Содержание

ВНИМАНИЕ:

В данном документе все ссылки указывают на разделы и главы в пособие «Управление комплектом», если не указано иное пособие.

1. Безопасность сетей Ethernet

Лабораторная работа № 1.

Аудит безопасности протокола SNMP.

Цель работы:

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

Порядок выполнения работы:

1. Постройте топологию сети, показанную на рисунке 1.

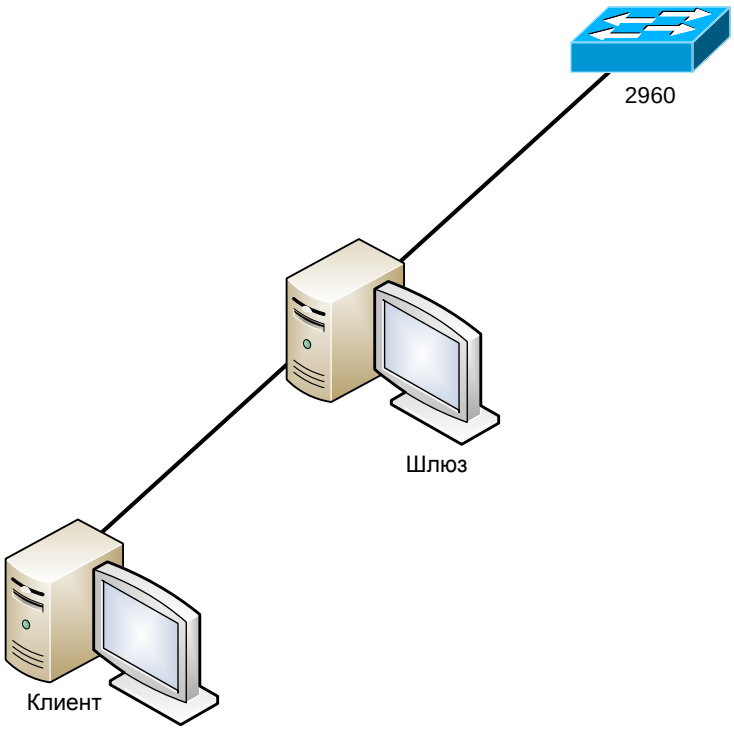

Рисунок 1.

2. Настройте маршрутизацию между сетями.
3. Изучите раздел 9.1 «Протокол SNMP» теоретического пособия.
4. Настройте SNMP-протокол на коммутаторе.
5. На Шлюзе запустите tcpdump. Отсеивайте из потока только пакеты протокола SNMP.
6. Запустите утилиту iReasoning MIB Browser.
7. Загрузите базу MIB RFC-1213.
8. С Клиента на коммутаторе выясните следующие параметры:
    - название устройства, время работы устройства, службы, запущенные на устройстве (ветвь system);

- количество интерфейсов на устройстве, содержимое таблицы интерфейсов, назначение двух дополнительных виртуальных портов (ветвь interfaces);
- IP-адрес устройства, содержимое таблицы маршрутизации (ветвь ip);
- TCP-соединения, установленные устройством (ветвь tcp).

9. Выясните из перехваченных на шлюзе пакетов SNMP Community String.
10. Со Шлюза выясните состояние портов коммутатора.
11. Сделайте вывод о безопасности протоколов SNMP v1/v2c, границах их применимости и предложите методы защиты этих протоколов.

Лабораторная работа № 2.

Аудит безопасности протокола STP.

Цель работы:

Изучение уязвимостей алгоритма Spanning Tree и Rapid Spanning Tree.

Порядок выполнения работы:

1. Изучите раздел 2.9 «Аудит безопасности протокола связующего дерева STP» теоретического пособия.
2. Соберите сеть с топологией, представленной на рисунке 2.

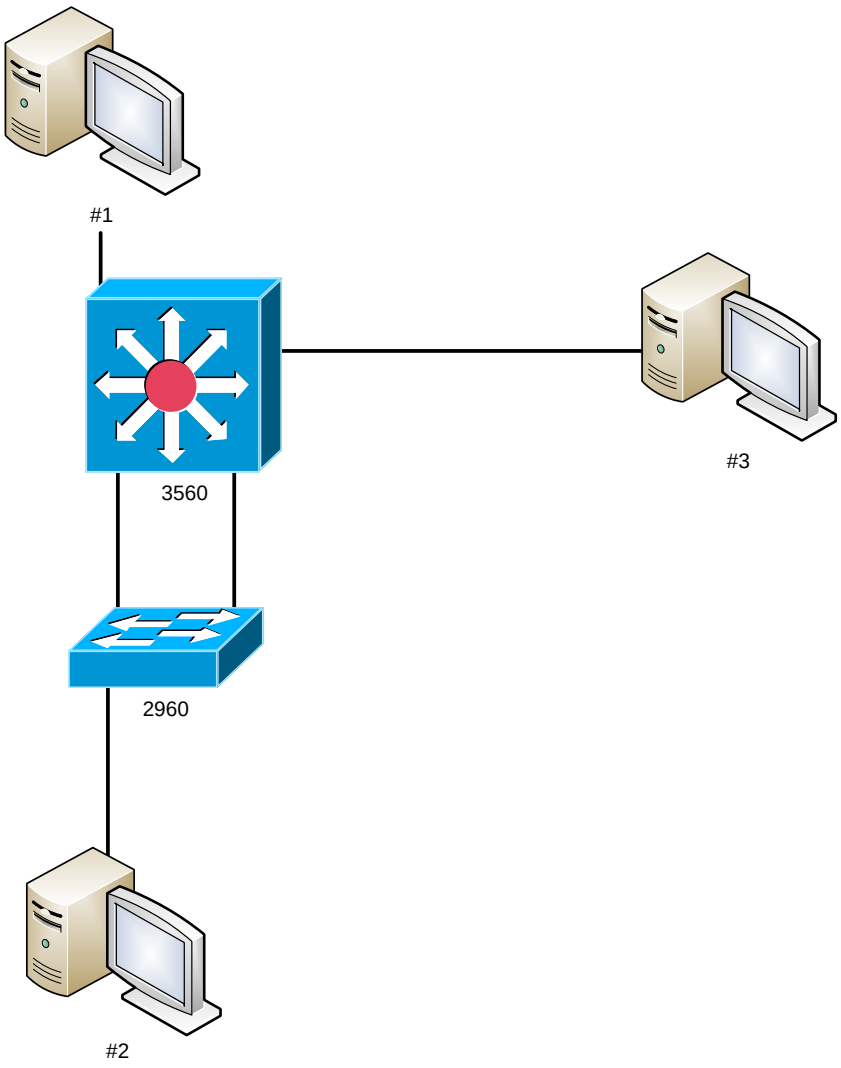

Рисунок 2.

3. Настройте и активизируйте на коммутаторах протокол Spanning Tree.
4. Параллельно с шагом 3 запустите на машине #3 утилиту tcpdump и выясните MAC-адреса коммутаторов, анализируя содержимое пактов BPDU.
5. Сбросьте настройки коммутатора в фабричные и перезагрузите его.

Лабораторная работа № 3.

Виртуальные локальные сети IEEE 802.1q.

Цель работы:

Изучение технологий виртуальных сетей. Получение навыков настройки VLAN на основе тэгов IEEE 802.1q в сети, построенной на коммутаторах Cisco.

Порядок выполнения работы:

1. Изучите раздел 4.8 «Виртуальные сети. Сети на базе маркированных кадров» теоретического пособия.
2. Постройте топологию сети, представленную на рисунке 3.

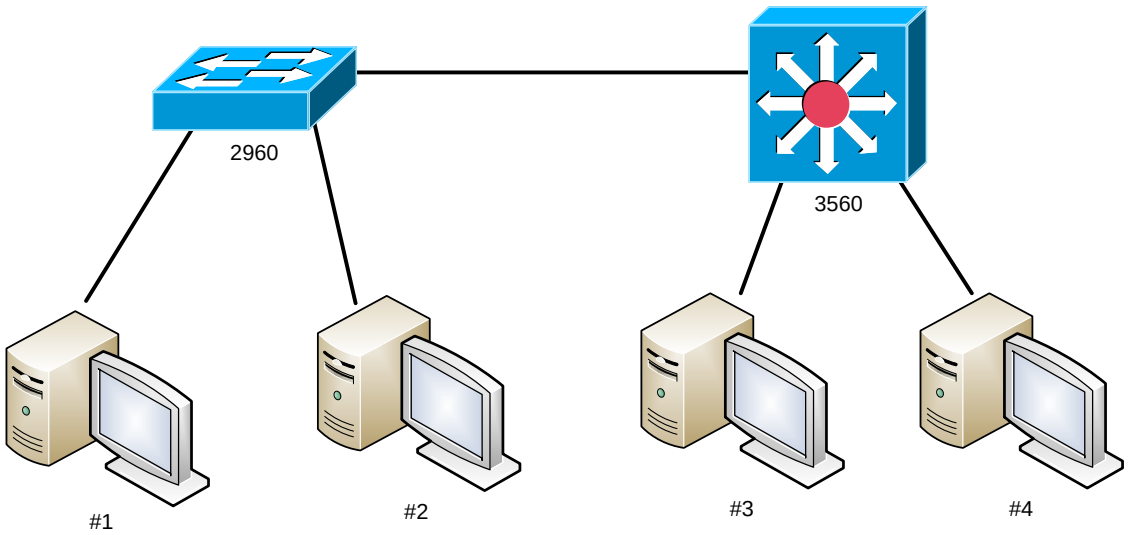

Рисунок 3. Коммутируемая топология для настройки виртуальных сетей VLAN.

3. Сконфигурируйте VLAN на основе тегов таким образом, чтобы рабочие станции 1 и 4 принадлежали виртуальной сети №1, станция 2 принадлежала виртуальной сети №2, а станция №3 – виртуальной сети №3 и при этом являлась общедоступным ресурсом. То есть машины в виртуальных сетях №1 и №2 не должны взаимодействовать между собой, но должны взаимодействовать с машиной №3.
4. Проверьте правильность конфигурации сети. Результаты мониторинга покажите и поясните преподавателю.
5. Сбросьте настройки коммутаторов в фабричные и перезагрузите его.

Лабораторная работа № 4.

Базовые механизмы безопасности коммутаторов.

Цель работы:

Изучение технологий Trusted Hosts, IP-MAC Binding и Port Security.

Порядок выполнения работы:

1. Соберите топологию сети, представленную на рисунке 4.

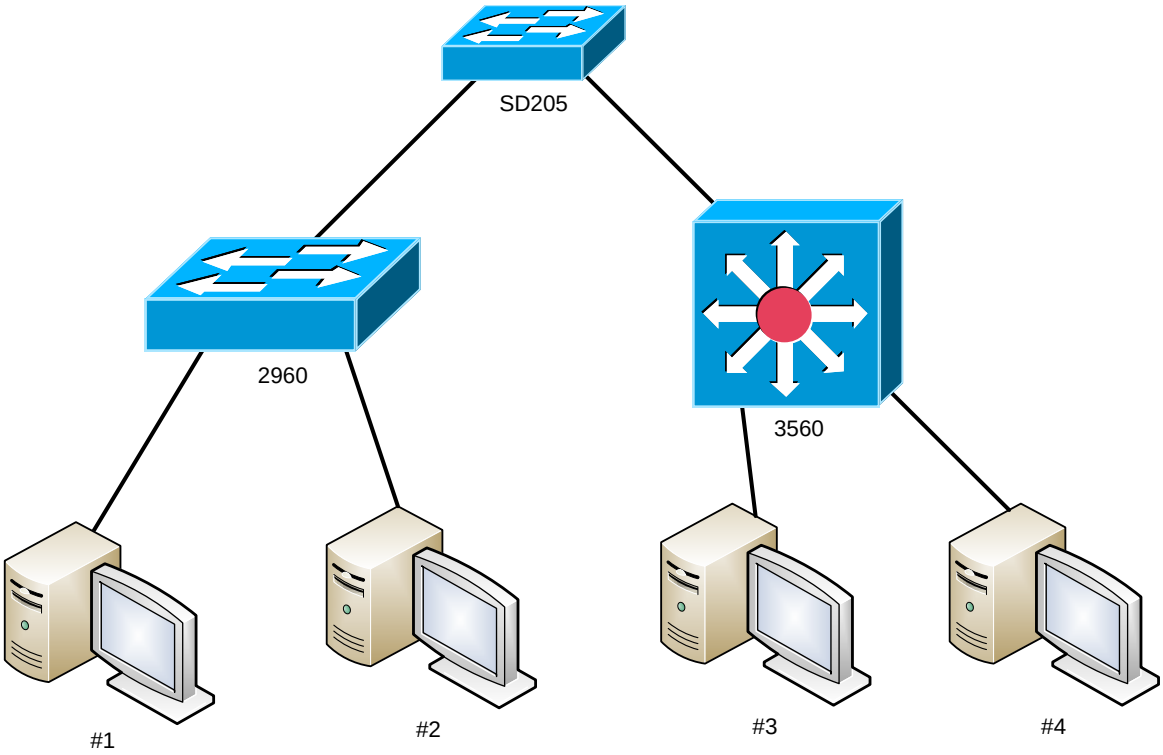

Рисунок 4.

2. Настройте коммутаторы таким образом, чтобы ими могли управлять только машины #1 и #3.
3. Проверьте выполненные настройки.

4. Очистите таблицы коммутации на всех коммутаторах.
5. С машин #1 и #2 «пропингуйте» машину #3.
6. Убедитесь, что в таблицах коммутации не присутствует аппаратного адреса машины #4.
7. Заблокируйте на обоих коммутаторах таблицу коммутации в режиме Permanent.
8. Попытайтесь осуществить взаимодействие с 4-ым компьютером с любого компьютера. Объясните полученный результат.

9. Сбросьте блокировку таблиц коммутации.

10. Используя технологию IP-MAC Binding, настройте на коммутаторах фильтры таким образом, чтобы в сети могли работать только машины #1 и #3.

11. Сбросьте настройки коммутаторов в фабричные и перезагрузите его.

Лабораторная работа № 5.

Безопасность на основе сегментации трафика.

Цель работы:

Изучение механизма сегментации трафика.

Порядок выполнения работы:

1. Соберите топологию сети, представленную на рисунке 5.

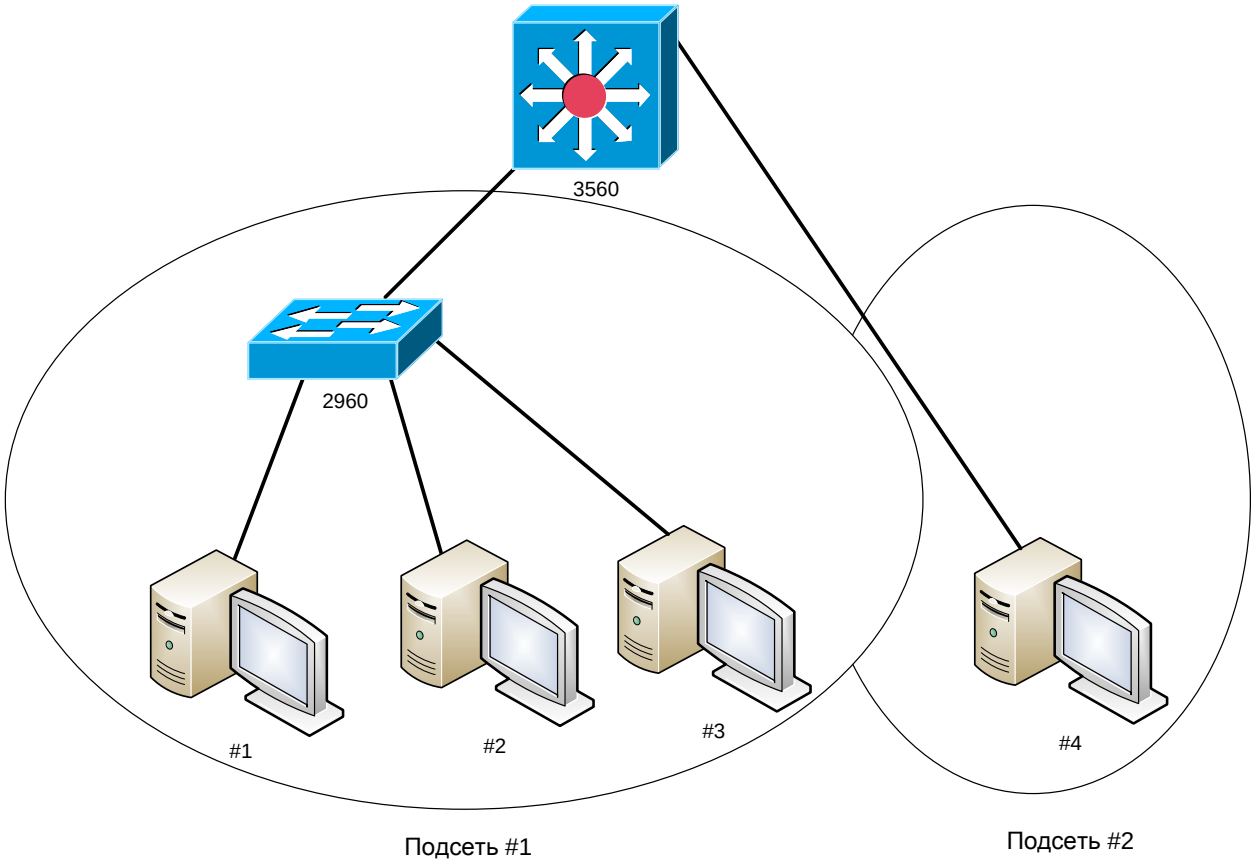

Рисунок 5.

2. Изучите 3.3 «Layer 3 Features» (меню «IP Interface Settings»).
3. Создайте IP-подсети, как это показано на рисунке 5. Назначьте каждому компьютеру IP-адрес из собственной подсети.
4. Организуйте на коммутаторе DES-3010G принцип «расчески» – каждый компьютер, подключенный к коммутатору, может обмениваться информацией только с внешним миром, но не с другими компьютерами, подключенными к этому же коммутатору.
5. Проверьте правильность сделанных настроек.
6. Сбросьте настройки коммутатора в фабричные и перезагрузите его.

Лабораторная работа № 6.

Безопасность на основе протокола IEEE 802.1x.

Цель работы:
Изучение протокола IEEE 802.1x, способов его настройки на сетевых узлах, способов настройки сервера RADIUS.

Порядок выполнения работы:

1. Соберите сеть с топологией, представленной на рисунке 16.

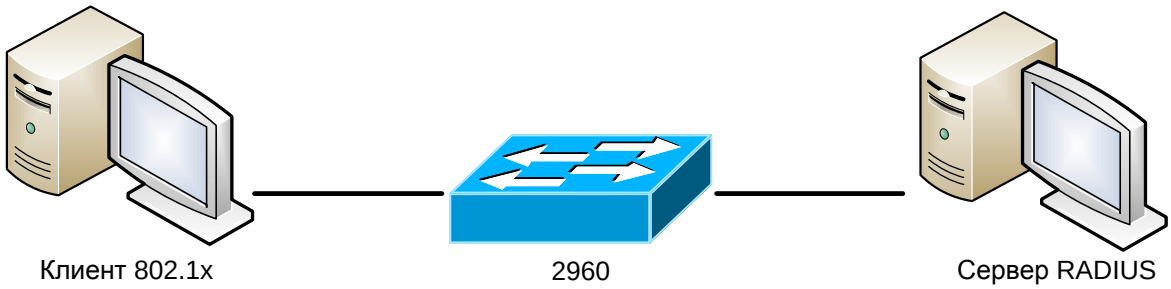

Рисунок 16. Топология коммутируемой сети.

2. Изучите раздел 2.7 «Протокол IEEE 802.1x» теоретического пособия.
3. Настройте сервер RADIUS, используя утилиту *freeradius*.

4. Включите протокол 802.1x на коммутаторе. Используйте авторизацию на основе портов.
5. Переведите порт коммутатора, к которому подключен клиент 802.1x, в неавторизованное состояние.

6. Настройте клиента 802.1x, используя утилиту *wpa_supplicant*.
7. Запустите клиента 802.1x.

8. Проверьте успешность авторизации порта путём:
   - взаимодействия между машинами;
   - анализа журнала (логов) клиента 802.1x;
   - анализа журнала сервера.

9. Физически отключите кабель клиента от порта коммутатора, а затем заново подключите. Выясните, в каком состоянии (авторизации) находится порт клиента. Ответьте на вопрос, можно ли нарушить безопасность сети путём физического подключения неавторизованной машины на авторизованный порт коммутатора.

10. Соберите сеть с топологией, представленной на рисунке 17.

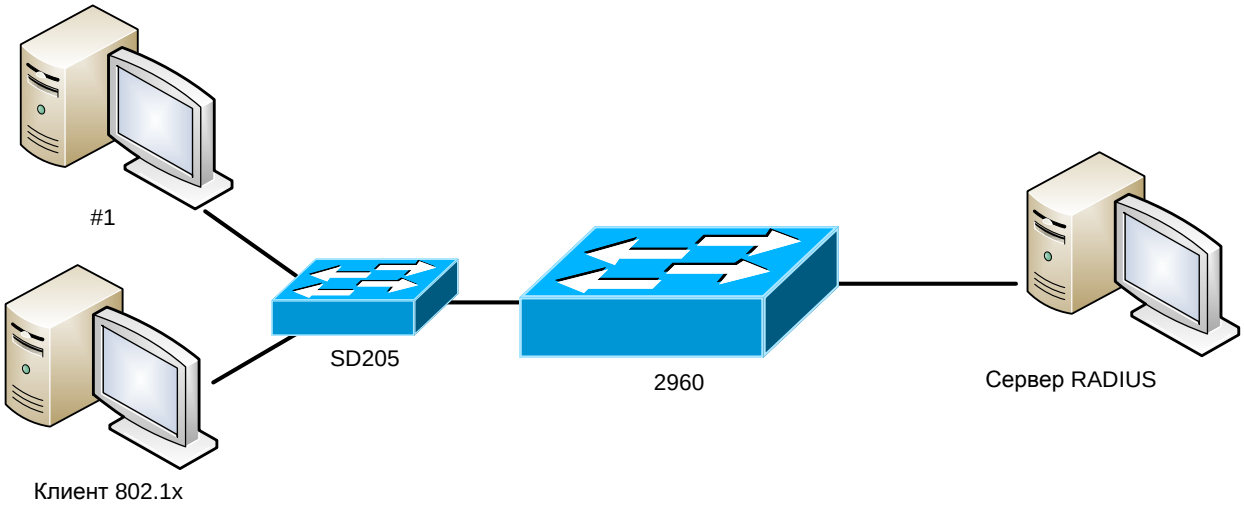

Рисунок 17. Топология коммутируемой сети.

11. Авторизуйте порт коммутатора 2960, используя клиента 802.1x.
12. Попробуйте осуществить взаимодействие машины № 1 и сервера RADIUS. Какие выводы можно сделать об уязвимостях в безопасности протокола 802.1x на основе портов.

ВНИМАНИЕ: Далее работа может выполняться одновременно только одной бригадой

13. Соберите сеть с топологией, представленной на рисунке 18.

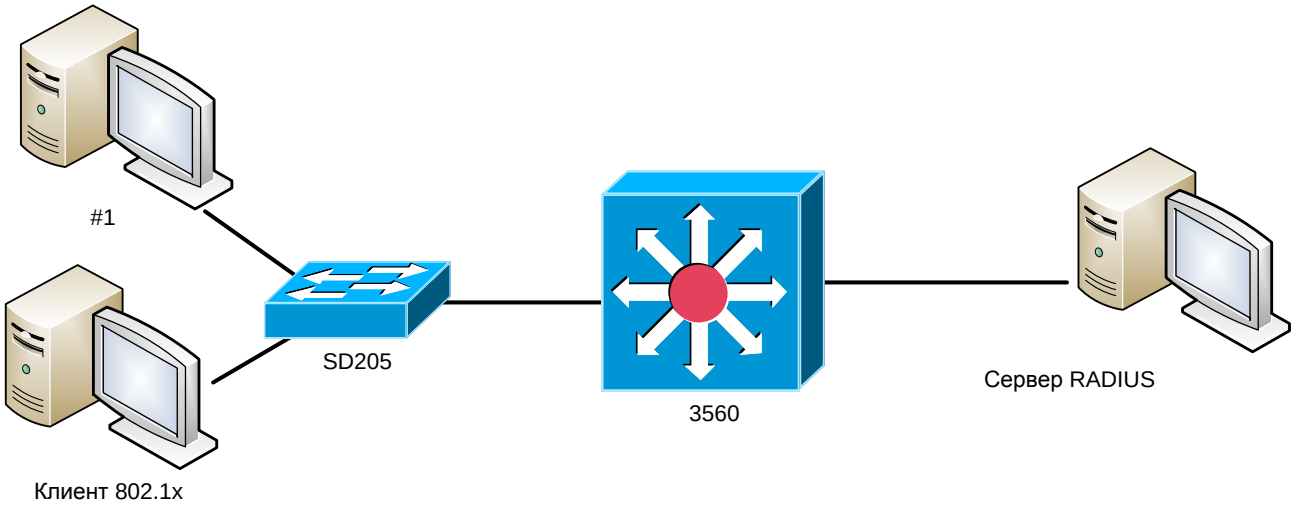

Рисунок 18. Топология коммутируемой сети.

14. Включите протокол 802.1x на коммутаторе. Используйте авторизацию на основе MAC-адресов.
15. Переведите порт коммутатора 3560, к которому подключен коммутатор SD205, в неавторизованное состояние. Затем инициируйте данный порт MAC-адресом машины, на которой запущен клиент 802.1x.
16. Запустите клиента 802.1x.
17. Проверьте успешность авторизации порта путём:
    - взаимодействия между клиентом и сервером;
    - анализа журнала (логов) клиента 802.1x;
    - анализа журнала сервера.

18. Попробуйте осуществить взаимодействие между машиной № 1 и сервером.

19. Настройте и запустите клиента 802.1x на машине № 1. Теперь попробуйте осуществить взаимодействие между машиной № 1 и сервером. На основе полученных результатов сделайте вывод о защищенности протокола 802.1x на основе MAC-адресов.

20. Сбросьте настройки коммутатора в фабричные и перезагрузите его.

Лабораторная работа № 7.

Списки контроля доступа ACL.

Цель работы:

Изучение технологии Access Control Lists.

Порядок выполнения работы:

1. Соберите сеть с топологией, представленной на рисунке 9.

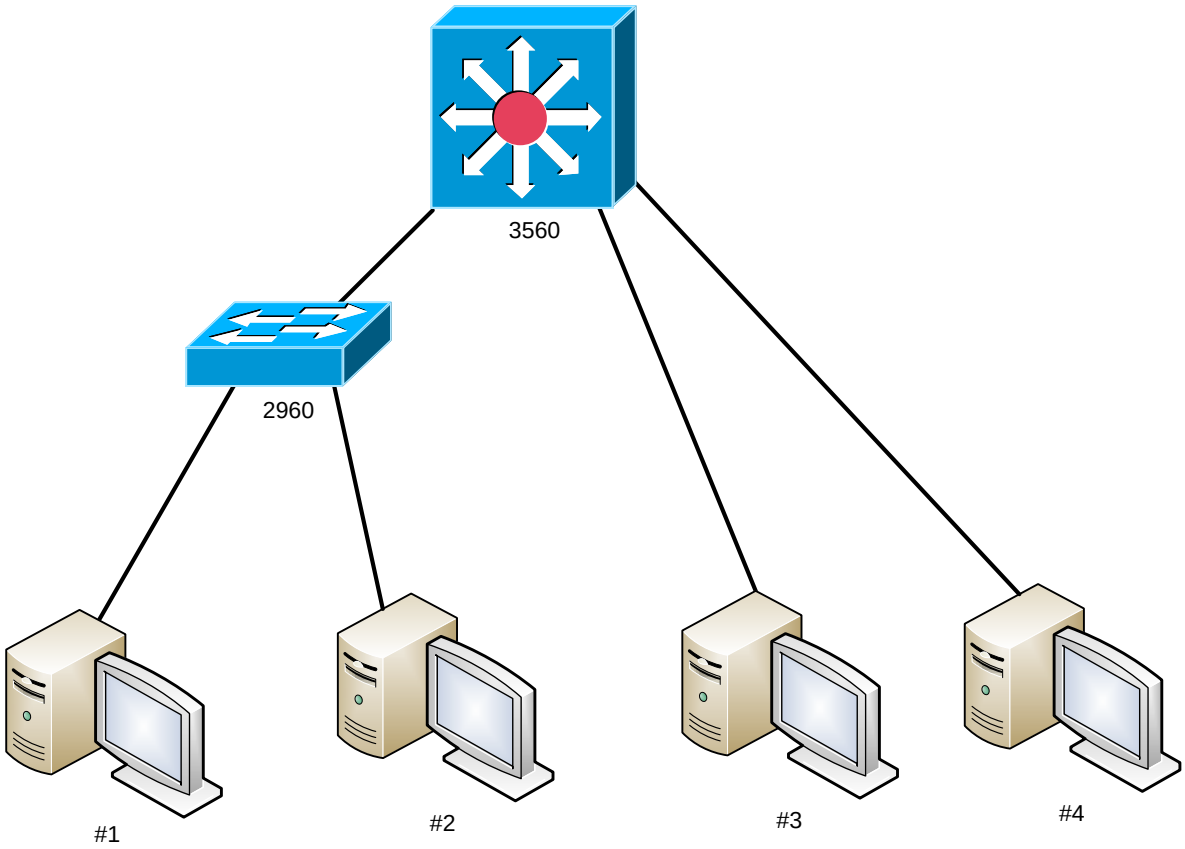

Рисунок 9.

2. Изучите раздел 4.5 «Списки контроля доступа» теоретического пособия.
3. Настройте списки контроля доступа таким образом, чтобы:
   - коммутатор 2960 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 идёт от машины #2 к машине #3 «зеркалиловался» на порт машины #4.
4. Проверьте созданные настройки.

2. Безопасность сетей Wi-Fi

Лабораторная работа № 8.

Шифрование канала с использованием протокола WEP.

Цель работы:

Получение навыков построения сетей Wi-Fi с использованием механизма шифрования WEP.

Порядок выполнения работы:

1. Постройте сеть, топология которой представлена на рисунке 11.

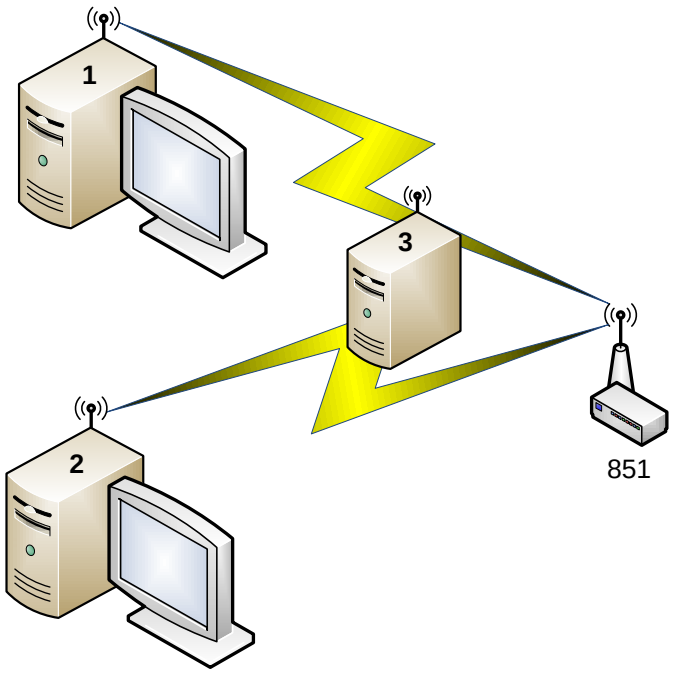

Рисунок 11.

2. Изучите раздел 5.2 «Механизмы шифрования в беспроводных сетях» теоретического пособия.

3. Включите точку доступа, настройте канал и имя сети. Включите внутренний DHCP-сервер. Включите шифрование WEP, используя 40-битный ключ.
4. Ассоциируйте два компьютера с этой точкой доступа.
5. Запустите на третьем компьютере утилиту «Airodump-ng» для перехвата пакетов.
6. Выполните взаимодействие между компьютерами 1 и 2.
7. Убедитесь (по экрану airodump-ng), что несколько пакетов с данными было перехвачено.
8. 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.

Лабораторная работа № 9.

Шифрование канала с использованием протокола WPA.

Цель работы:

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

Порядок выполнения работы:

1. Постройте сеть, топология которой представлена на рисунке 12.

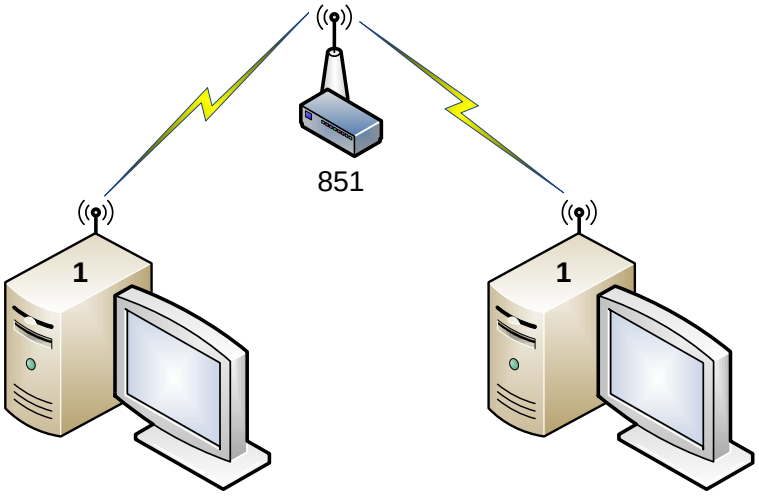

Рисунок 12.

2. Используя 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.

```
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,
причём файл не будет сохранён на диске, что позволит оценить реальную
пропускную способность сети. Скорость передачи данных будет указана в
выводе команды scp.
```

4. Используя утилиту tcpdump, 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.

Лабораторная работа № 10.

Аутентификация беспроводных клиентов на основе учётных записей пользователей и аппаратных адресов компьютеров.

Цель работы:

Получение навыков построения защищённых wi-fi сетей с использованием RADIUS-сервера и фильтрации по MAC-адресам.

Порядок выполнения работы:

1. Постройте сеть, топология которой представлена на рисунке 13.
2. Используя утилиту freeradius, настройте RADIUS-сервер и создайте двух произвольных пользователей.
3. Настройте маршрутизатор Cisco 851 на использованием IEEE 802.1x.
4. Настройте клиентов, используя утилиту wpa_supplicant.
5. Проверьте работоспособность сети.

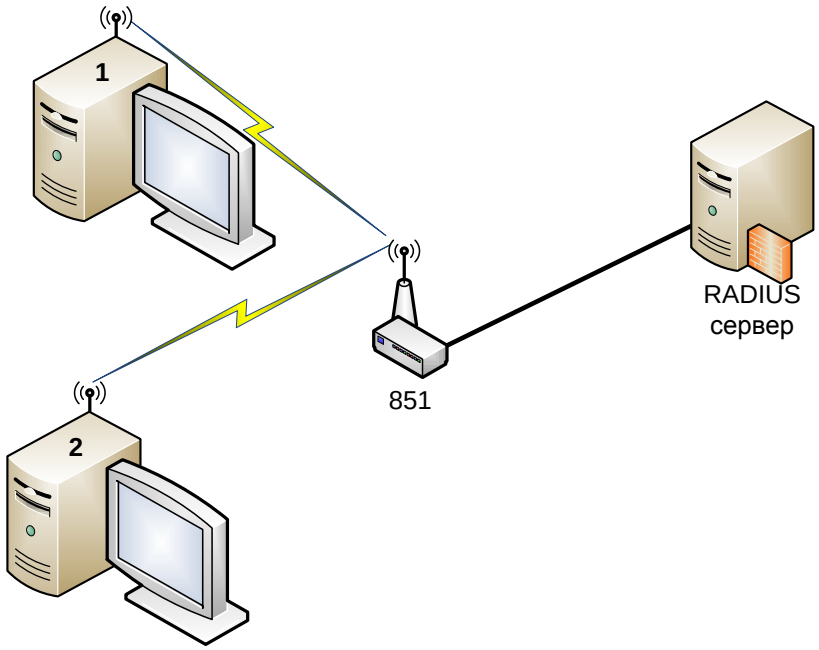

Рисунок 13. Использование RADIUS-сервера.

6. Соберите топологию, представленную на рисунке 14.
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 A с помощью запрещенных списков MAC-адресов.
8. Проверьте правильность выполненных настроек.

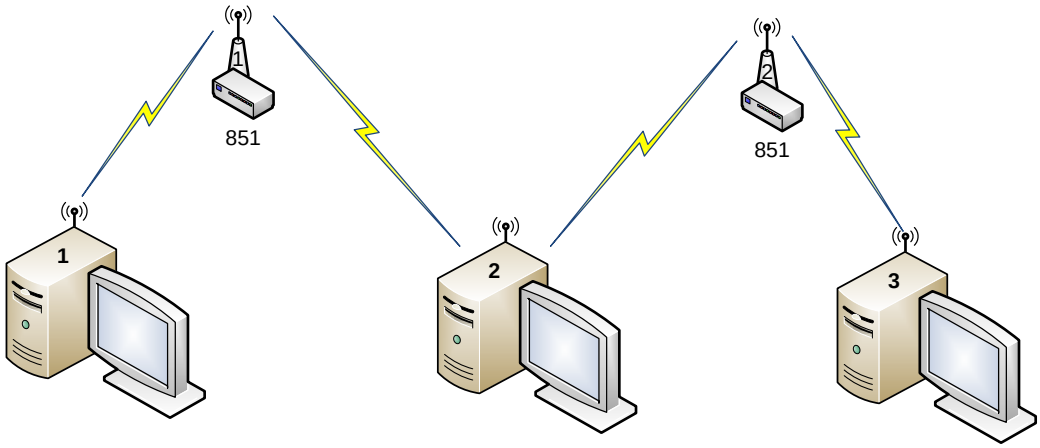

Рисунок 14. Использование фильтрации по MAC-адресам.

Лабораторная работа № 11.

Обнаружение атак диссоциации с использованием ОС Linux.

Цель работы:

Изучение работы и возможностей утилиты Kismet.

Порядок выполнения работы:

1. Постройте сеть, топология которой представлена на рисунке 15.

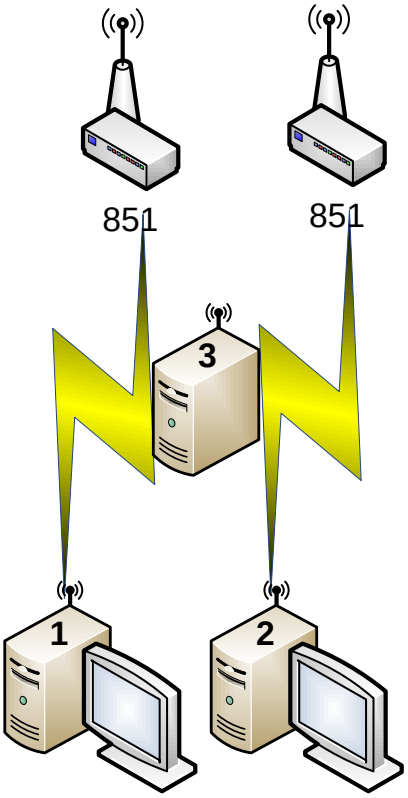

Рисунок 15.

2. Включите и настройте 2 точки доступа на разные каналы и имена сетей. Включите внутренний DHCP-сервер точки доступа.
3. Подключите 2 компьютера к разным сетям, как показано на рисунке 15.
4. Запустите Kismet на 3 компьютере. Просмотрите обнаруженные сети.
5. Определите каналы, на которых располагаются точки доступа.
6. Посмотрите, какие типы пакетов перехватываются, когда компьютеры ассоциированы, но не активны. Наблюдайте за графиком количества перехваченных пакетов в секунду
7. Выполните взаимодействие между 2 компьютерами, находящимися в одной сети (например, скопируйте файл с одного компьютера на другой с помощью scp). Какие типы пакетов появились в эфире? Как изменился график?
8. Определите клиентов обнаруженных сетей.
9. Запустите на одном из 2 компьютеров, подключенных к одной сети, непрерывную атаку диссоциации на вторую сеть (с помощью MDK или с помощью aireplay).
10. Посмотрите на реакцию Kismet.

3. Механизмы построения защищенных сетей с использованием брандмауэров

Лабораторная работа № 12.

Протокол PPPoE.

Цель работы:

Изучение протокола PPPoE и способов его настройки и использования в ОС Linux и брандмауэре ASA5505.

Порядок выполнения работы:

1. Соберите топологию сети, представленную на рисунке 16.

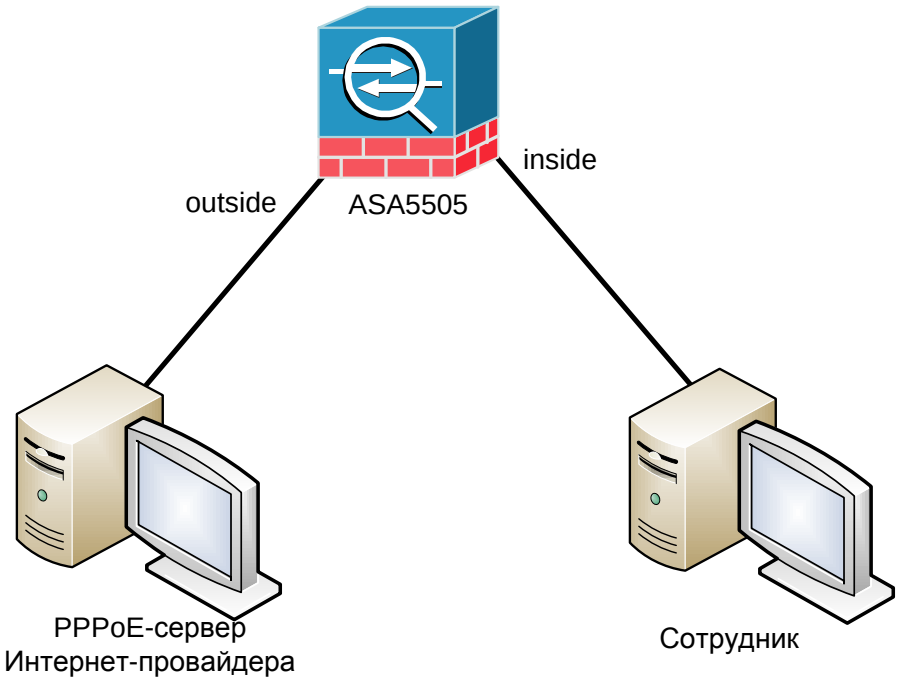

Рисунок 16.

2. Настройте рабочие станции и брандмауэр таким образом, чтобы интерфейс outside ASA5505 и PPPoE-сервер принадлежали одной IP-подсети, а интерфейс inside ASA5505 и машина сотрудника – другой.
3. Изучите главу 8.1 «Протокол PPPoE» теоретического пособия.
4. Используя утилиту rp-pppoe, настройте PPPoE-сервер на машине Интернет-провайдера.
5. Настройте ASA5505 в качестве PPPoE-клиента (используя созданную в п.5 учетную запись пользователя). Установите PPPoE-туннель.
6. Осуществите доступ с машины сотрудника в сеть Интернет, то есть к машине провайдера.

Лабораторная работа № 13.

Технология Network Address Translation.

Цель работы:

Изучение технологии NAT и способов её настройки на брандмауэре ASA5505.

Порядок выполнения работы:

1. Соберите топологию сети, представленную на рисунке 17.

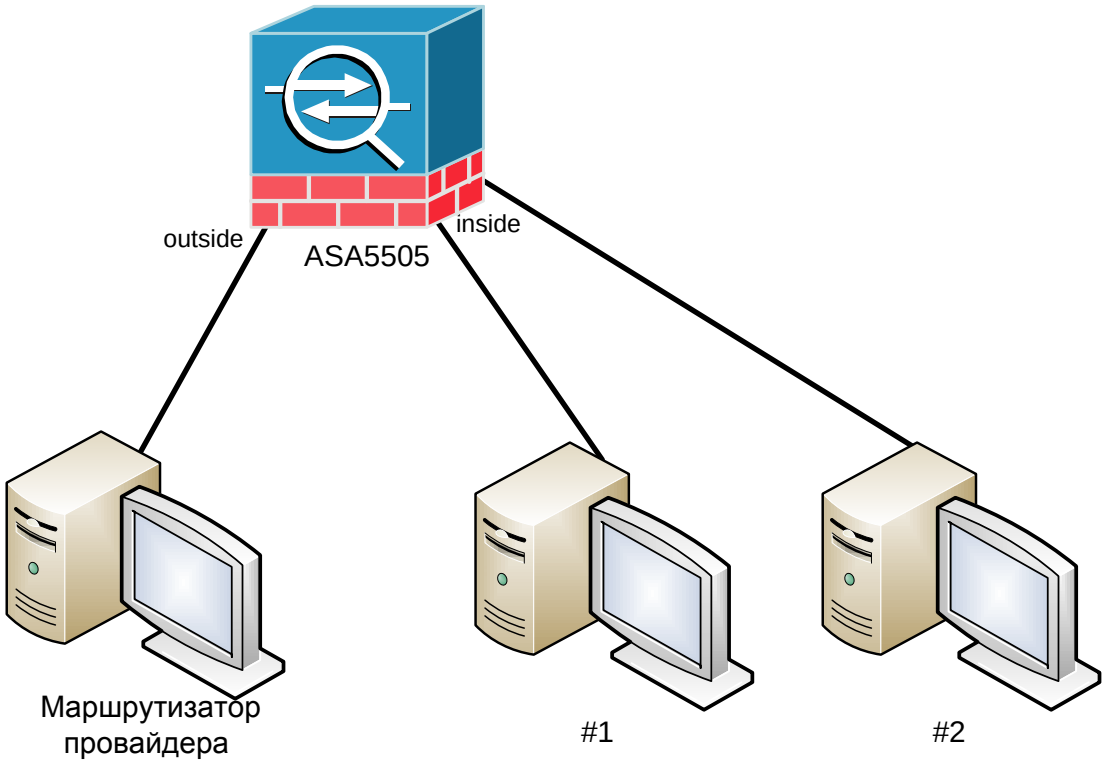

Рисунок 17.

2. Настройте рабочие станции и брандмауэр таким образом, чтобы интерфейс outside ASA5505 и маршрутизатор провайдера принадлежали одной IP-подсети, а интерфейс inside ASA5505 и машины #1 и #2 – другой.
3. Настройте и запустите на маршрутизаторе провайдера веб-сервер.
4. Изучите главу 7.1.4 «Транслятор адресов» теоретического пособия.
5. Настройте NAT на ASA5505.
6. Одновременно осуществите обращение с машин #1 и #2 к веб-серверу провайдера.
7. Если попытка успешна (получена стартовая страница Apache), то запустите на машине провайдера утилиту tcpdump и снова осуществите запрос к веб-серверу с машин локальной сети.
8. Проанализируйте результаты, выдаваемые утилитой tcpdump и ответьте на вопрос: какой IP-адрес и номер порта стоит в адресе отправителя запросов, получаемых веб-сервером.

Лабораторная работа № 14.

Виртуальные частные сети.

Цель работы:

Изучение протокола IPSec и способа его настройки в ОС Linux и на брандмауэре ASA5505.

Порядок выполнения работы:

1. Соберите топологию сети, представленную на рисунке 19.

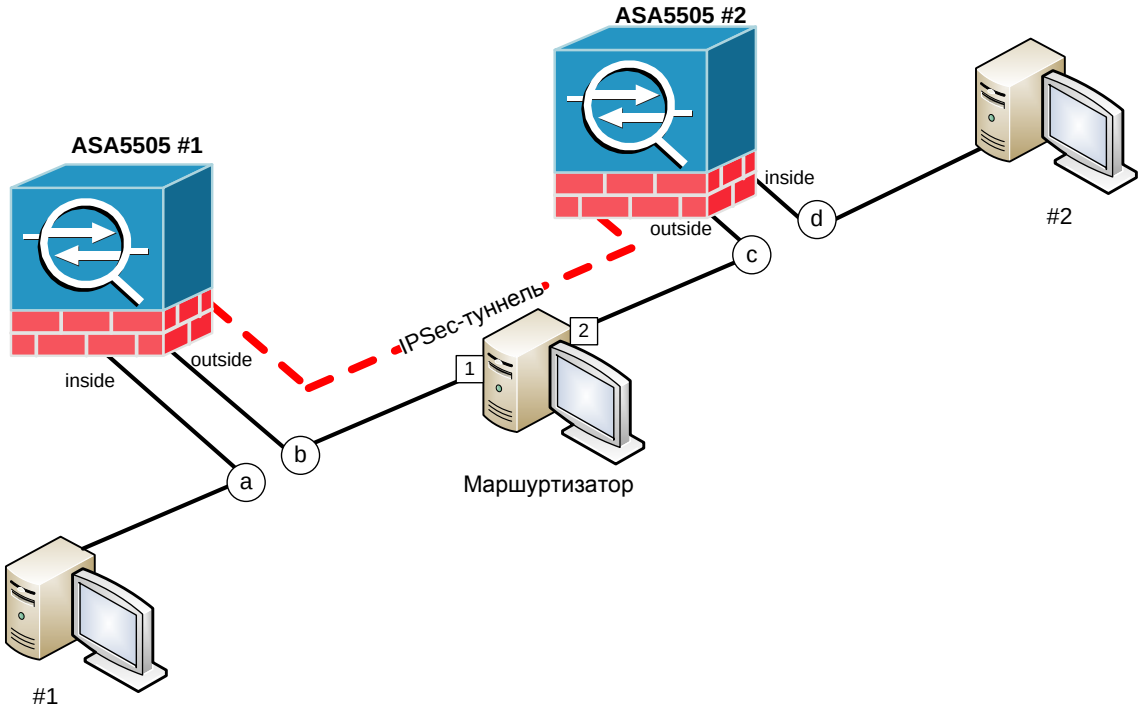

Рисунок 19.

2. Настройте рабочие станции и брандмауэры таким образом, чтобы создать четыре различных IP-подсети: a, b, c и d (в соответствие с рисунком 19).
3. Изучите главу 8.2.3 «Протокол IPSec» теоретического пособия.
4. Настройте IPSec-туннель, как это показано на рисунке 19.
5. Проверьте работоспособность сети, обратившись с машины #1 на машину #2.

4. Механизмы построения защищенных сетей с использованием ОС Linux

Лабораторная работа № 15.

Утилита iptables.

Цель работы:

Получение навыков построения программного межсетевого экрана на базе ОС Linux с использованием утилиты iptables.

Порядок выполнения работы:

1. Соберите топологию сети, представленную на рисунке 20.

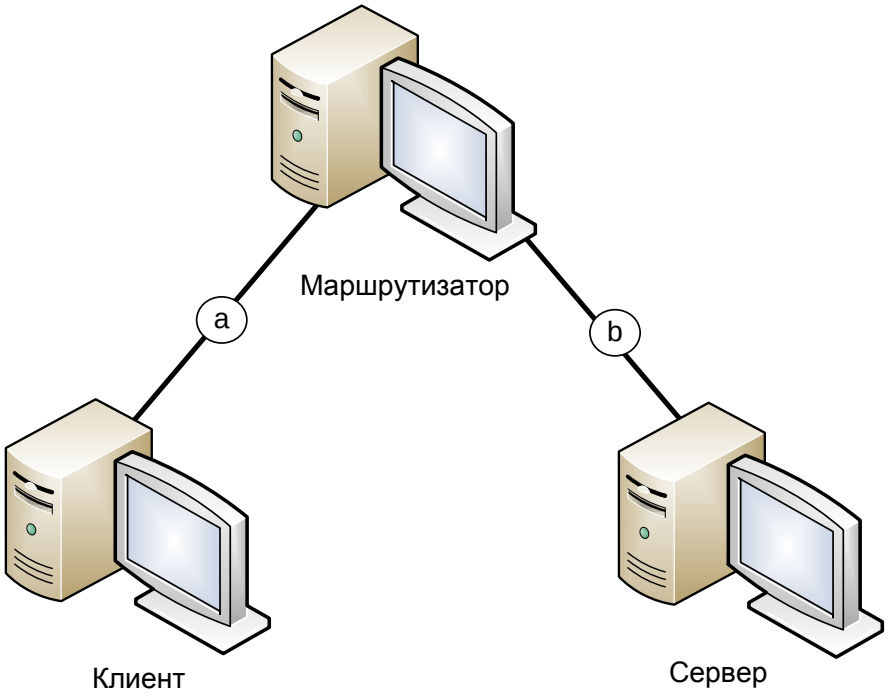

Рисунок 20.

2. Настройте рабочие станции таким образом, чтобы создать две различных IP-подсети: a и b (в соответствие с рисунком 20).
3. Настройте и запустите на сервере веб и файловый сервисы.
4. Используя утилиту iptables, настройте на маршрутизаторе транслятор сетевых адресов и создайте два правила межсетевого экрана, согласно которым:
   - ✓ клиент может обращаться к веб-серверу;
   - ✓ клиент не может обращаться к файловому серверу.
5. Проверьте правильность сделанных настроек (в том числе используя утилиту tcpdump).

Лабораторная работа № 16.

Цифровые сертификаты.

Цель работы:

Изучение технологии цифровых сертификатов и получение навыков построения зашифрованной сети на базе этой технологии и ОС Linux.

Порядок выполнения работы:

1. Соберите топологию сети, представленную на рисунке 21.

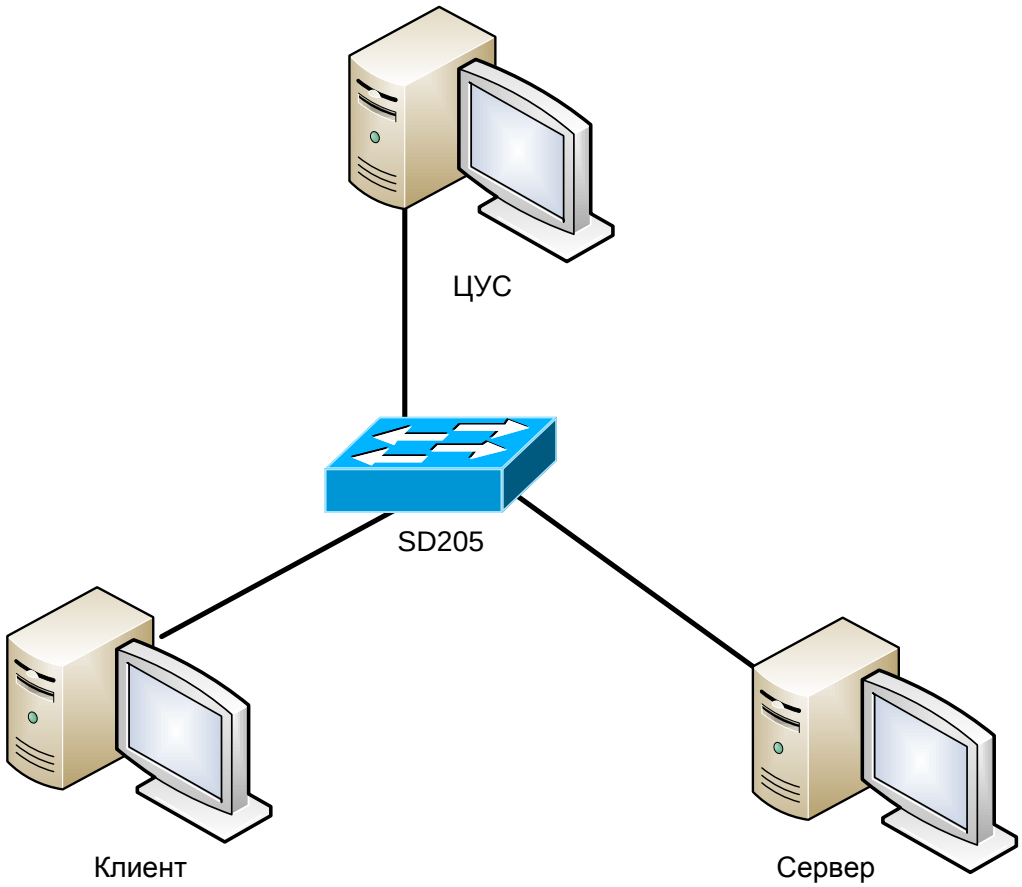

Рисунок 21.

2. Изучите главу 8.2.4 «Протокол SSL/TLS» теоретического пособия.
3. Запустите веб-сервис на сервере.
4. Инициируйте соединение клиента с веб-сервером и с помощью утилиты tcpdump убедитесь, что данные передаются без шифрования.
5. Создайте центр управления сертификатами (ЦУС) средствами openssl.
6. Создайте сертификат для веб-сервера. Настройте веб-сервер на работу с сертификатом.
7. Инициируйте соединение клиента с веб-сервером по протоколу HTTPS. Средствами браузера изучите сертификат. С помощью tcpdump изучите передаваемые пакеты и убедитесь, что передаваемая информация шифруется.

Лабораторная работа № 17.

Детектор вторжений snort.

Цель работы:

Получение навыков построения систем обнаружения вторжений на базе ОС Linux с использованием утилиты snort.

Порядок выполнения работы:

1. Соберите топологию сети, представленную на рисунке 22.

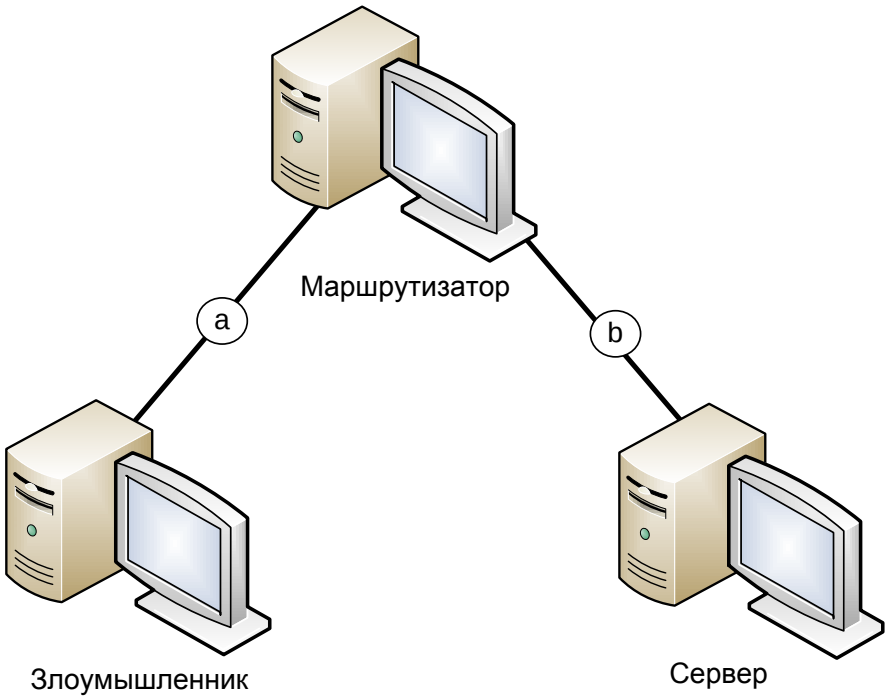

Рисунок 22.

2. Настройте рабочие станции таким образом, чтобы создать две различных IP-подсети: a и b (в соответствие с рисунком 22).
3. Изучите главу 7.2 «Системы обнаружения атак и вторжений» теоретического пособия. Скрипт посылает UDP-пакеты заданного размера на заданный порт заданной машины.
4. Запустите скрипт snort.pl (находится на диске в каталоге /root/Desktop/Scripts/) следующим образом:

```
# chmod +x snort.pl
# perl snorl.pl
```

5. Запустите snort на маршрутизаторе. Snort будет вести журнал в файл /var/log/snort/alert. Чтобы просматривать журнал в режиме реального времени, выполните команду: # tail -f /var/log/snort/alert.

6. На компьютере злоумышленника запустите скрипт snort.pl с параметрами
   <IP-адрес_сервера> 0 0 0
7. Наблюдайте за файлом журнала snort. При выполнении какого-либо правила Snort запишет информацию об этом в журнал. Найдите сработавшее правило и изучите его.

Лабораторная работа № 18.

Туннелирование соединений с использованием протокола SSL.

Цель работы:

Изучение принципов безопасного обмена информации с использованием протокола SSL и ОС Linux.

Порядок выполнения работы:

1. Соберите топологию сети, представленную на рисунке 23.

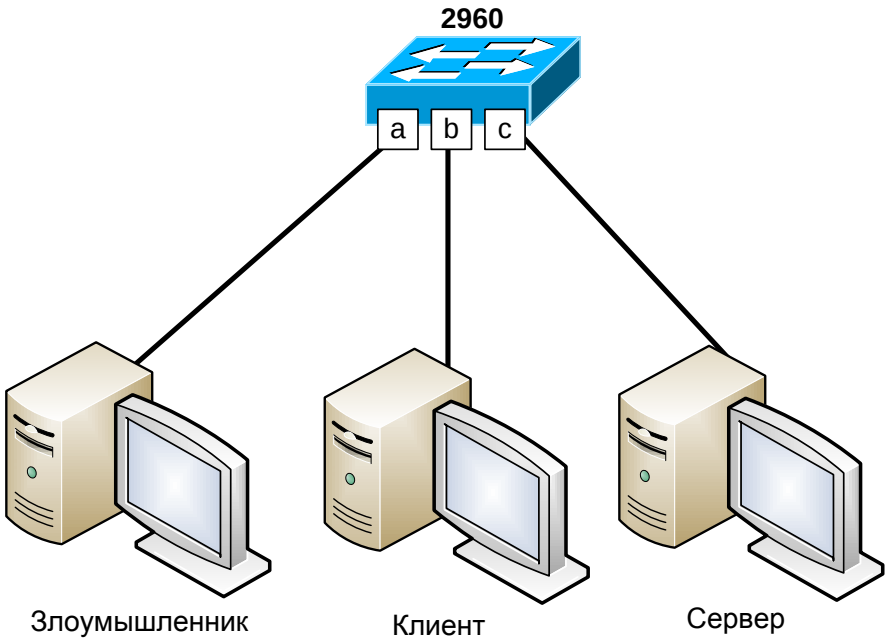

Рисунок 23.

2. Настройте «зеркалирование» (Port Mirroring) на коммутаторе следующим образом: порт «a» – приёмник, порт «b» – источник. Таким образом, злоумышленник сможет «прослушивать» весь трафик клиента.
3. Изучите главу 8.2.4 «Протокол SSL/TLS» теоретического пособия.
4. Запустите на сервер POP3-сервер с авторизацией через /etc/passwd.
5. Получите почту пользователя root с машины клиента. Параллельно с этим процессом запустите утилиту tcpdump на компьютере злоумышленника. Обнаружьте пароль на почтовый ящик в перехваченных пакетах.
6. На сервере запустите утилиту stunnel на 995 порту для запуска почтового сервера.
7. Включите использование SSL/TLS на клиенте. Выполните шаг 5.
8. Сравните перехваченные утилитой tcpdump пакеты.

Лабораторная работа № 19.

Удаленное управление по защищённому протоколу SSH.

Цель работы:

Изучение протокола SSH и способов его применения в ОС Linux.

Порядок выполнения работы:

1. Соберите топологию сети, представленную на рисунке 24.

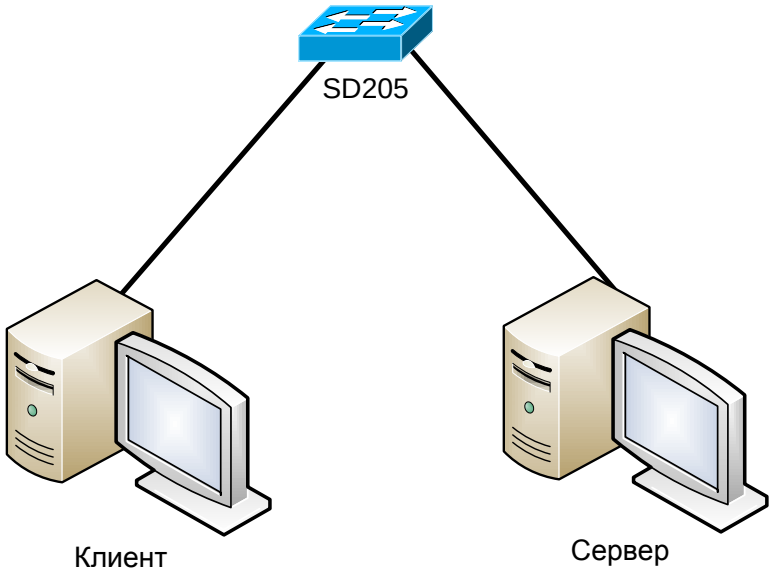

Рисунок 24.

2. Изучите главу 9.2 «Протокол SSH» теоретического пособия.
3. Проверьте, работает ли на компьютерах ssh-сервер (***ps ax | grep ssh***). Если не работает, то запустите его командой ***/etc/rc.d/sshd start***.
4. Попробуйте подключиться с клиента на сервер с использованием протокола SSH. Изучите переданные пакеты с помощью tcpdump. Посмотрите, какие события были отмечены в файле журнала ***/var/log/auth.log***.
5. Перезагрузите удалённый сервер, не подключаясь к нему.
6. Удалённо перезапустите демон ssh без подключения.
7. Подключитесь к удалённому серверу и перезапустите демон ssh. Обратите внимание на то, что сеанс не завершился.
8. Запустите FTP-сервис на сервере.
9. Выполните передачу файла через FTP с помощью утилиты wget. Анализируйте проходящие пакеты с помощью утилиты tcpdump (-XX). Запомните скорость передачи.

10. Выполните передачу файла через ssh. Анализируйте проходящие пакеты с помощью tcpdump (-XX). Запомните скорость передачи. Сравните передаваемые пакеты и скорость передачи данных.
11. Включите сжатие ssh и повторите замер скорости. В каждом тесте анализируйте результаты для файла, состоящего из нулей, для файла, содержащего случайную последовательность (dd if=/dev/urandom of=file bs=1M count=10), для текстового конфигурационного файла и для бинарного файла.
12. Напишите скрипт, который будет создавать файл размеров 10МБ со случайными данными, архивировать его и передавать с удалённой на локальную машину.