

Приложение 3.5.1 к ОПОП по специальности 09.02.01 Компьютерные системы и комплексы

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет
им. Г. И. Носова»
Многопрофильный колледж

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ
ДЛЯ ЛАБОРАТОРНЫХ И ПРАКТИЧЕСКИХ ЗАНЯТИЙ
МЕЖДИСЦИПЛИНАРНОГО КУРСА
МДК.05.01 СЕТЕВАЯ БЕЗОПАСНОСТЬ И ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА
ЗАЩИТЫ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ**

для обучающихся специальности

09.02.01 Компьютерные системы и комплексы

Магнитогорск, 2024

ОДОБРЕНО

Предметной / Предметно-цикловой комиссией
«Информатики и вычислительной техники»
Председатель Т.Б. Ремез
Протокол № 5 от «31» января 2024

Методической комиссией МпК

Протокол № 3 от «21» февраля 2024.

Разработчик:

Преподаватель отделения №2 «Информационных технологий и транспорта» Н. А. Криворучко
Многопрофильного колледжа ФГБОУ ВО «МГТУ им. Г.И. Носова»

Методические указания для лабораторных занятий разработаны на основе рабочей программы ПМ. 05 Обслуживание средств защиты информации в компьютерных системах и сетях.

Содержание лабораторных и практических занятий ориентировано на формирование общих и профессиональных компетенций по основной профессиональной образовательной программе по специальности 09.02.01 Компьютерные системы и комплексы: МДК.05.01 Сетевая безопасность и программно-аппаратные средства защиты телекоммуникационных систем.

СОДЕРЖАНИЕ

1 ВВЕДЕНИЕ	4
2 МЕТОДИЧЕСКИЕ УКАЗАНИЯ	5
Лабораторное занятие №1	5
Лабораторное занятие № 2	7
Лабораторное занятие № 3	9
Лабораторное занятие № 4	11
Лабораторное занятие № 5	13
Лабораторное занятие № 6	15
Лабораторное занятие № 7	19
Лабораторное занятие № 8	22
Лабораторное занятие № 9	26
Лабораторное занятие № 10	28
Лабораторное занятие № 11	33
Лабораторное занятие № 12	35
Лабораторное занятие № 13	42
Лабораторное занятие № 14	44
Лабораторное занятие № 15	46
Лабораторное занятие № 16	48

1 ВВЕДЕНИЕ

Важную часть теоретической и профессиональной практической подготовки обучающихся составляют лабораторные занятия.

Состав и содержание лабораторных занятий направлены на реализацию Федерального государственного образовательного стандарта среднего профессионального образования.

Ведущей дидактической целью лабораторных занятий является экспериментальное подтверждение и проверка существенных теоретических положений (законов, зависимостей).

В соответствии с рабочей программой ПМ. 05 Обслуживание средств защиты информации в компьютерных системах и сетях, МДК.05.01 Сетевая безопасность и программно-аппаратные средства защиты телекоммуникационных предусмотрено проведение лабораторных занятий.

В результате их выполнения, обучающийся должен:

уметь:

У1. Настраивать стек протоколов TCP/IP и использовать встроенные утилиты операционной системы для диагностики работоспособности сети.

У2. Использовать программно-аппаратные средства технического контроля.

Содержание практических и лабораторных занятий ориентировано на подготовку обучающихся к освоению профессионального модуля программы подготовки специалистов среднего звена по специальности и овладению **профессиональными компетенциями:**

ПК 5.1. Обеспечивать защиту информации в сети с использованием программно-аппаратных средств А также формированию **общих компетенций:**

ОК 01 Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам.

ОК 02 Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности.

ОК 03 Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях.

Выполнение обучающихся практических и лабораторных занятий по ПМ. 05 Обслуживание средств защиты информации в компьютерных системах и сетях, МДК.05.01 Сетевая безопасность и программно-аппаратные средства защиты телекоммуникационных направлено на:

- обобщение, систематизацию, углубление, закрепление, развитие и детализацию полученных теоретических знаний по конкретным темам междисциплинарных курсов;

- формирование умений применять полученные знания на практике, реализацию единства интеллектуальной и практической деятельности;

- формирование и развитие умений: наблюдать, сравнивать, сопоставлять, анализировать, делать выводы и обобщения, самостоятельно вести исследования, оформлять результаты в виде таблиц, схем, графиков;

- развитие интеллектуальных умений у будущих специалистов: аналитических, проективных, конструктивных и др.;

- выработку при решении поставленных задач профессионально значимых качеств, таких как самостоятельность, ответственность, точность, творческая инициатива.

Лабораторные занятия проводятся в рамках соответствующей темы, после освоения дидактических единиц, которые обеспечивают наличие знаний, необходимых для ее выполнения.

2 МЕТОДИЧЕСКИЕ УКАЗАНИЯ

Тема 1.1. Безопасность сетей Ethernet Лабораторное занятие №1

Настройка протокола SNMP

Цель работы: Изучение способов мониторинга и управления сетью на основе протокола SNMP с использованием собственных механизмов безопасности.

Выполнение работы способствует формированию:

У1. Настраивать стек протоколов TCP/IP и использовать встроенные утилиты операционной системы для диагностики работоспособности сети.

У2. Использовать программно-аппаратные средства технического контроля.

Материальное обеспечение:

учебно-лабораторный стенд «Сетевая безопасность»0

Порядок выполнения работы:

1. Постройте топологию сети, показанную на рисунке 1.

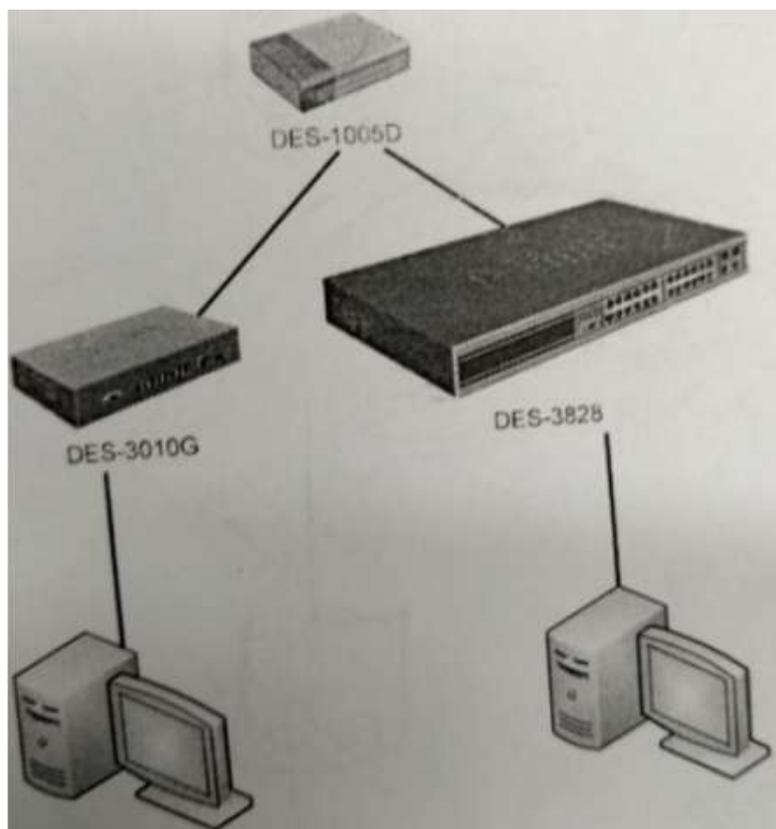


Рисунок 1 – Схема сети

2. Изучите раздел «Протокол SNMP» теоретического пособия.
3. Настройте SNMP-протокол на коммутаторах.
4. Изучите раздел «Утилиты управления сетью по протоколу SNMP».
5. Запустите утилиту iReasoning MIB Browser.
6. Загрузите базу MIB RFC-1213.
7. На обоих коммутаторах (DES-3010 и DES-3828) выясните следующие параметры:

- название устройства, время работы устройства, службы, запущенные на устройстве (ветвь system);
 - количество интерфейсов на устройстве, содержимое таблицы интерфейсов, название двух дополнительных виртуальных портов (ветвь interfaces);
 - IP-адрес устройства, содержимое таблицы маршрутизации (ветвь ip);
 - TCP-соединения, установленные устройством (ветвь tcp).
8. Загрузите базы MIB Time, DES-3010G-L2MGMT из каталога root/Desktop/SNMP/DES3000-MIB/private/.
 9. Определите текущее системное время коммутатора.
 10. Определите состояние портов коммутатора (база DES-3010G-L2MGMT, ветвь swL2PortinfoTable, таблица swL2PortMgmt).

Форма представления результата: Отчет о проделанной работе, выполненная работа.

Критерии оценки:

Оценка «отлично» ставится, если задание выполнено верно.

Оценка «хорошо» ставится, если ход выполнения задания верный, но была допущена одна или две ошибки, приведшие к неправильному ответу.

Оценка «удовлетворительно» ставится, если в работе не получен ответ и приведено неполное выполнение задания, но ход выполнения задания.

Оценка «неудовлетворительно» ставится, если задание не выполнено.

Тема 1.1. Безопасность сетей Ethernet

Лабораторное занятие № 2

Настройка протоколов STP, RSTP, MSTP

Цель работы: Изучение алгоритма Spanning Tree и Rapid Spanning Tree

Выполнение работы способствует формированию:

У1. Настраивать стек протоколов TCP/IP и использовать встроенные утилиты операционной системы для диагностики работоспособности сети.

У2. Использовать программно-аппаратные средства технического контроля.

Материальное обеспечение:

учебно-лабораторный стенд «Сетевая безопасность»

Порядок выполнения работы:

1. Изучите раздел «Аудит безопасности протокола связующего дерева STP» теоретического пособия и раздел «L2 Features» (меню «Spanning Tree»).
2. Соберите сеть с топологией, представленной на рисунке 2.

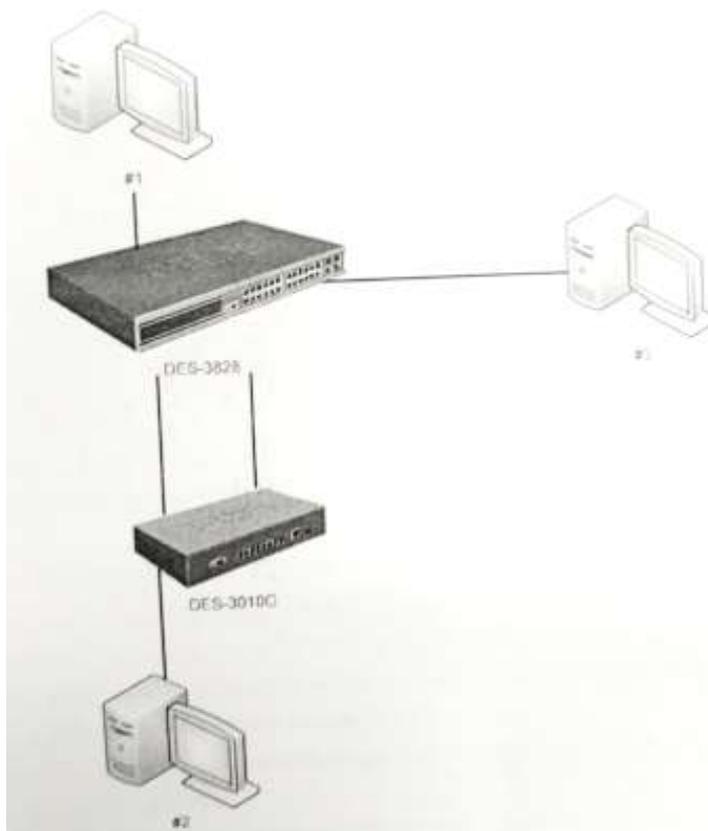


Рисунок 2 – Схема сети

3. Настройте и активизируйте на коммутаторах протокол Spanning Tree (*замечание: по причине недоработки компанией D-Link программного обеспечения коммутатора DES-3828 приоритет коммутатора на данной модели выставить невозможно. Поэтому приоритет коммутатора DES-3828 постоянен и равен 32768, что не мешает выполнению практической работы*).
4. Параллельно с шагом 3 запустите на машине #3 утилите tcdump и выясните MAC-адреса коммутаторов, анализируя содержимое пакетов BPDU.
5. Сбросьте настройки коммутатора в фабричные и перезагрузите его.

Форма представления результата: Отчет о проделанной работе, выполненная работа.

Критерии оценки:

Оценка «отлично» ставится, если задание выполнено верно.

Оценка «хорошо» ставится, если ход выполнения задания верный, но была допущена одна или две ошибки, приведшие к неправильному ответу.

Оценка «удовлетворительно» ставится, если в работе не получен ответ и приведено неполное выполнение задания, но ход выполнения задания.

Оценка «неудовлетворительно» ставится, если задание не выполнено.

Тема 1.1. Безопасность сетей Ethernet

Лабораторное занятие № 3

Списки контроля доступа ACL

Цель работы: Изучение технологии Access Control Lists.

Выполнение работы способствует формированию:

У1. Настраивать стек протоколов TCP/IP и использовать встроенные утилиты операционной системы для диагностики работоспособности сети.

У2. Использовать программно-аппаратные средства технического контроля.

Материальное обеспечение:

учебно-лабораторный стенд «Сетевая безопасность»

Порядок выполнения работы:

1. Соберите сеть с топологией, представленной на рисунке 3.

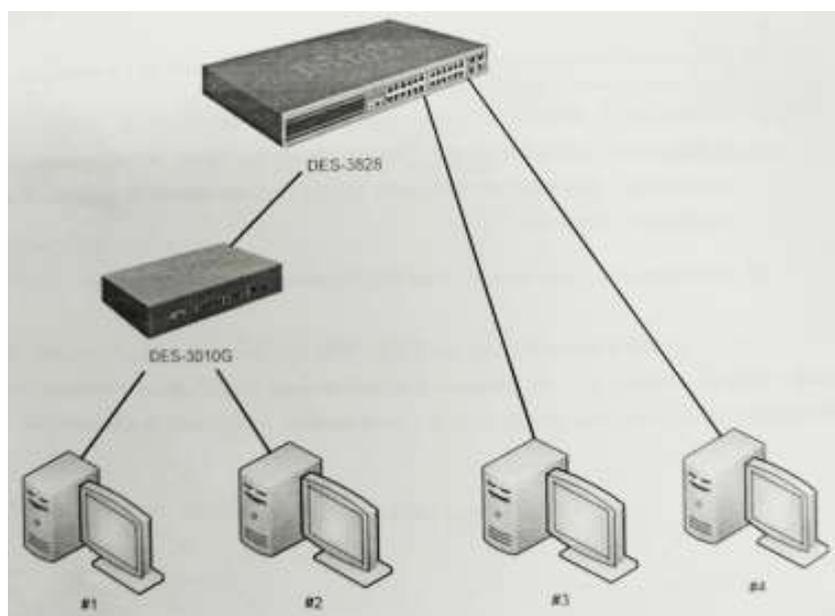


Рисунок 3 – Топология сети

2. Изучите раздел «Списки контроля доступа» теоретического пособия и раздел «ACL» (меню «Access Profile Table»).
3. Настройте списки контроля доступа таким образом, чтобы:
 - ни один из коммутаторов DES-3010 не мог «пропинговать» машину #4;
 - машина #1 могла «пропинговать» машину #3, но не могла – машину #4;
 - машина #2 могла скачать файл с машины #4 (используя ftp-протокол), но не могла получить почтовые сообщения;
 - только тот трафик, который идет от машины #2 к машине #3 «зеркалировался» на порт машины #4.
4. Проверьте созданные настройки.

Форма представления результата: отчет о проделанной работе, выполненная работа.

Критерии оценки:

Оценка «отлично» ставится, если задание выполнено верно.

Оценка «хорошо» ставится, если ход выполнения задания верный, но была допущена одна или две ошибки, приведшие к неправильному ответу.

Оценка «удовлетворительно» ставится, если в работе не получен ответ и приведено неполное выполнение задания, но ход выполнения задания.

Оценка «неудовлетворительно» ставится, если задание не выполнено.

Тема 1.1. Безопасность сетей Ethernet

Лабораторное занятие № 4

Контроль над подключением узлов к портам коммутатора. Функции Port Security, Port Binding

Цель работы: Изучение функций IP-MAC Binding и Port Binding.

Выполнение работы способствует формированию:

У1. Настраивать стек протоколов TCP/IP и использовать встроенные утилиты операционной системы для диагностики работоспособности сети.

У2. Использовать программно-аппаратные средства технического контроля.

Материальное обеспечение:

учебно-лабораторный стенд «Сетевая безопасность»

Порядок выполнения работы:

1. Соберите топологию сети, представленную на рисунке 4.

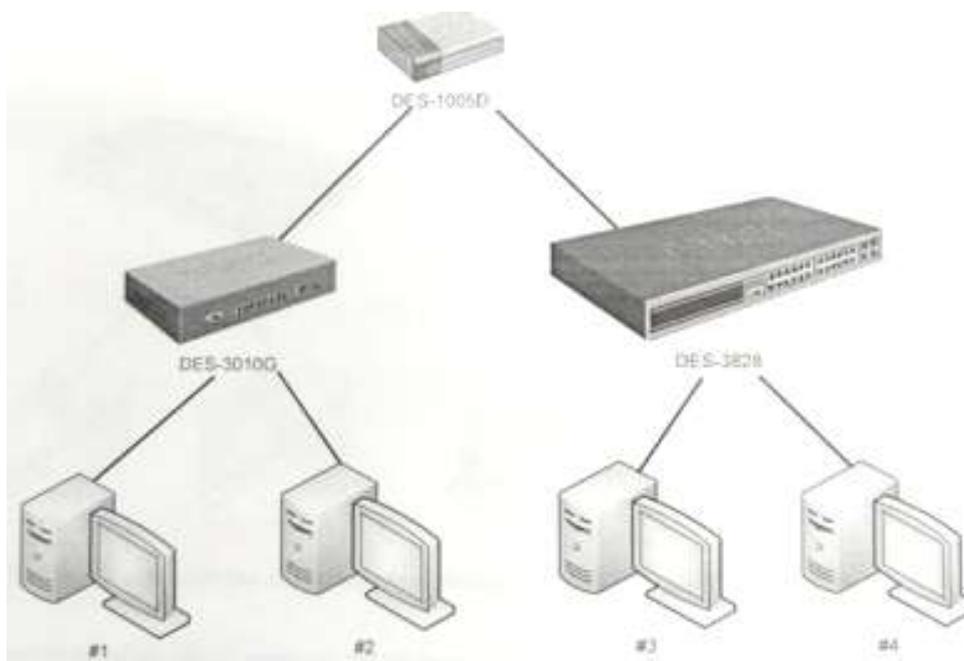


Рисунок 4 -Топология сети

2. Изучите разделы «Ограничение количества управляющих компьютеров», «Настройка безопасности индивидуального порта» и «Технология фильтрации IP-MAC Binding» теоретического пособия.
3. Изучите раздел «Security» (меню «Trusted Hosts»).
4. Настройте коммутаторы таким образом, чтобы ими могли управлять только машины #1 и #3.
5. Проверьте выполненные настройки.
6. Изучите раздел «Security» (меню «Port Security»).
7. Очистите таблицы коммутации на всех коммутаторах.
8. С машин #1 и #2 «пропингуйте» машину #3.
9. Убедитесь, что в таблицах коммутации не присутствует аппаратного адреса машины #4.
10. Заблокируйте на обоих коммутаторах таблица коммутации в режиме Permanent.

11. Попробуйте осуществить взаимодействие с 4-ым компьютером с любого компьютера. Объясните полученный результат.
12. Изучите раздел. «Administration» (меню «IP-MAC Binding»).
13. Сбросьте блокировку таблиц коммутации.
14. Используя технологию IP-Mac Binding, настройте на коммутаторах фильтры таким образом, чтобы в сети могли работать только машины #1 и #3.
15. Сбросьте настройки коммутаторов в заводские и перезагрузите его.

Форма представления результата: Отчет о проделанной работе, выполненная работа.

Критерии оценки:

Оценка «отлично» ставится, если задание выполнено верно.

Оценка «хорошо» ставится, если ход выполнения задания верный, но была допущена одна или две ошибки, приведшие к неправильному ответу.

Оценка «удовлетворительно» ставится, если в работе не получен ответ и приведено неполное выполнение задания, но ход выполнения задания.

Оценка «неудовлетворительно» ставится, если задание не выполнено.

Тема 1.2 Безопасность беспроводных локальных сетей

Лабораторное занятие № 5

Настройка беспроводной сети WPA

Цель работы: Получение навыков построения сетей Wi-Fi с использованием механизма шифрования WPA.

Выполнение работы способствует формированию:

У1. Настраивать стек протоколов TCP/IP и использовать встроенные утилиты операционной системы для диагностики работоспособности сети.

У2. Использовать программно-аппаратные средства технического контроля.

Материальное обеспечение:

учебно-лабораторный стенд «Сетевая безопасность»

Порядок выполнения работы:

1. Постройте сеть, топология которой представлена на рисунке 5.

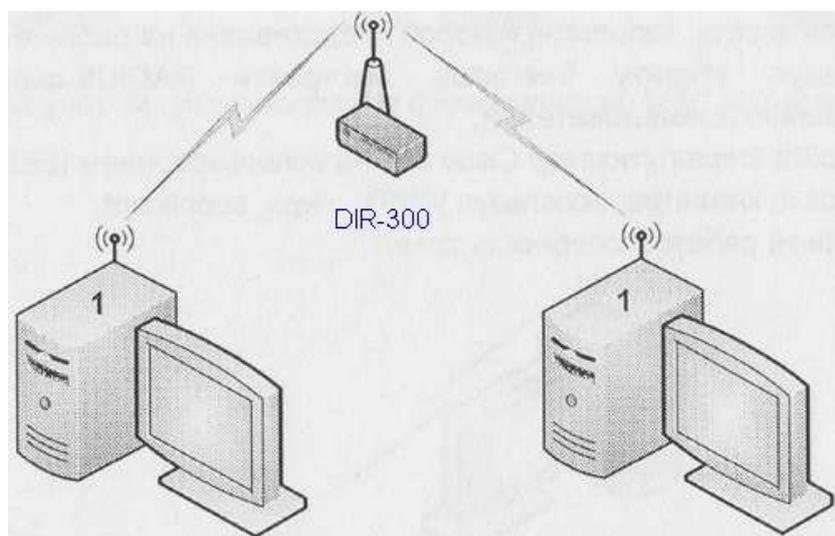


Рисунок 5 – Топология сети

2. Используйте утилиту `wpa_supplicant`, настройте защищенную сеть с использованием аутентификации WPA и системой шифрования TKIP.
3. Используя `ssh`, сравните полезную пропускную способность канала до и после использования WPA.

Примечание –

Для проверки скорости соединения воспользуйтесь SSH

1. На первом компьютере задайте пароль пользователю `root: passwd`.
2. На втором компьютере для копирования файла выполните команду:

`scp ip_адрес_компьютера_1: путь_к_файлу /dev/null`

Эта команда скопирует указанный файл с первого компьютера на второй, причем файл не будет сохранен на диске, что позволит оценить реальную пропускную способность сети. Скорость передачи данных будет указана в выводе команды `scp`.

4. Используя утилиту `tcdump` осуществите перехват пакетов. Изучите содержимое перехваченных пакетов до и после применения WPA.
5. Используя утилиту `wpa_supplicant`, настройте защищенную сеть с использованием аутентификации WPA2/PSK и системой шифрования TKIP.

6. Используя ssh, сравните полезную пропускную способность канала до и после использования WPA2/PSK.
7. Используя утилиту wpa_supplicant, настройте защищенную сеть с использованием аутентификации WPA2/PSK и системой шифрования AES.
8. Используя ssh, сравните полезную пропускную способность канала с использованием системы шифрования TKIP с системой шифрования AES.

Форма представления результата: Отчет о проделанной работе, выполненная работа.

Критерии оценки:

Оценка «отлично» ставится, если задание выполнено верно.

Оценка «хорошо» ставится, если ход выполнения задания верный, но была допущена одна или две ошибки, приведшие к неправильному ответу.

Оценка «удовлетворительно» ставится, если в работе не получен ответ и приведено неполное выполнение задания, но ход выполнения задания.

Оценка «неудовлетворительно» ставится, если задание не выполнено.

Тема 1.2. Безопасность беспроводных локальных сетей

Лабораторное занятие № 6

Беспроводная сеть с точкой доступа

Цель: Получение навыков построения сетей беспроводной сети с точкой доступа.

Выполнение работы способствует формированию:

У1. Настраивать стек протоколов TCP/IP и использовать встроенные утилиты операционной системы для диагностики работоспособности сети.

У2. Использовать программно-аппаратные средства технического контроля

Материальное обеспечение:

рабочее место, оснащенное ПК;
инструкция для работы.

Задание:

1 Построить беспроводную сеть с точкой доступа

Порядок выполнения работы:

1 Построить схему сети

2 Выполнить настройки точки доступа

3 Проверить работоспособность сети

Ход работы:

1. Постройте схему сети, представленную на рисунке 6.

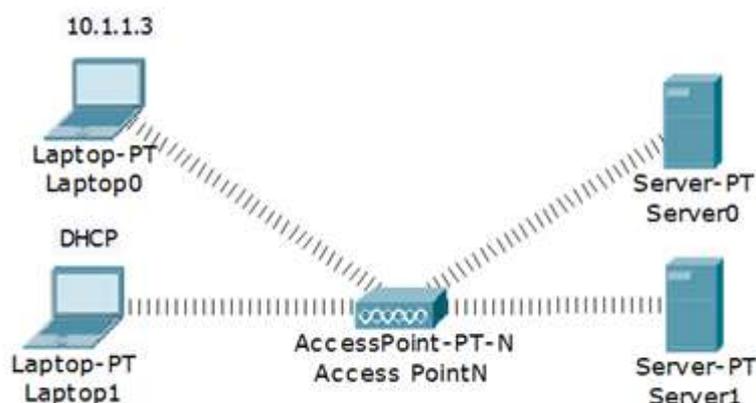


Рисунок 6 – Схема сети

Точка доступа в английской терминологии – Wireless Access Point.

2. Настроить точки доступа, по рис. 7.

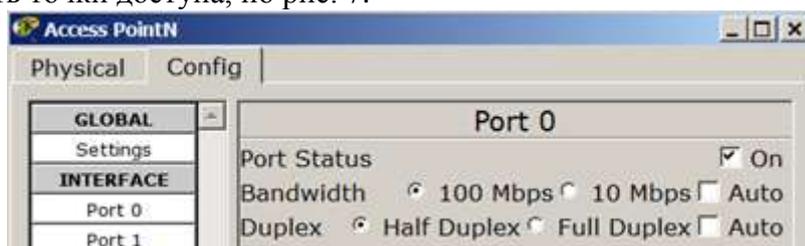


Рисунок 7 - Настройки точки доступа

3. Статическая настройка ноутбука (рисунок 8).

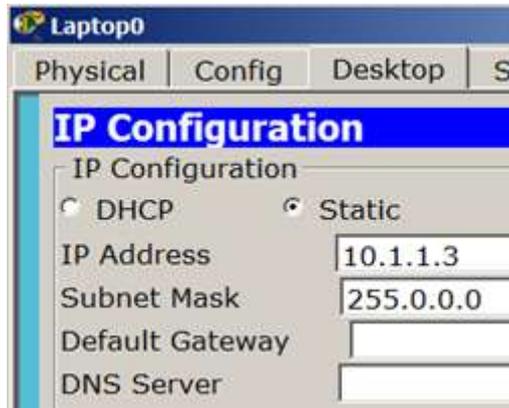


Рисунок 8 - Задаем IP адрес для L0

4. Динамическая настройка ноутбука (рисунок 9).

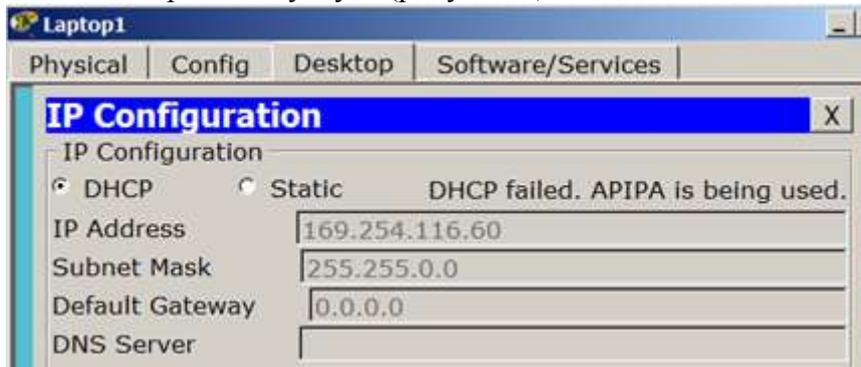


Рисунок 9 - Включаем переключатель DHCP для L1

5. Настройка серверов (рисунок 10).



Рисунок 10 - Сервера настроены по умолчанию

6. Точку доступа POINT N можете заменить на POINT 0, при этом настройки хостов можно не менять (рисунок 11).

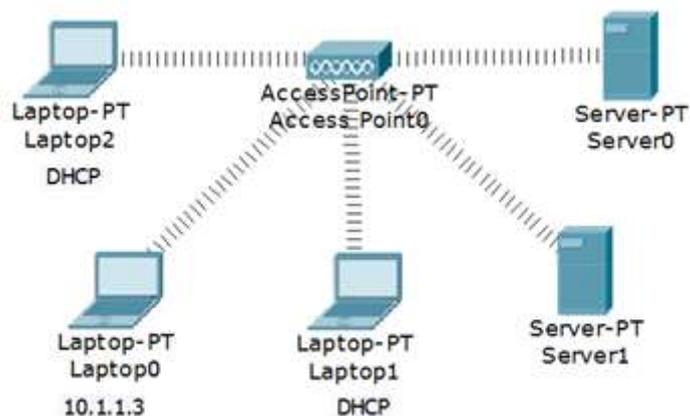


Рисунок 11 - Беспроводная связь установлена

Форма представления результата: отчет о проделанной работе, выполненная работа.

Критерии оценки:

Оценка «отлично» ставится, если задание выполнено верно.

Оценка «хорошо» ставится, если ход выполнения задания верный, но была допущена одна или две ошибки, приведшие к неправильному ответу.

Оценка «удовлетворительно» ставится, если в работе не получен ответ и приведено неполное выполнение задания, но ход выполнения задания.

Оценка «неудовлетворительно» ставится, если задание не выполнено.

Тема 1.2. Безопасность беспроводных локальных сетей

Лабораторное занятие № 7

Беспроводная сеть между офисами

Цель: Получение навыков построения сетей беспроводной сети.

Выполнение работы способствует формированию:

У1. Настраивать стек протоколов TCP/IP и использовать встроенные утилиты операционной системы для диагностики работоспособности сети.

У2. Использовать программно-аппаратные средства технического контроля

Материальное обеспечение:

рабочее место, оснащенное ПК;
инструкция для работы.

Задание:

1 Построить беспроводную сеть между офисами

Порядок выполнения работы:

1 Построить схему сети.

2 Выполнить настройки.

3 Проверить работоспособность сети.

Ход работы:

Настроить следующую беспроводную сеть (рисунок 12).

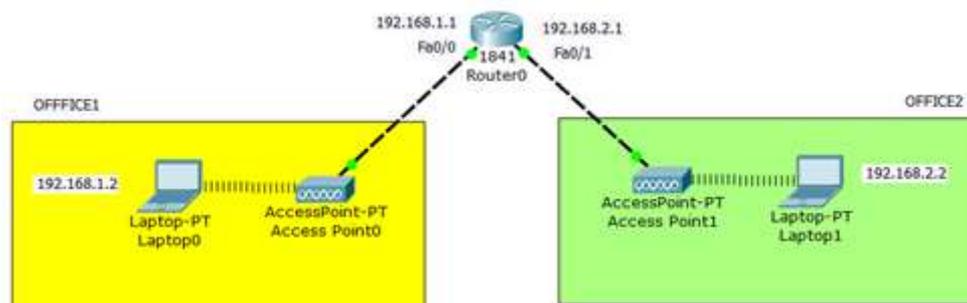


Рисунок 12 - WI-FIсеть между офисами

Снабжаем ноутбука wi-fi адаптерами WPC300N. Настройки обоих ноутбуков аналогичны (рисунок 13).

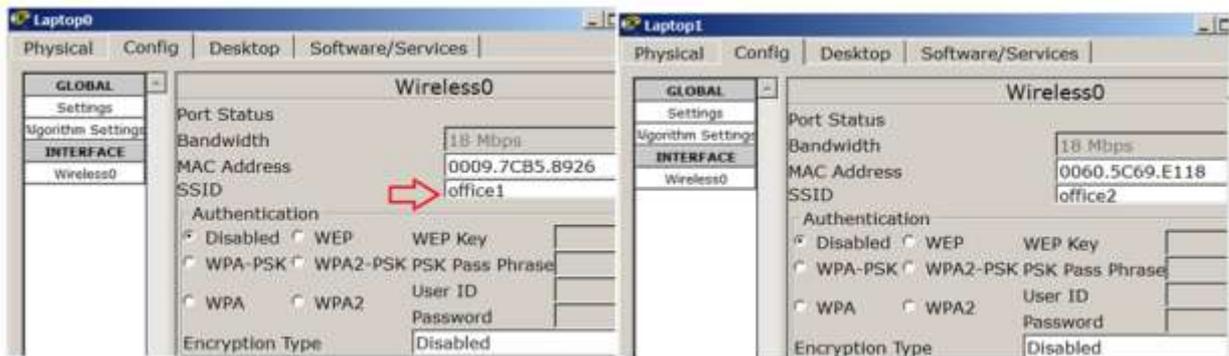


Рисунок 13 - Настройки ноутбуков

Примечание

Каждая беспроводная локальная сеть использует уникальное сетевое имя для идентификации сети. Это имя также называется идентификатором обслуживания сети - SSID. Когда вы будете устанавливать адаптер Wi-Fi, нужно будет указать SSID. Если вы хотите подключиться к существующей беспроводной сети, вы должны использовать имя этой сети. Имя может иметь длину до 32 символов и содержать буквы и цифры.

Помимо SSID на ноутбуках настраивается шлюз (рисунок 14).

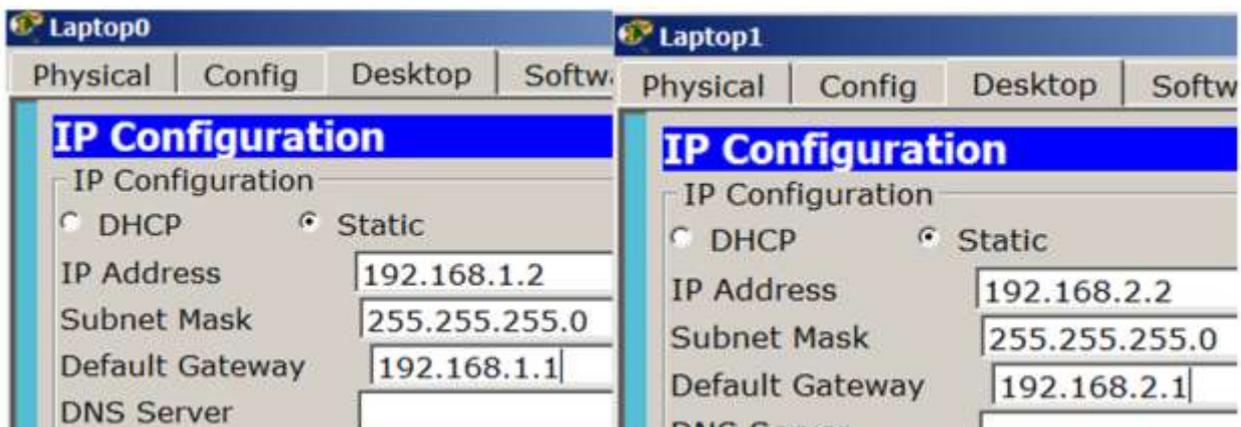


Рисунок 14 - На L0 и L1 указываем адрес шлюза

SSID задаем на обеих точках доступа (рисунок 15).

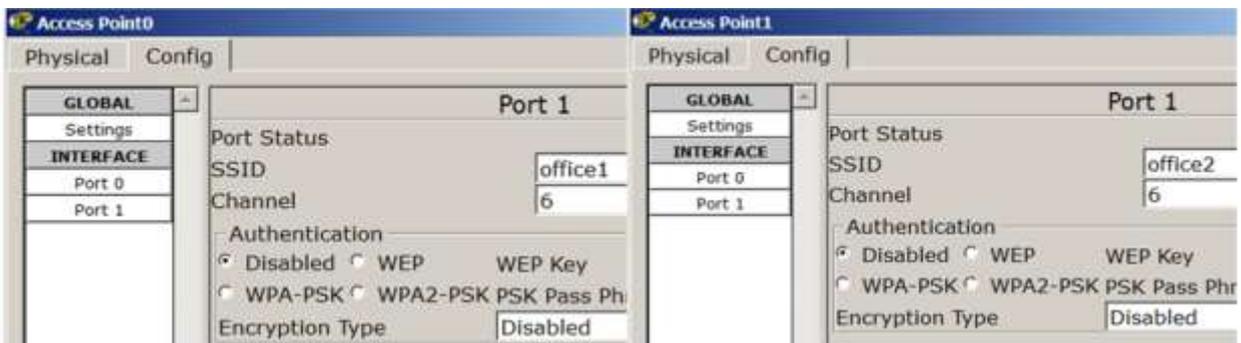
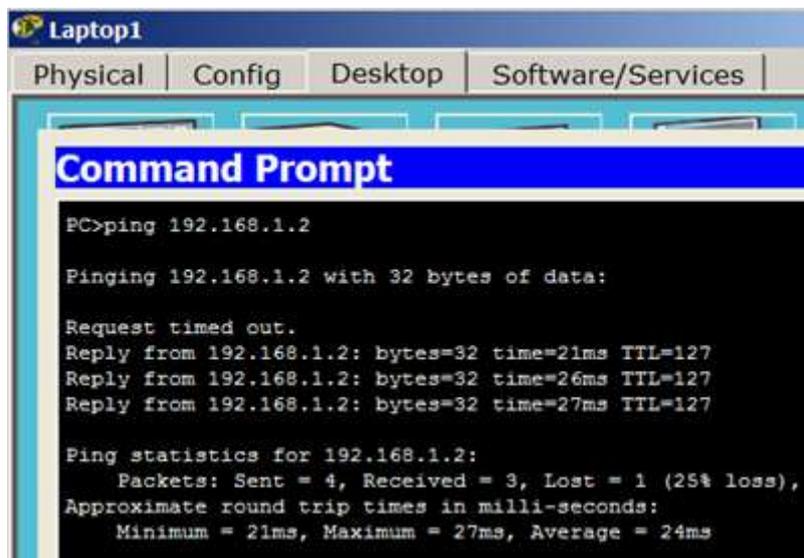


Рисунок 15 - Задаем SSID на точках доступа

Проверяем связь ПК из разных офисов (рисунок 16).



```
Laptop1
Physical | Config | Desktop | Software/Services

Command Prompt

PC>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.2: bytes=32 time=21ms TTL=127
Reply from 192.168.1.2: bytes=32 time=26ms TTL=127
Reply from 192.168.1.2: bytes=32 time=27ms TTL=127

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 21ms, Maximum = 27ms, Average = 24ms
```

Рисунок 16 - Связь L1 и L0 присутствует

Форма представления результата: отчет о проделанной работе, выполненная работа.

Критерии оценки:

Оценка «отлично» ставится, если задание выполнено верно.

Оценка «хорошо» ставится, если ход выполнения задания верный, но была допущена одна или две ошибки, приведшие к неправильному ответу.

Оценка «удовлетворительно» ставится, если в работе не получен ответ и приведено неполное выполнение задания, но ход выполнения задания.

Оценка «неудовлетворительно» ставится, если задание не выполнено.

Тема 1.2. Безопасность беспроводных локальных сетей Лабораторное занятие № 8

Настройка коммутуруемого WI-FI соединения

Цель: Получение навыков построения коммутуруемого WI-FI соединения.

Выполнение работы способствует формированию:

У1. Настраивать стек протоколов TCP/IP и использовать встроенные утилиты операционной системы для диагностики работоспособности сети.

У2. Использовать программно-аппаратные средства технического контроля

Материальное обеспечение:

рабочее место, оснащенное ПК;

инструкция для работы.

Задание:

1 Построить коммутуруемое WI-FI соединение

Порядок выполнения работы:

1 Построить схему сети.

2 Выполнить настройки.

3 Проверить работоспособность сети.

Ход работы:

Настройка коммутуруемого WI-FI соединения

Соберем и настроим сеть, изображенную на рисунок 17.

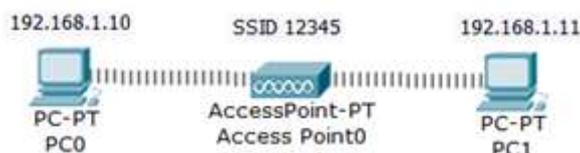


Рисунок 17 - WI-FI сеть

Сначала зададим имя сети (SSID) на точке доступа (рисунок 18).

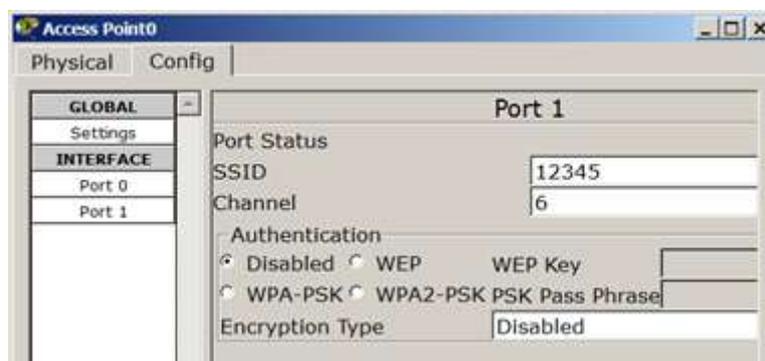


Рисунок 18 - Задаем SSID на точке доступа

В оба ПК вставляем беспроводной адаптер Linksys-WPM-300N (рисунок 19).

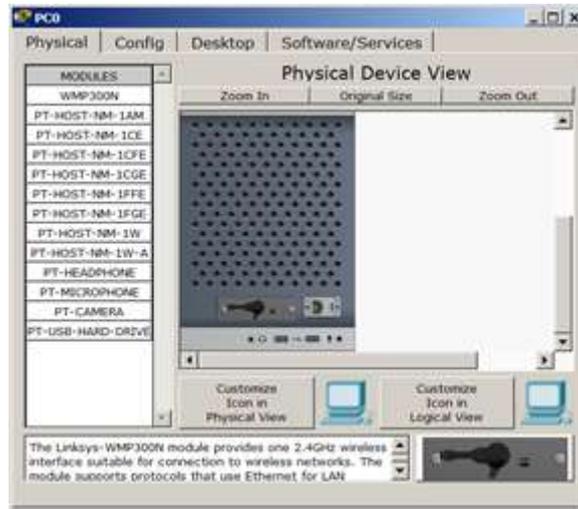


Рисунок 19 - Адаптер Linksys-WPM-300N вставлен в PC0

Устанавливаем связь точки доступа и PC0, для этого нажимаем на кнопку PC Wireless (рисунок 20).



Рисунок 20 - Нажимаем на кнопку PCWireless

Теперь открываем вкладку Connect и нажимаем на кнопку Connect (рисунок 21).

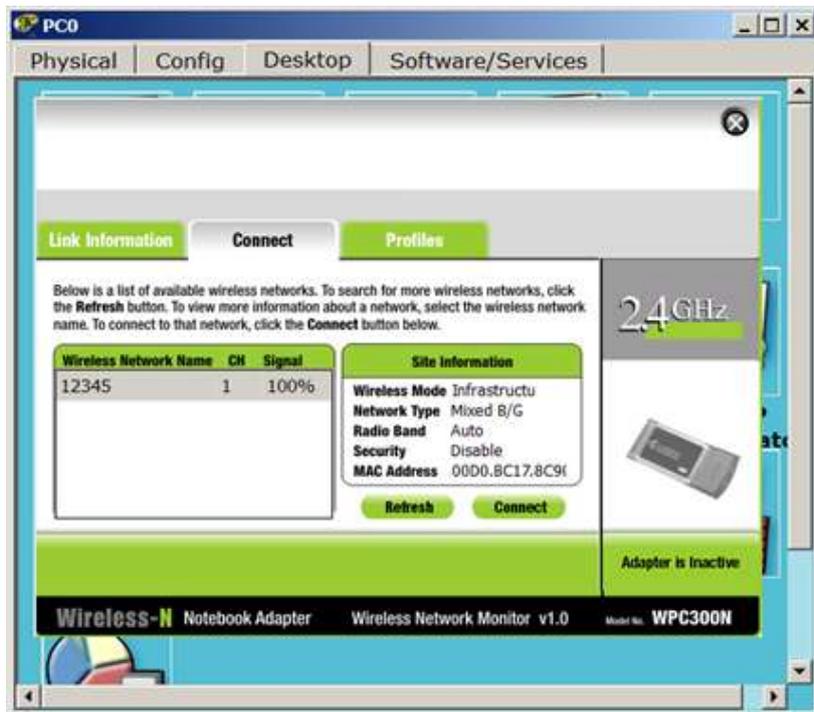


Рисунок 21 - Нажимаем на кнопку Connect и окно закрываем

В результате у нас получается динамическая связь PC0 и Access Point-PT (рисунок 22).



Рисунок 22 - Динамическая связь точки доступа и беспроводного адаптера

Меняем динамический адрес на статический (рисунок 23).



Рисунок 23 - Меняем динамический адрес на статический

Аналогично настраиваем PC1 и проверяем связь между ПК.

Форма представления результата: отчет о проделанной работе, выполненная работа.

Критерии оценки:

Оценка «отлично» ставится, если задание выполнено верно.

Оценка «хорошо» ставится, если ход выполнения задания верный, но была допущена одна или две ошибки, приведшие к неправильному ответу.

Оценка «удовлетворительно» ставится, если в работе не получен ответ и приведено неполное выполнение задания, но ход выполнения задания.

Оценка «неудовлетворительно» ставится, если задание не выполнено.

Тема 1.2. Безопасность беспроводных локальных сетей Лабораторное занятие № 9

Беспроводная сеть с беспроводным роутером

Цель работы: Получение навыков построения сетей Wi-Fi

Выполнение работы способствует формированию:

У1. Настраивать стек протоколов TCP/IP и использовать встроенные утилиты операционной системы для диагностики работоспособности сети.

У2. Использовать программно-аппаратные средства технического контроля.

Материальное обеспечение:

учебно-лабораторный стенд «Сетевая безопасность»

Задание:

1 Построить коммутируемое WI-FI соединение

Порядок выполнения работы:

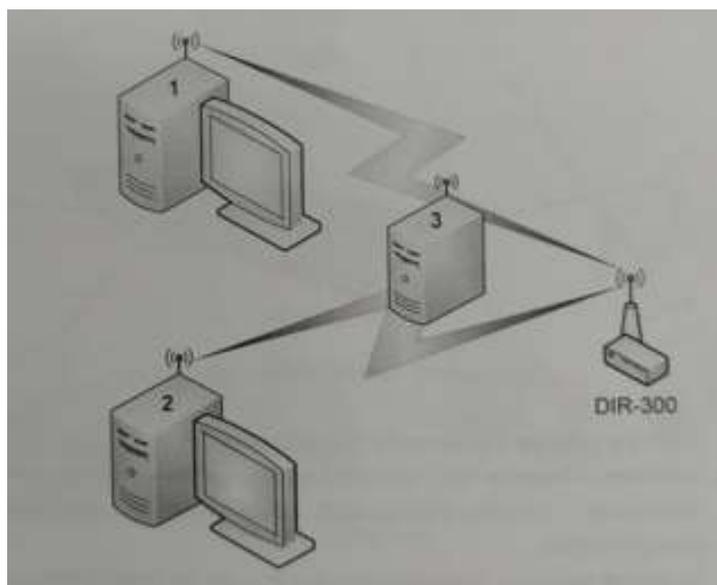
1 Построить схему сети.

2 Выполнить настройки.

3 Проверить работоспособность сети.

Порядок выполнения работы:

1. Постройте сеть, топология которой представлена на рисунке 24.



- Изучите раздел «Механизмы шифрования в беспроводных сетях» теоретического пособия.
- Включите точку доступа, настройте канал и имя сети. Включите внутренний DHCP-сервер. Включите шифрование WEP, используя 40-битный ключ.
- Ассоциируйте два компьютера с этой точкой доступа.
- Запустите на третьем компьютере утилиту «Airodump-ng» для перехвата пакетов.
- Выполните взаимодействие между компьютерами 1 и 2.
- Убедитесь (по экрану airodump-ng), что несколько пакетов с данными было перехвачено.
- Сгенерируйте файл словаря, содержащий несколько произвольных ключей и добавьте в конец файла заданный ключ. Длина словаря должна быть не меньше 10000 записей.

Скрипт для генерации находится на диске в каталоге /root/Desktop/Scripts/wep.

9. Используя полученный словарь и перехваченные пакеты выполните атаку на файл с перехваченными пакетами с помощью утилиты «WepAttack».
10. Выполните эти же действия, изменяя длину ключа и используя в качестве перехватчика Kismet вместо airodump. Варьируйте размер файла словаря, добавляя или удаляя записи. Сделайте вывод о влиянии длины ключа и размера словаря на скорость атаки.

Форма представления результата: Отчет о проделанной работе, выполненная работа.

Критерии оценки:

Оценка «отлично» ставится, если задание выполнено верно.

Оценка «хорошо» ставится, если ход выполнения задания верный, но была допущена одна или две ошибки, приведшие к неправильному ответу.

Оценка «удовлетворительно» ставится, если в работе не получен ответ и приведено неполное выполнение задания, но ход выполнения задания.

Оценка «неудовлетворительно» ставится, если задание не выполнено.

Тема 1.3. Принципы обеспечения безопасности сети Лабораторное занятие № 10

Подключение и основные настройки межсетевого экрана

Цель работы: Получение навыков настройки межсетевого экрана

Выполнение работы способствует формированию:

- У1. Настраивать стек протоколов TCP/IP и использовать встроенные утилиты операционной системы для диагностики работоспособности сети.
- У2. Использовать программно-аппаратные средства технического контроля.

Материальное обеспечение:

учебно-лабораторный стенд «Сетевая безопасность»

Задание:

- 1 Настроить межсетевой экран

Порядок выполнения работы:

- 1 Построить схему сети.
- 2 Выполнить настройки.
- 3 Проверить работоспособность сети.

Порядок выполнения работы:

1. Подключение к Cisco ASA

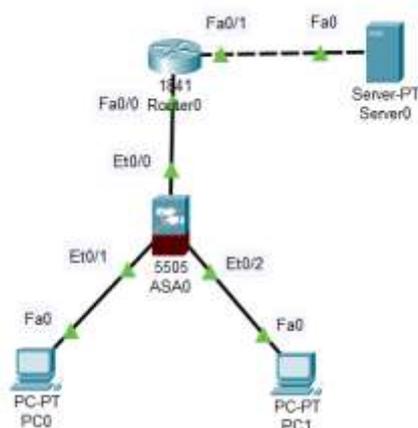


Рисунок 25 – Схема сети

Ciscoasa en

Password {пароль пустой Нажимаем <Enter>}

ciscoasa#show version {Смотрим что может ASA}

2. Проверка лицензии

ciscoasa#show run

ciscoasa#show running-config

Видно что DHCP на ASA преднастроен. Заходим на PC, ставим галку DHCP и компьютеры получают IP-адреса.

ciscoasa#conf t

ciscoasa(config)#enable password cisco

ciscoasa(config)#username admin password cisco

ciscoasa(config)#

Если набрать команду:

ciscoasa(config)#show run

то увидим, что пароли на enable и username зашифрованы

3. Настройка удаленного доступа к МЭ

Теперь нужно выбрать протокол, по которому будем осуществлять удаленное подключение.

```
ciscoasa(config)#ssh 192.168.1.0 255.255.255.0 inside
ciscoasa(config)#aaa authentication ssh console LOCAL
ciscoasa(config)#
```

Теперь не выходя из режима конфигурирования, мы можем воспользоваться командой

```
ciscoasa(config)#show run
```

Заходим на МЭ по SSH

```
C:\>ssh -l admin 192.168.1.1
```

```
Password: cisco
```

```
ciscoasa>
```

```
ciscoasa>en
```

```
Password: cisco
```

Введите команду:

```
ciscoasa#show run
```

Готово: SSH настроен

4 Настройка Security Level

Security Level – это уровень доверия. Чем больше Security Level тем выше доверие. **Настраиваем виланы.**

```
ciscoasa(config)#interface vlan 1
```

```
ciscoasa(config-if)#security-level 95
```

```
ciscoasa(config-if)#end
```

```
ciscoasa#
```

```
ciscoasa# conf t
```

```
ciscoasa(config)#int vlan2
```

```
ciscoasa(config-if)#ip address 210.210.0.2 255.255.255.252
```

```
ciscoasa(config-if)#no shutdown
```

```
ciscoasa(config-if)#exit
```

```
ciscoasa(config)#
```

Настраиваем роутер

```
Router>en
```

```
Router#conf t
```

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

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

```
Router(config-if)#ip ad
```

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

```
Router(config-if)#no sh
```

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

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

```
Router(config)#int fa0/1
```

```
Router(config-if)#ip ad
```

```
Router(config-if)#ip address 210.210.1.1 255.255.255.0
```

```
Router(config-if)#no sh
```

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

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

```
Router#
```

Настраиваем сервер

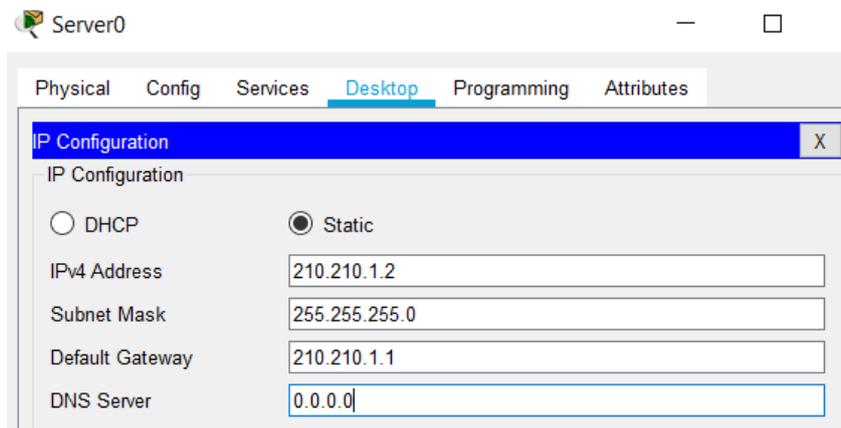


Рисунок 26 – Настройки сервера

5. Настройка маршрута по умолчанию

```
ciscoasa(config)#route outside 0.0.0.0 0.0.0.0 210.210.0.1
ciscoasa(config)#end
```

Пингуем сервер

ciscoasa#ping 210.210.1.2. Пинг проходит.

Пропишем маршрут на маршрутизаторе

```
Router(config)#ip route 192.168.1.0 255.255.255.0 210.210.0.2
Router(config)#end
Router#
```

Сохраним настройки

```
Router#wr mem
```

Пингуем с компьютера роутер

```
C:\>ping 210.210.0.1
```

Пинг не идет. Требуется настройка инспектирования трафика.

6. Настройка инспектирования трафика (Stateful Inspection)

```
ciscoasa(config)#class-map inspection_default
ciscoasa(config-cmap)#match default-inspection-traffic
ciscoasa(config-cmap)#exit
ciscoasa(config)#policy-map global_policy
ciscoasa(config-pmap)#class inspection_default
ciscoasa(config-pmap-c)#inspect icmp
ciscoasa(config-pmap-c)#exit
ciscoasa(config)#service-policy global_policy global
```

Сохраняем настройки

```
ciscoasa(config)#wr mem
```

Опять пингуем роутер

```
C:\>ping 210.210.0.1
```

Пинг проходит.

Пингуем сервер

```
C:\>ping 210.210.1.2
```

Пинг проходит.

Пингуем компьютер с сервера

Пинг не проходит. ASA отбрасывает пакет.

Проверяем веб-сервер

Для этого на компьютере заходи в веб браузер и набираем <http://210.210.1.2>.

Веб браузер не работает.

Добавляем на ASA инспектирование http.

```

ciscoasa(config)#policy-map global_policy
ciscoasa(config-pmap)#class inspection_default
ciscoasa(config-pmap-c)#inspec
ciscoasa(config-pmap-c)#inspect http
ciscoasa(config-pmap-c)#end
ciscoasa#

```

Опть проверяем веб-сервер
 Веб браузер заработал.

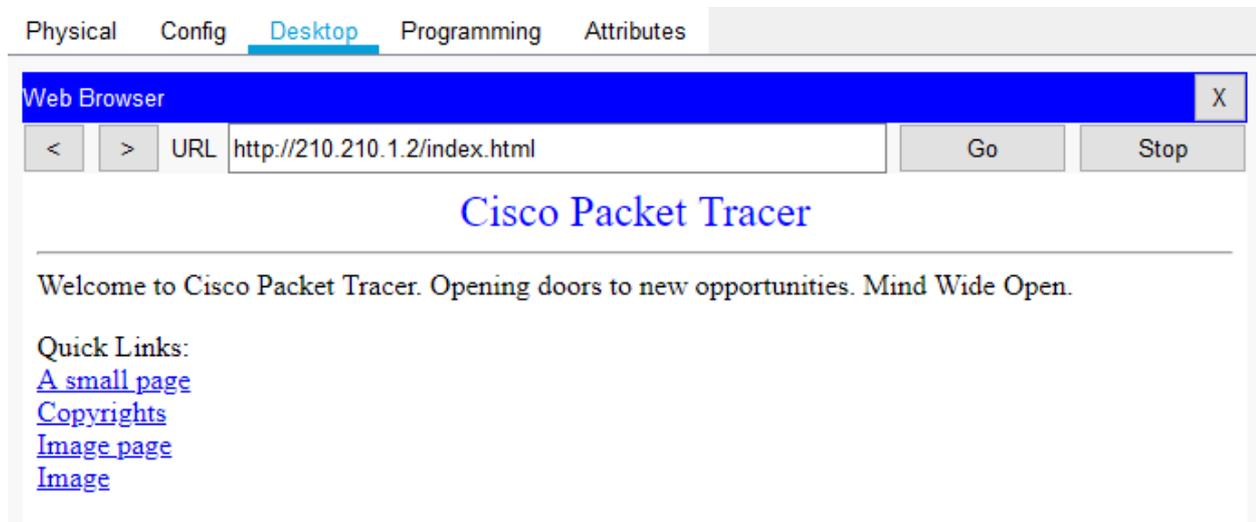


Рисунок 27 – Web Browser

7. Настройка NET

Удаляем маршрут на роутере

```

Router(config)#no ip route 192.168.1.0 255.255.255.0 210.210.0.2
Router(config)#end
Router#

```

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

Сохраним настройки

```

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

```

На компьютерах пинг сервера 210.210.1.2 пропал.

Настраиваем NAT

```

ciscoasa(config)#object network FOR-NAT
ciscoasa(config-network-object)#subnet 192.168.1.0 255.255.255.0
ciscoasa(config-network-object)#nat (inside,outside) dynamic interface
ciscoasa(config-network-object)#end
ciscoasa#wr mem
Building configuration...
Cryptochecksum: 1f3251dc 58e24059 618f3bdf 695f2396

```

1233 bytes copied in 1.901 secs (648 bytes/sec)

```

[OK]
ciscoasa#

```

NAT настроен.

Пингуем сервер

```

Ping 210.210.1.2

```

Пинг проходит.

Проверяем на ASA

```
ciscoasa#show nat
```

```
Auto NAT Policies (Section 2)
```

```
1 (inside) to (outside) source dynamic FOR-NAT interface
```

```
translate_hits = 4, untranslate_hits = 4
```

```
ciscoasa#
```

настройка межсетевого экрана ASA завершена.

Форма представления результата: Отчет о проделанной работе, выполненная работа.

Критерии оценки:

Оценка «отлично» ставится, если задание выполнено верно.

Оценка «хорошо» ставится, если ход выполнения задания верный, но была допущена одна или две ошибки, приведшие к неправильному ответу.

Оценка «удовлетворительно» ставится, если в работе не получен ответ и приведено неполное выполнение задания, но ход выполнения задания.

Оценка «неудовлетворительно» ставится, если задание не выполнено.

Тема 1.3. Принципы обеспечения безопасности сети Лабораторное занятие № 11

Настройка сервера AAA

Цель работы: получение навыков построения защищенных Wi-Fi сетей с использованием RADIUS-сервера и фильтрации по MAC-адресам.

Выполнение работы способствует формированию:

У1. Настраивать стек протоколов TCP/IP и использовать встроенные утилиты операционной системы для диагностики работоспособности сети.

У2. Использовать программно-аппаратные средства технического контроля.

Материальное обеспечение:

учебно-лабораторный стенд «Сетевая безопасность»

Порядок выполнения работы:

1. Постройте сеть, топология которой представлена на рисунке 28.
2. Используя утилиту freeradius, настройте RADIUS-сервер и создайте двух произвольных пользователей.
3. Настройте маршрутизатор DIR-300 на использование IEEE 802.1x.
4. Настройте клиентов, используя утилиту wpa_supplicant.
5. Проверьте работоспособность сети.

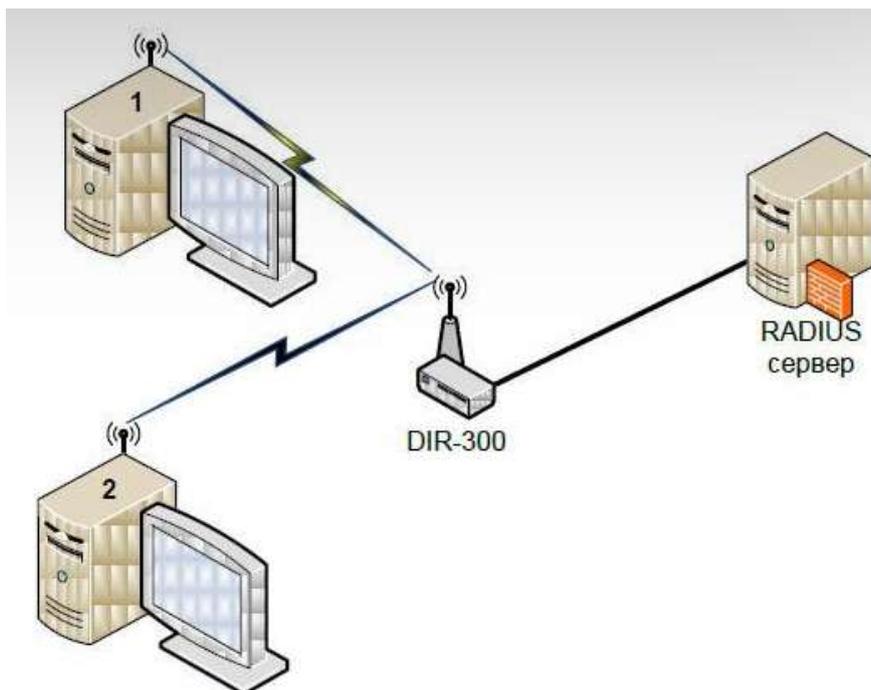


Рисунок 28 – Топология сети

6. Соберите топологию, представленную на рисунке 29.
7. К точке доступа 1 разрешить подключение компьютеров 1 и 2 с помощью разрешенных списков MAC-адресов. К точке доступа 2 запретить подключение с компьютера А с помощью запрещенных списков MAC-адресов.
8. Проверьте правильность выполненных настроек.

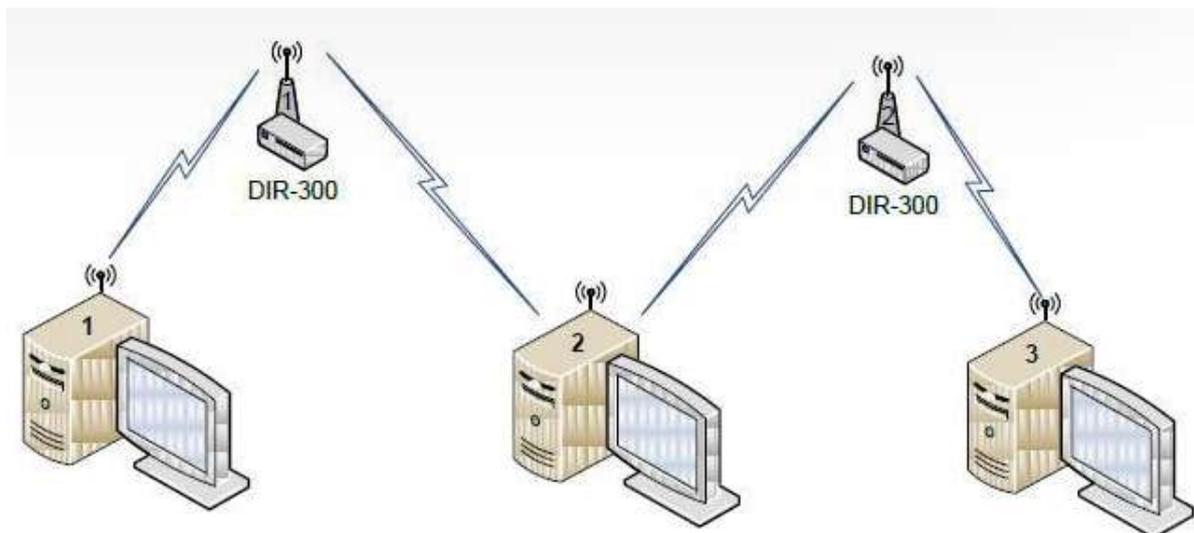


Рисунок 29 - Топология сети

Форма представления результата: Отчет о проделанной работе, выполненная работа.

Критерии оценки:

Оценка «отлично» ставится, если задание выполнено верно.

Оценка «хорошо» ставится, если ход выполнения задания верный, но была допущена одна или две ошибки, приведшие к неправильному ответу.

Оценка «удовлетворительно» ставится, если в работе не получен ответ и приведено неполное выполнение задания, но ход выполнения задания.

Оценка «неудовлетворительно» ставится, если задание не выполнено

Тема 1.3. Принципы обеспечения безопасности сети Лабораторное занятие № 12

Настройка NAT

Цель работы: получение навыков настройки NAT.

Выполнение работы способствует формированию:

- У1. Настраивать стек протоколов TCP/IP и использовать встроенные утилиты операционной системы для диагностики работоспособности сети.
- У2. Использовать программно-аппаратные средства технического контроля.

Материальное обеспечение:

учебно-лабораторный стенд «Сетевая безопасность»

Задание:

- 1 Настроить NAT.

Порядок выполнения работы:

- 1 Построить схему сети.
- 2 Выполнить настройки.
- 3 Проверить работоспособность сети.

Ход работы:

Здание 1. Настройка статического NAT

NAT (Network Address Translation) — трансляция сетевых адресов, технология, которая позволяет преобразовывать (изменять) IP адреса и порты в сетевых пакетах. NAT используется чаще всего для осуществления доступа устройств из локальной сети предприятия в Интернет, либо наоборот для доступа из Интернет на какой-либо ресурс внутри сети. Локальная сеть предприятия строится на частных IP адресах:

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз
PC1	Fa0	192.168.1.2/24	255.255.255.0	192.168.1.1
PC2	Fa0	192.168.2.2/24	255.255.255.0	192.168.2.1
PC3	Fa0	192.168.3.2/24	255.255.255.0	192.168.3.1

- 10.0.0.0 — 10.255.255.255 (10.0.0.0/255.0.0.0 (/8))
- 172.16.0.0 — 172.31.255.255 (172.16.0.0/255.240.0.0 (/12))
- 192.168.0.0 — 192.168.255.255 (192.168.0.0/255.255.0.0 (/16))

Эти адреса не маршрутизируются в Интернете, и провайдеры должны отбрасывать пакеты с такими IP адресами отправителей или получателей. Для преобразования частных адресов в Глобальные (маршрутизируемые в Интернете) применяют NAT.

Новый термин

NAT — технология трансляции сетевых адресов, т.е. подмены адресов (или портов) в заголовке IP-пакета. Другими словами, пакет, проходя через маршрутизатор, может поменять свой адрес источника и/или назначения. Подобный механизм служит для обеспечения доступа из LAN, где используются частные IP-адреса, в Internet, где используются глобальные IP-адреса.

Существует три вида трансляции *Static NAT*, *Dynamic NAT*, *Overloading (PAT)*.

– **Static NAT (статический NAT)** осуществляет преобразование IP адреса один к одному, то есть сопоставляется один адрес из внутренней сети с одним адресом из внешней сети. Иными словами, при прохождении через маршрутизатор, адрес(а) меняются на строго заданный адрес, один-к-одному (Например, 10.1.1.5 всегда заменяется на 11.1.1.5 и обратно). Запись о такой трансляции хранится неограниченно долго, пока есть соответствующая строка в конфигурации роутера.

– **Dynamic NAT (динамический NAT)** производит преобразование внутреннего адреса/ов в один из группы внешних адресов. То есть, перед использованием динамической трансляции, нужно задать *pat*-пул внешних адресов. В этом случае при прохождении через маршрутизатор, новый адрес выбирается динамически из некоторого диапазона адресов, называемого пулом (*pool*). Запись о трансляции хранится некоторое время, чтобы ответные пакеты могли быть доставлены адресату. Если в течение некоторого времени трафик по этой трансляции отсутствует, трансляция удаляется и адрес возвращается в пул. Если требуется создать трансляцию, а свободных адресов в пуле нет, то пакет отбрасывается. Иными словами, хорошо бы, чтобы число внутренних адресов было ненамного больше числа адресов в пуле, иначе высока вероятность проблем с выходом в WAN.

– **Overloading(или PAT)** позволяет преобразовывать несколько внутренних адресов в один внешний. Для осуществления такой трансляции используются порты, поэтому такой NAT называют **PAT (Port Address Translation)**. С помощью PAT можно преобразовывать внутренние адреса во внешний адрес, заданный через пул или через адрес на внешнем интерфейсе.

Задание 1. Статическая трансляция адресов NAT

На рисунке 30 имеется внешний адрес 20.20.20.20 (внешний интерфейс *fa0/1*) и внутренняя сеть 10.10.10.0 (внутренний интерфейс *fa0/0*). Нужно настроить NAT. Предполагается, что адреса уже прописаны, и сеть поднята (рабочая).

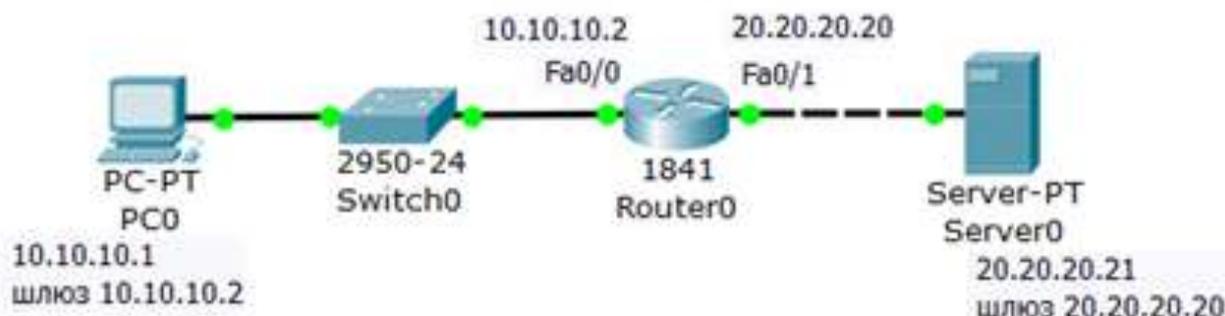


Рисунок 30 - Схема сети

На R0 добавляем *access-list*, разрешаем все (*any*)

Разрешаем весь трафик, то есть, любой IP адрес (рисунок 4.2).

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 1 permit any
Router(config)#ip nat inside source list 1 interface fa 0/1 overload
Router(config)#
```

Рисунок 4.2 - Составляем лист допуска

Создаем правило трансляции

Теперь настроим трансляцию на интерфейсах (на внутреннем inside, на внешнем – outside), то есть, для R0 указываем внутренний и внешний порты (рисунок 4.3).

```
Router(config)#int fa 0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#int fa 0/1
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#
```

Рисунок 4.3 - Для R0 назначаем внутренний и внешний порты

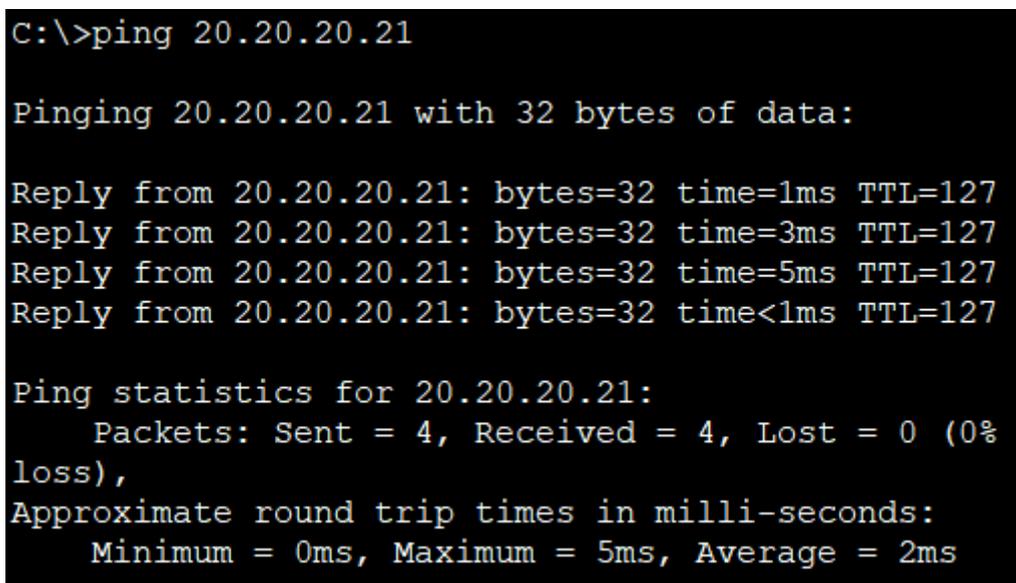
Выходим из режима глобального конфигурирования и записываем настройки роутера в микросхему памяти (рисунок 4.4).

```
Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#sh ip nat translations
Router#wr mem
Building configuration...
[OK]
Router#
```

Рисунок 4.4 - Сохраняем настройки в ОЗУ

Проверяем работу сети (просмотр состояния таблицы NAT)

С PC0 пингуем провайдера и убеждаемся, что PC1 и сервер могут общаться (рисунок 31).



```
C:\>ping 20.20.20.21

Pinging 20.20.20.21 with 32 bytes of data:

Reply from 20.20.20.21: bytes=32 time=1ms TTL=127
Reply from 20.20.20.21: bytes=32 time=3ms TTL=127
Reply from 20.20.20.21: bytes=32 time=5ms TTL=127
Reply from 20.20.20.21: bytes=32 time<1ms TTL=127

Ping statistics for 20.20.20.21:
    Packets: Sent = 4, Received = 4, Lost = 0 (0%
loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 5ms, Average = 2ms
```

Рисунок 31 - Из внутренней сети пингуем внешнюю сеть

Для просмотра состояния таблицы NAT, одновременно с пингом используйте команду **Router#sh ip nat translations** (я запустил пинг с машины 10.10.10.1, т.е., с PC1 на адрес 20.20.20.21, т.е., на S0) – рисунок 32.

```
Router>sh ip nat translations
Pro  Inside global      Inside local        Outside local       Outside global
icmp 20.20.20.20:37     10.10.10.1:37      20.20.20.21:37     20.20.20.21:37
icmp 20.20.20.20:38     10.10.10.1:38      20.20.20.21:38     20.20.20.21:38
icmp 20.20.20.20:39     10.10.10.1:39      20.20.20.21:39     20.20.20.21:39

Router>
```

Рисунок 32 - Вовремя пинга просматриваем состояние таблицы NAT

Вопрос !

Если в схему добавить PC1 (рисунок 33), то будет ли работать статический NAT между ним и S0?

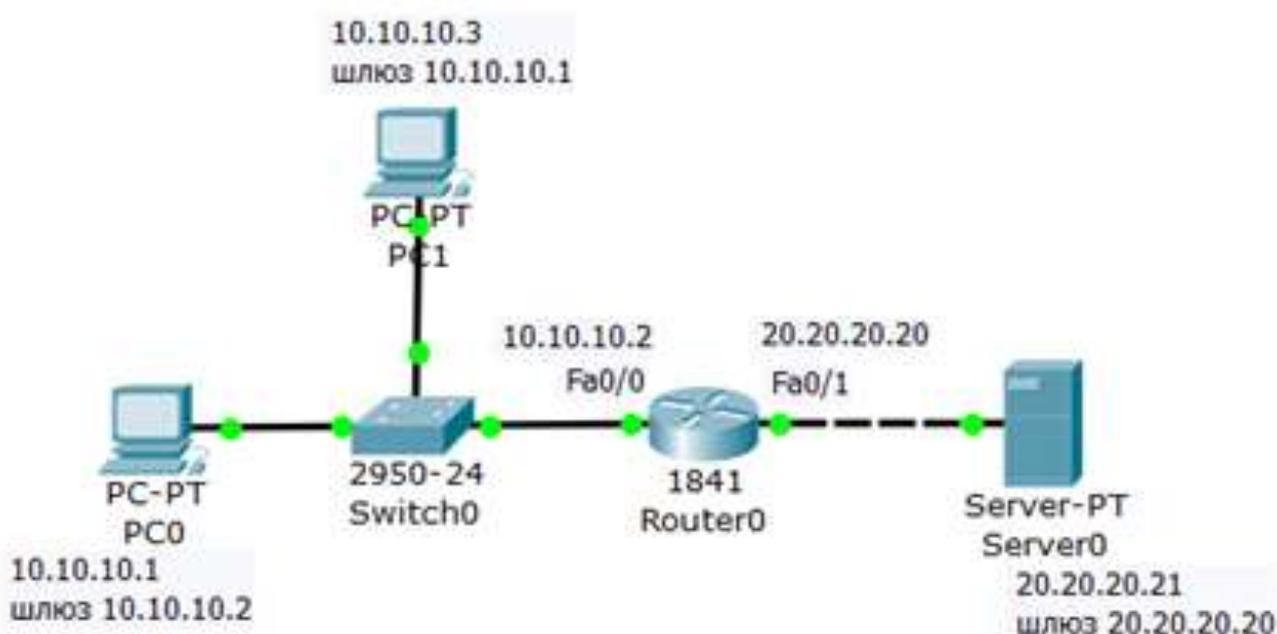


Рисунок 33 - Задание для самостоятельной работы

Задание 2. Настройка статического NAT

Статический NAT - сопоставляет один NAT inside (внутренний=частный локальный ip-адрес) с одним NAT outside (глобальным=публичным внешним ip-адресом) – рисунок 34. Здесь ISP (Internet Service Provider) - поставщик Интернет-услуг (Интернет-провайдер).

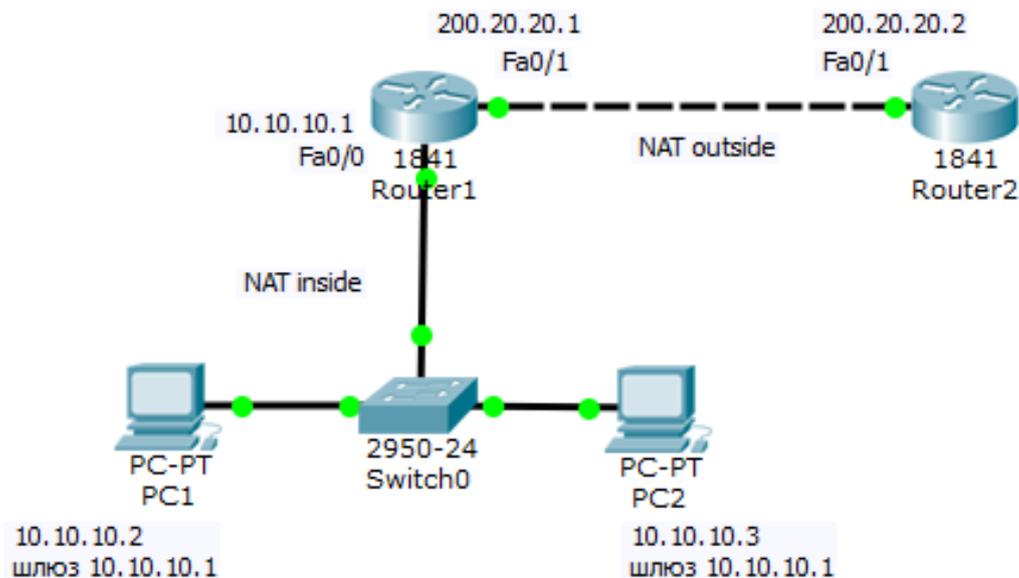


Рисунок 34 - Схема сети

Алгоритм настройки R1

Ниже приведена последовательность команд конфигурирования маршрутизатора R1 по шагам.

Шаг 1. Настройка дефолта на R1

```
R1(config)# ip route 0.0.0.0 0.0.0.0 200.20.20.2
```

Шаг 2. Настройка внутреннего интерфейса в отношении NAT

```
R1(config)# interface fastethernet 0/0
```

```
R1(config-if)# ip nat inside
```

Шаг 3. Настройка внешнего интерфейса в отношении NAT

```
R1(config)# interface fastethernet 0/1
```

```
R1(config-if)# ip nat outside
```

Шаг 4. Настройка сопоставления ip-адресов.

```
R1(config)# ip nat inside source static 10.10.10.2 200.10.21.5
```

В результате этой команды ip-адресу 200.10.21.5 всегда будет соответствовать внутренний ip-адрес 10.10.10.2, т.е. если мы будем обращаться к адресу 200.10.21.5 то отвечать будет PC1. Полный листинг команд приведен на рисунке 35.

```
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 0.0.0.0 0.0.0.0 200.20.20.2
Router(config)#interface fastethernet 0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface fastethernet 0/1
Router(config-if)#ip nat outside
Router(config-if)#ip nat inside source static 10.10.10.2 200.10.21.5
Router(config)#exit
Router#
```

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

Router#

Рисунок 35 - Полный листинг команд по настройке R1

Команды для проверки работы NAT

Проверим связь PC1 и R2 (рисунок 36).

```
Packet Tracer PC Command Line 1.0
PC>ping 200.20.20.2

Pinging 200.20.20.2 with 32 bytes of data:

Reply from 200.20.20.2: bytes=32 time=0ms TTL=254

Ping statistics for 200.20.20.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>|
```

Рисунок 36 - PC1 видит R2

Проверим, что R1 видит соседние сети (рисунок 37).

```
Router#ping 10.10.10.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/2/7 ms

Router#ping 200.20.20.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.20.20.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/5 ms

Router#|
```

Рисунок 37 - R1 видит PC1 и R2

Проверим механизм работы статического NAT: команда **show ip nat translations** выводит активные преобразования, а команда **show ip nat statistics** выводит статистику по NAT преобразованиям (рисунок 38).

```
Router#show ip nat translations
Pro Inside global      Inside local      Outside local     Outside global
icmp 200.10.21.5:33    10.10.10.2:33    200.20.20.2:33   200.20.20.2:33
icmp 200.10.21.5:34    10.10.10.2:34    200.20.20.2:34   200.20.20.2:34
icmp 200.10.21.5:35    10.10.10.2:35    200.20.20.2:35   200.20.20.2:35
icmp 200.10.21.5:36    10.10.10.2:36    200.20.20.2:36   200.20.20.2:36
--- 200.10.21.5        10.10.10.2        ---                ---
```

```
Router#show ip nat statistics
Total translations: 1 (1 static, 0 dynamic, 0 extended)
Outside Interfaces: FastEthernet0/1
Inside Interfaces: FastEthernet0/0
Hits: 7 Misses: 30
Expired translations: 20
Dynamic mappings:
```

Рисунок 38 - Проверка механизма работы статического NAT

Из иллюстрации видим, что глобальному ip-адресу 200.10.21.5 соответствует локальный ip-адрес 10.10.10.2, а также, какой интерфейс является внешним, а какой -внутренним.

Форма представления результата: Отчет о проделанной работе, выполненная работа.

Критерии оценки:

Оценка «отлично» ставится, если задание выполнено верно.

Оценка «хорошо» ставится, если ход выполнения задания верный, но была допущена одна или две ошибки, приведшие к неправильному ответу.

Оценка «удовлетворительно» ставится, если в работе не получен ответ и приведено неполное выполнение задания, но ход выполнения задания.

Оценка «неудовлетворительно» ставится, если задание не выполнено

Тема 1.3. Принципы обеспечения безопасности сети Лабораторное занятие № 13

Виртуальные частные сети

Цель работы: изучение протокола IPSec и способа его настройки в ОС Linux и на брандмауэре D-Link DFL-800.

Выполнение работы способствует формированию:

У1. Настраивать стек протоколов TCP/IP и использовать встроенные утилиты операционной системы для диагностики работоспособности сети.

У2. Использовать программно-аппаратные средства технического контроля.

Материальное обеспечение:

учебно-лабораторный стенд «Сетевая безопасность»

Задание:

- 1 Построить виртуальные частные сети

Порядок выполнения работы:

- 1 Построить схему сети.
- 2 Выполнить настройки.
- 3 Проверить работоспособность сети.

Ход работы:

1. Соберите топологию сети, представленную на рисунке 39.

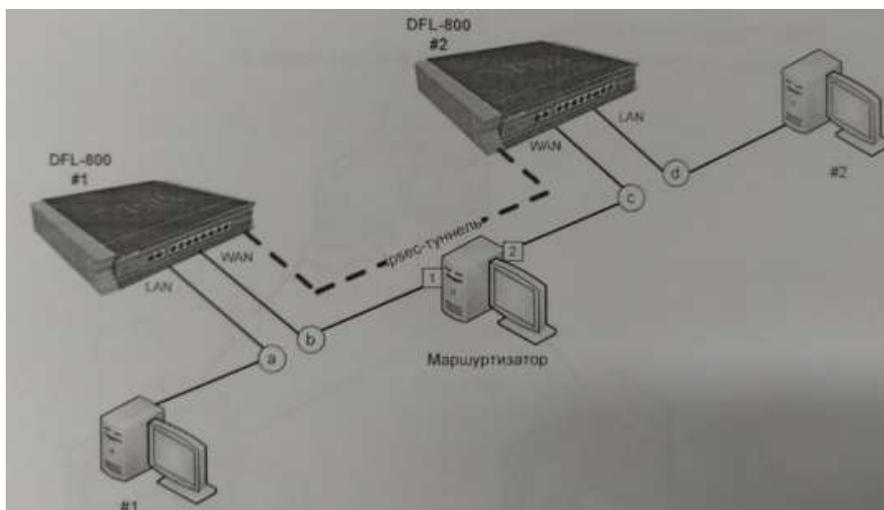


Рисунок 39 – Топология сети

2. Настройте рабочие станции и брандмауэры таким образом, чтобы создать четыре различных IP-подсети: a, b, c и d (в соответствии с рисунком 10).
3. Изучите главу «Протокол IPSec» теоретического пособия, а также главы «Настройка протокола IPSec на D-Link DFL-800» и «Протокол IPSec».
4. Настройте IPSec-туннель, как это показано на рисунке 10.
5. Проверьте работоспособность сети, обратившись с машины #1 на машину #2.

Форма представления результата: Отчет о проделанной работе, выполненная работа.

Критерии оценки:

Оценка «отлично» ставится, если задание выполнено верно.

Оценка «хорошо» ставится, если ход выполнения задания верный, но была допущена одна или две ошибки, приведшие к неправильному ответу.

Оценка «удовлетворительно» ставится, если в работе не получен ответ и приведено неполное выполнение задания, но ход выполнения задания.

Оценка «неудовлетворительно» ставится, если задание не выполнено.

Тема 1.3. Принципы обеспечения безопасности сети

Лабораторное занятие № 14

Функции отказоустойчивости

Цель работы: изучить назначение функций отказоустойчивости.

Выполнение работы способствует формированию:

У1. Настраивать стек протоколов TCP/IP и использовать встроенные утилиты операционной системы для диагностики работоспособности сети.

У2. Использовать программно-аппаратные средства технического контроля.

Материальное обеспечение:

учебно-лабораторный стенд «Сетевая безопасность»

Задание:

1 Настроить агрегирование

Порядок выполнения работы:

1 Построить схему сети.

2 Выполнить настройки.

3 Проверить работоспособность сети.

Ход работы:

Создание агрегированного канала с помощью команд CLI

Таблица 1 - Команды для настройки Link Aggregation

Команда	Параметры	Описание
create link_aggregation	group_id <value> {type[lacp/static]}	Создать агрегированный канал, динамически или статически
delete link_aggregation	group_id <value>	Удалить агрегированный канал
config link_aggregation group_	id <value> master_port <port> ports <portlist> state [enabled disabled]	Настроить параметры агрегированного канала
config link_aggregation algorithm	mac_source mac_destination mac_source_dest ip_source ip_destination ip_source_dest	Задать алгоритм агрегирования
show link_aggregation	group_id <value 1-32> algorithm	Проверка правильности настроек агрегированного канала
config lacp_ports	<portlist> mode [active passive] Настройка портов LACP show lacp_ports {<portlist>}	Проверка правильности настроек портов LACP

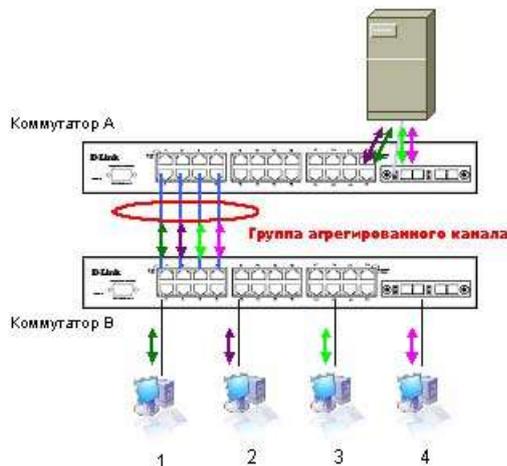


Рисунок 40 – Статическое агрегирование каналов

1. Создать группы агрегированного канала на коммутаторе А командой `create link_aggregation group_id 2 type static`
2. Задать алгоритм агрегирования портов, распределяющий трафик по портам агрегированного канала на основе для MAC-адреса источника командой `config link_aggregation algorithm mac_source`
3. Настроить созданную группы. Включить порты 2, 4, 6 и 8 коммутатора А в группу агрегированного канала 1, порт 2 сделать «связующим» портом командой `config link_aggregation group_id 1 master_port 2 ports 2,4,6,8 state enable`
4. Просмотреть конфигурации группы агрегированного канала на коммутаторе А командой `show link_aggregation`.
5. Повторить шаги 1 и 2 для коммутатора В.
6. Настройка созданной группы на коммутаторе В. Включить порты 1, 3, 5 и 7 коммутатора В в группу агрегированного канала 1, порт 3 сделать «связующим» портом командой `config link_aggregation group_id 1 master_port 1 ports 1,3,5,7 state enable`

Форма представления результата: Отчет о проделанной работе, выполненная работа.

Критерии оценки:

Оценка «отлично» ставится, если задание выполнено верно.

Оценка «хорошо» ставится, если ход выполнения задания верный, но была допущена одна или две ошибки, приведшие к неправильному ответу.

Оценка «удовлетворительно» ставится, если в работе не получен ответ и приведено неполное выполнение задания, но ход выполнения задания.

Оценка «неудовлетворительно» ставится, если задание не выполнено.

Тема 1.3. Принципы обеспечения безопасности сети Лабораторное занятие № 15

Настройка VLAN

Цель работы: Изучить настройку функции Port-based Q-in-Q.

Выполнение работы способствует формированию:

- У1. Настраивать стек протоколов TCP/IP и использовать встроенные утилиты операционной системы для диагностики работоспособности сети.
- У2. Использовать программно-аппаратные средства технического контроля.

Материальное обеспечение:

учебно-лабораторный стенд «Сетевая безопасность»

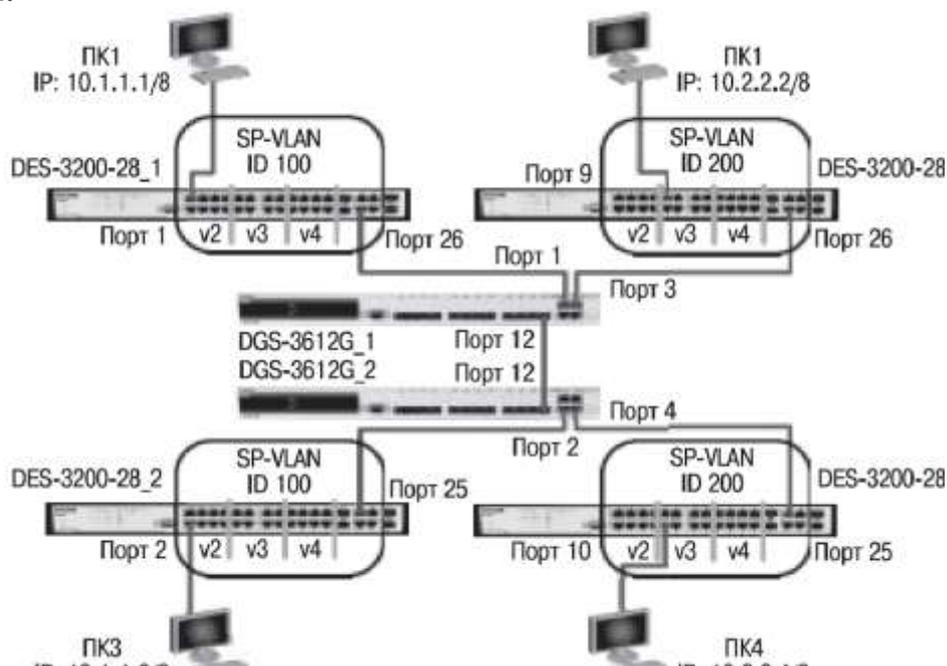
Задание:

- 1 Настроить настройку функции Port-based Q-in-Q.

Порядок выполнения работы:

- 1 Построить схему сети.
- 2 Выполнить настройки.
- 3 Проверить работоспособность сети.

Ход работы:



Настройка функции Port-based Q-in-Q

1. Настройка DES-3200-28_1 (остальные коммутаторы данной серии настраиваются аналогично)

Удалите порты из VLAN по умолчанию *config vlan default delete 1-24* для использования в других VLAN

Создайте VLAN v2, v3, v4 *create vlan v2 tag 2*

create vlan v3 tag 3

create vlan v4 tag 4

Добавьте в VLAN v2 порты 1-8 как *config vlan v2 add untagged 1-8*

немаркированные

Добавьте в VLAN v3 порты 9-16 как *config vlan v3 add untagged 9-16*
немаркированные

Добавьте в VLAN v4 порты 17-24 как *config vlan v4 add untagged 17-24*
немаркированные

Добавьте магистральные порты 25 и 26 *config vlan v2 add tagged 25-26*
как маркированные в VLAN v2, v3, v4 *config vlan v3 add tagged 25-26*
config vlan v4 add tagged 25-26

Приложение

2. Настройка DGS-3612G_1 (остальные коммутаторы
данной серии настраиваются аналогично)

Включите функцию Q-in-Q *enable qinq*

Удалите порты из Q-in-Q VLAN *config vlan default delete 1-12*
по умолчанию

Создайте Q-in-Q VLAN с SP-VLAN ID, *create vlan d100 tag 100*
равным d100, для первого клиента

Создайте Q-in-Q VLAN с SP-VLAN ID, *create vlan d200 tag 200*
равным d200, для второго клиента

Настройте порты доступа в Q-in-Q *config vlan d100 add*
VLAN d100 *untagged 1-2*

Курс

Построение коммутируемых компьютерных сетей

Схема 1:

Настройте порты доступа в Q-in-Q *config vlan d200 add*
VLAN d200 *untagged 3-4*

Настройте порт 12 как Uplink-порт *config vlan d100 add tagged 12*
в Q-in-Q VLAN d100 и d200 *config vlan d200 add tagged 12*

Настройте роли портов доступа *config qinq ports 1-4 role uni missdrop*
и отключите режим Missdrop на них *disable*

Упражнения

Задание Наблюдение

Проверьте доступность соединения *ping <IP-address>*
командой ping:

– от ПК1 к ПК2

– от ПК3 к ПК4

– от ПК1 к ПК3

– от ПК2 к ПК4

Проверьте настройку функции Q-in-Q *qinq ports all*

Что вы наблюдаете? Запишите:

Форма представления результата: Отчет о проделанной работе, выполненная работа.

Критерии оценки:

Оценка «отлично» ставится, если задание выполнено верно.

Оценка «хорошо» ставится, если ход выполнения задания верный, но была допущена одна или две ошибки, приведшие к неправильному ответу.

Оценка «удовлетворительно» ставится, если в работе не получен ответ и приведено неполное выполнение задания, но ход выполнения задания.

Оценка «неудовлетворительно» ставится, если задание не выполнено.

Тема 1.3. Принципы обеспечения безопасности сети

Лабораторное занятие № 16

Защита от сетевых атак

Цель работы: Изучить настройку системы предотвращения вторжений (IPS)

Выполнение работы способствует формированию:

У1. Настраивать стек протоколов TCP/IP и использовать встроенные утилиты операционной системы для диагностики работоспособности сети.

У2. Использовать программно-аппаратные средства технического контроля.

Материальное обеспечение:

учебно-лабораторный стенд «Сетевая безопасность»

Задание:

1 Настроить настройку системы предотвращения вторжений (IPS).

Порядок выполнения работы:

- 1 Построить схему сети.
- 2 Выполнить настройки.
- 3 Проверить работоспособность сети.

Ход работы:

Настройка системы предотвращения вторжений (IPS)

Система предотвращения вторжений (IPS) изучает конкретные шаблоны атак и оповещает или противостоит подобным атакам, когда они случаются. Одной лишь системы IPS недостаточно для того, чтобы превратить маршрутизатор в надежный межсетевой экран для Интернета, но совместно с другими средствами безопасности организовать эффективную защиту можно.

Топология

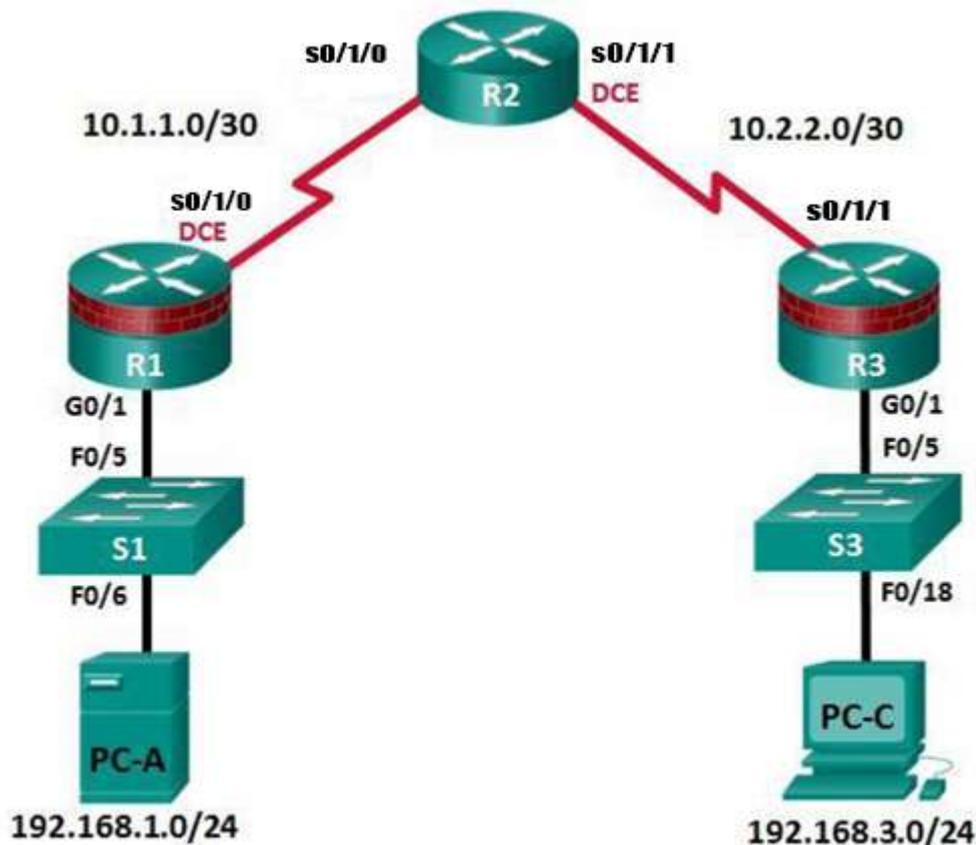


Таблица IP-адресов

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию	Порт коммутатора
R1	G0/1	192.168.1.1	255.255.255.0	Н/П	S1 F0/5
	S0/1/0 (DCE)	10.1.1.1	255.255.255.252	Н/П	Н/П
R2	S0/1/0	10.1.1.2	255.255.255.252	Н/П	Н/П
	S0/1/1 (DCE)	10.2.2.2	255.255.255.252	Н/П	Н/П
R3	G0/1	192.168.3.1	255.255.255.0	Н/П	S3 F0/5
	S0/1/1	10.2.2.1	255.255.255.252	Н/П	Н/П
PC-A Сервер Syslog	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

Задачи

- Включение IOS IPS.
- Настройка ведения журнала.
- Изменение сигнатуры IPS.
- Проверка IPS.

Исходные данные/сценарий

Ваша задача - включить систему IPS на маршрутизаторе R1 для проверки трафика, поступающего в сеть 192.168.1.0.

Сервер Syslog используется для ведения журнала сообщений IPS. Вы должны настроить маршрутизатор для идентификации сервера Syslog, который будет получать сообщения журнала.

При использовании сервиса Syslog для мониторинга сети очень важно, чтобы в сообщениях syslog отображались правильные дата и время.

Необходимые ресурсы

- 3 маршрутизатора (Cisco 1941)
- 2 коммутатора (Cisco 2960 или аналогичный)
- 2 ПК, как показано на топологической схеме

Часть 1: Настройка базовых параметров маршрутизатора

В части 1 вы создадите топологию сети и настроите базовые параметры, такие как имена хостов, IP-адреса интерфейсов, маршрутизация, доступ к устройствам и пароли.

Примечание. Выполните шаги, указанные в части 1, на всех трех маршрутизаторах. Ниже указана процедура только для маршрутизатора R1.

Шаг 1: Подключите сетевые кабели, как показано на топологической схеме.

Присоедините устройства, как показано на топологической схеме, и установите необходимые кабельные соединения.

Шаг 2: Настройте основные параметры для каждого маршрутизатора.

- а. Задайте имена хостов, как показано на топологической схеме.
- б. Настройте IP-адреса интерфейсов, как показано в таблице IP-адресов.
- в. Настройте тактовую частоту последовательных интерфейсов маршрутизатора с помощью последовательного DCE-кабеля.

```
R1(config)# interface S0/1/0
```

```
R1(config-if)# clock rate 64000
```

- д. Чтобы предотвратить попытки маршрутизатора неправильно интерпретировать введенные команды, отключите функцию DNS-поиска.

```
R1(config)# no ip domain-lookup
```

Шаг 3: Настройте маршрутизацию RIP на маршрутизаторах

```
Router>en
```

```
Router#conf t
```

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

```
Router(config)#router rip
```

```
Router(config-router)#version 2
```

```
Router(config-router)#network 192.168.1.1
```

```
Router(config-router)#network 10.1.1.1
```

```
Router(config-router)#end
```

```
Router#
```

Шаг 4: Настройте параметры IP для хостов.

Настройте статический IP-адрес, маску подсети и шлюз по умолчанию для компьютеров PC-A и PC-C, как показано в таблице IP-адресов.

Шаг 5: Проверьте базовую связь по сети.

- а. Отправьте эхо-запрос с компьютера PC-A в локальной сети маршрутизатора R1 на компьютер PC-C в локальной сети маршрутизатора R3.

Если запрос завершается с ошибкой, измените значения основных параметров устройства перед тем, как продолжить работу.

Примечание. Если эхо-запрос с компьютера PC-A на компьютер PC-C выполнен успешно, это означает, что протокол маршрутизации настроен правильно и работает корректно. Если эхо-запрос был выполнен с ошибкой, но интерфейсы устройств активны и IP-адреса заданы верно, воспользуйтесь командами **show run** и **show ip route**, чтобы определить проблемы, связанные с протоколом маршрутизации.

Шаг 6: Настройте учетную запись пользователя, шифрованные пароли и криптографические ключи для SSH.

Примечание. В данной задаче установлена минимальная длина пароля в 10 символов, однако для облегчения процесса выполнения работы пароли были относительно упрощены. В рабочих сетях рекомендуется использовать более сложные пароли.

a. Используйте команду `security passwords`, чтобы задать минимальную длину пароля в 10 символов.

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

b. Настройте доменное имя.

```
R1(config)#ip domain-name ccnasecurity.com
```

c. Настройте криптографические ключи для SSH.

```
R1(config)#crypto key generate rsa general-keys modulus 1024
```

d. Создайте учетную запись пользователя `admin01` и пароль `cisco12345`.

```
R1(config)#username admin01 privilege 15 secret cisco12345
```

e. Настройте линию 0 консоли на использование локальной базы данных пользователей для входа в систему.

Для дополнительной безопасности команда `exec-timeout` обеспечивает выход из системы линии, если в течение 5 минут отсутствует активность. Команда `logging synchronous` предотвращает прерывание ввода команд сообщениями консоли.

Примечание. Чтобы исключить необходимость постоянного повторного входа в систему во время работы, вы можете ввести команду `exec-timeout` с параметрами `0 0`, чтобы отключить проверку истечения времени ожидания. Однако такой подход не считается безопасным.

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

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

```
R1(config-line)#exec-timeout 5 0
```

```
R1(config-line)#logging synchronous
```

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

f. Настройте линию `aux 0` на использование локальной базы данных пользователей для входа в систему.

```
R1(config)#line aux 0
```

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

```
R1(config-line)#exec-timeout 5 0
```

g. Настройте линию vty 0 4 на использование локальной базы данных пользователей для входа в систему и разрешите доступ только для соединений по SSH.

```
R1(config-line)#line vty 0 4
R1(config-line)#login local
R1(config-line)#transport input ssh
R1(config-line)#exec-timeout 5 0
R1(config-line)#exit
```

h. Настройте пароль привилегированного доступа с надежным шифрованием.

```
R1(config)#enable secret class12345
```

Шаг 7: Сохраните основную текущую конфигурацию для каждого маршрутизатора.

Сохраните текущую конфигурацию в конфигурацию запуска в привилегированном режиме.

```
R1# copy running-config startup-config
```

Часть 2: Включение IOS IPS

Примечание. В Packet Tracer файлы сигнатур уже импортированы на маршрутизаторы. Это XML-файлы по умолчанию, хранящиеся во флеш-памяти. По этой причине не нужно настраивать открытый криптографический ключ и вручную импортировать файлы сигнатур.

Шаг 1: Включение пакета Security Technology.

a. На маршрутизаторе R1 введите команду show version для просмотра сведений о лицензии Technology Package.

b. Если пакет Security Technology не активирован, сделайте это с помощью следующей команды.

```
R1(config)# license boot module c1900 technology-package securityk9
```

c. Примите условия лицензионного соглашения с конечным пользователем.

d. Сохраните текущую конфигурацию и **перезагрузите маршрутизатор**, чтобы включить лицензию.

```
Router(config)#do wr
```

e. Убедитесь, что пакет Security Technology включен, с помощью команды show version.

Шаг 2: Проверка связи по сети.

a. Отправьте эхо-запрос с компьютера PC-C на компьютер PC-A. Эхо-запрос должен быть выполнен успешно.

b. Отправьте эхо-запрос с компьютера PC-A на компьютер PC-C. Эхо-запрос должен быть выполнен успешно.

Шаг 3: Создание каталога конфигурации IOS IPS во флеш-памяти.

На маршрутизаторе R1 создайте каталог во флеш-памяти с помощью команды mkdir. Присвойте каталогу имя ipsdir.

```
R1# mkdir ipsdir
Create directory filename [ipsdir]? <Enter>
```

Created dir flash:ipsdir

Шаг 4: Настройка каталога для хранения сигнатур IPS.

На маршрутизаторе R1 задайте только что созданный каталог в качестве места хранения сигнатур IPS.

```
R1(config)# ip ips config location flash:ipsdir
```

Шаг 5: Создание правила IPS.

На маршрутизаторе R1 создайте имя правила IPS с помощью команды `ip ips name name` в режиме глобальной настройки. Присвойте правилу IPS имя `iosips`.

```
R1(config)# ip ips name iosips
```

Шаг 6: Включение ведения журнала.

Система IPS в IOS поддерживает использование Syslog для отправки уведомлений о событиях. Функция уведомлений Syslog включена по умолчанию. Если консоль ведения журналов включена, будут отображаться сообщения Syslog, касающиеся IPS.

а. Если сервис Syslog не включен, включите его.

```
R1(config)# ip ips notify log
```

б. Убедитесь, что на маршрутизаторе включен сервис временных меток для ведения журналов, с помощью команды `show run`. Если сервис временных меток не включен, включите его.

```
R1(config)# service timestamps log datetime msec
```

с. Отправьте журнальные сообщения на сервер Syslog по IP-адресу 192.168.1.3.

```
R1(config)# logging host 192.168.1.3
```

Шаг 7: Настройка системы IPS в IOS на использование категорий сигнатур.

Выведите из использования категорию сигнатур `all` с помощью команды `retired true` (все сигнатуры в выпуске сигнатур). Верните в использование категорию `IOS_IPS Basic` с помощью команды `retired false`.

```
R1(config)# ip ips signature-category  
R1(config-ips-category)# category all  
R1(config-ips-category-action)# retired true  
R1(config-ips-category-action)# exit  
R1(config-ips-category)# category ios_ips basic  
R1(config-ips-category-action)# retired false  
R1(config-ips-category-action)# exit  
R1(config-ips-cateogry)# exit  
Do you want to accept these changes? [confirm] <Enter>
```

Шаг 8: Применение к интерфейсу правила IPS.

Примените к интерфейсу правило IPS с помощью команды `ip ips name direction` в режиме настройки интерфейса. Примените правило для исходящего трафика (outbound) на интерфейсе G0/1 маршрутизатора R1. После включения IPS некоторые журнальные сообщения будут отправлены на линию консоли, указывая на выполнение инициализации механизмов IPS.

Примечание. Направление in означает, что система IPS проверяет только трафик, входящий на интерфейс. Аналогичным образом, направление out означает, что система IPS проверяет только трафик, исходящий из интерфейса.

```
R1(config)# interface g0/1
R1(config-if)# ip ips iosips out
```

Часть 3: Изменение сигнатуры

Шаг 1: Изменение для сигнатуры действия при наступлении события (параметр event-action).

Верните в использование сигнатуру эхо-запроса (сигнатура 2004, идентификатор subsig 0), включите ее и измените действие сигнатуры на оповещение и отбрасывание.

```
R1(config)# ip ips signature-definition
R1(config-sigdef)# signature 2004 0
R1(config-sigdef-sig)# status
R1(config-sigdef-sig-status)# retired false
R1(config-sigdef-sig-status)# enabled true
R1(config-sigdef-sig-status)# exit
R1(config-sigdef-sig)# engine
R1(config-sigdef-sig-engine)# event-action produce-alert
R1(config-sigdef-sig-engine)# event-action deny-packet-inline
R1(config-sigdef-sig-engine)# exit
R1(config-sigdef-sig)# exit
R1(config-sigdef)# exit
Do you want to accept these changes? [confirm] <Enter>
```

Шаг 2: Проверка IPS с помощью команд show.

Используйте команду show ip ips all для просмотра сводки состояний конфигураций IPS. К каким интерфейсам и в каком направлении применяется правило iosips? G0/1 исходящие.

Шаг 3: Проверка правильности работы IPS.

a. Попробуйте отправить эхо-запрос с компьютера PC-C на PC-A. Эхо-запрос выполнен успешно? Поясните ответ.

Эхо-запрос должен быть выполнен с ошибкой. Это связано с тем, что для действия event-action для эхо-запроса было установлено правило IPS deny-packet-inline.

b. Попробуйте отправить эхо-запрос с компьютера PC-A на PC-C. Эхо-запрос выполнен успешно? Поясните ответ.

Эхо-запрос должен быть выполнен успешно. Это связано с тем, что правило IPS не относится к ответу на эхо-запрос. Когда компьютер PC-A отправляет эхо-запрос на компьютер PC-C, компьютер PC-C отправляет ответ на эхо-запрос.

Шаг 4: Просмотр сообщений Syslog.

a. Выберите сервер Syslog.

b. Перейдите на вкладку Services.

c. В левом меню навигации выберите SYSLOG для просмотра файла журнала.

Форма представления результата: Отчет о проделанной работе, выполненная работа.

Критерии оценки:

Оценка «отлично» ставится, если задание выполнено верно.

Оценка «хорошо» ставится, если ход выполнения задания верный, но была допущена одна или две ошибки, приведшие к неправильному ответу.

Оценка «удовлетворительно» ставится, если в работе не получен ответ и приведено неполное выполнение задания, но ход выполнения задания.

Оценка «неудовлетворительно» ставится, если задание не выполнено.