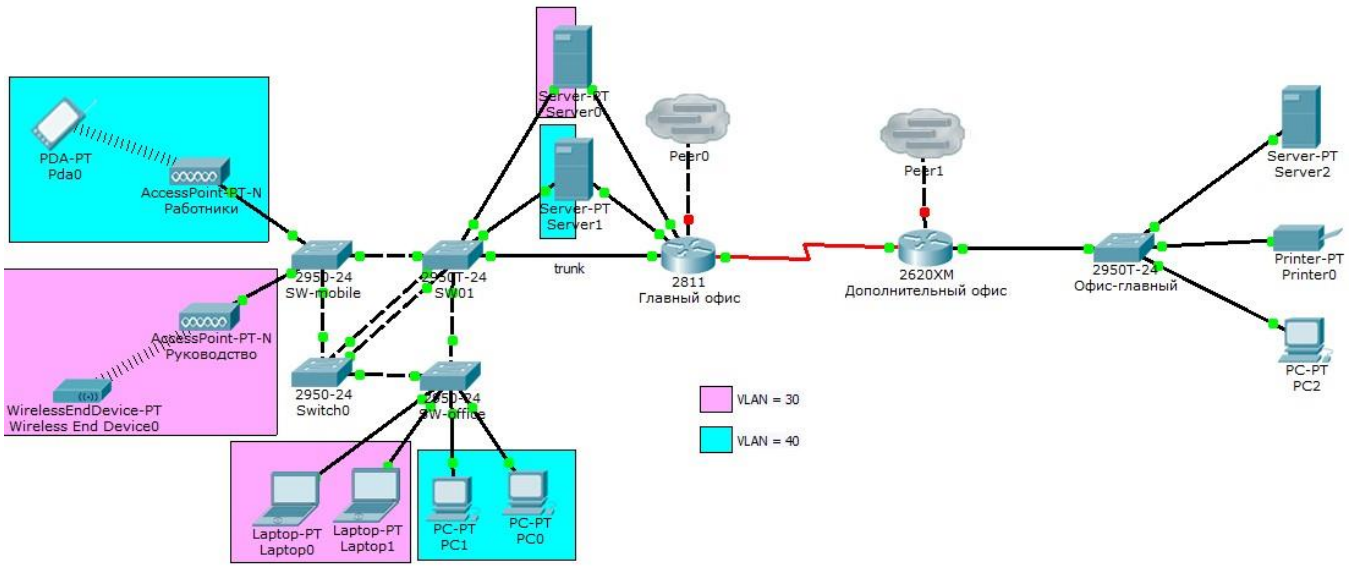


Рисунок 1 – Схема сети исследуемого предприятия

2.1. Настройте между коммутаторами Switch0 и SW1 агрегированный канал. Какой из коммутаторов выполняет пассивную и активную роль выбирает преподаватель.
2.2. Используя режим моделирования продемонстрируйте работоспособность созданного агрегированного канала. Подсказка - для этого можно временно в сеть добавить сетевые устройства.
2.3. Настройте коммутатор Switch 0 так, чтобы все его каналы участвовали в VLAN с номерами 30 и 40. Настройте коммутаторы SW-mobile, SW-office, SW01 так, чтобы коммутатор Switch 0 стал участником VLAN с номерами 30 и 40.
2.4. Проведите «вручную» расчет конфигурации сети после применения протокола STP в VLAN с номерами 1, 30, 40. Продемонстрируйте правильность своих расчетов результатами работы STP в моделируемой сети.
2.5. Измените конфигурацию сети так, чтобы корневыми коммутаторами для STP в сетях VLAN с номерами 30 и 40 были те, которые укажет преподаватель. Также преподаватель вправе потребовать изменить скорости передачи некоторых каналов.
2.6. Повторите п.2.4 с учетом сделанных настроек.
2.7. Используя режим моделирования продемонстрируйте путь прохождения юникастового трафика в сетях VLAN с номерами 30 и 40. (Например, ping).

Задание 2:

1. **Часть 1: Настройка основных параметров устройств**
   В части 1 потребуется настроить топологию сети и основные параметры, такие как IP-адреса интерфейсов, доступ к устройствам и пароли на устройствах.

Шаг 1: Создайте сеть согласно топологии.

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

Шаг 2: Выполните инициализацию и перезагрузку маршрутизатора и коммутатора.

Шаг 3: Выполните настройку маршрутизатора и коммутатора.

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

b. Назначьте устройству имя в соответствии с таблицей адресации.

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

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

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

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

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

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

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

j. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

2. Часть 2: Настройка базовых мер безопасности на маршрутизаторе

Шаг 1: Зашифруйте открытые пароли.

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

Шаг 2: Установите более надежные пароли.

Администратор должен следить за тем, чтобы пароли отвечали стандартным рекомендациям по созданию надежных паролей. В рекомендациях должны быть определены сочетания в пароле букв, цифр и специальных символов и его минимальная длина.

Примечание. Согласно данным рекомендациям по лучшим практическим методикам надежные пароли, примеры которых приведены в этой лабораторной работе, необходимо всегда использовать в реальной работе. Однако для упрощения выполнения работы в остальных лабораторных работах данного курса используются пароли cisco и class.

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

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

b. Установите минимальную длину 10 символов для всех паролей.

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

Шаг 3: Разрешите подключения по протоколу SSH.

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

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

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**

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**

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

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

e. Создайте ключ шифрования RSA с длиной 1024 бит.

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

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)#

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. Низкое значение этого таймера установлено специально для данной лабораторной работы.

R1(config)# **login block-for 30 attempts 2 within 120** Что

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

_____

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

_____

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#

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.

_____

_____

b. С помощью программы Tera Term подключитесь к маршрутизатору R1 по протоколу SSH.

Разрешает ли R1 подключение по протоколу SSH? _____.

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?

_____

_____

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#

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? _____

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.

_____

_____

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