Содержание

ВНИМАНИЕ:

Стенд позволяет выполнять большинство лабораторных работ одновременно двум бригадам. Имеются работы, которые рассчитаны на выполнение только одной бригадой (имеется указание).

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

1. Администрирование управляемых коммутаторов

Лабораторная работа № 1.

Знакомство с учебным стендом. Администрирование коммутаторов.

Цель работы:
Изучение структуры стенда, способов коммутации его составляющих. Получение навыков использования утилит для изучения трафика и мониторинга сети. Получение навыков в базовой настройке управляемых коммутаторов. Изучение способов оповещения администратора о системных событиях коммутатора.

Порядок выполнения работы:

1. Изучите раздел 1.1 «Описание комплекта». Найдите все описанные элементы комплекта.
2. С помощью проводов соедините patch-панель и коммутаторы таким образом, чтобы получить топологию, представленную на рисунке 1.

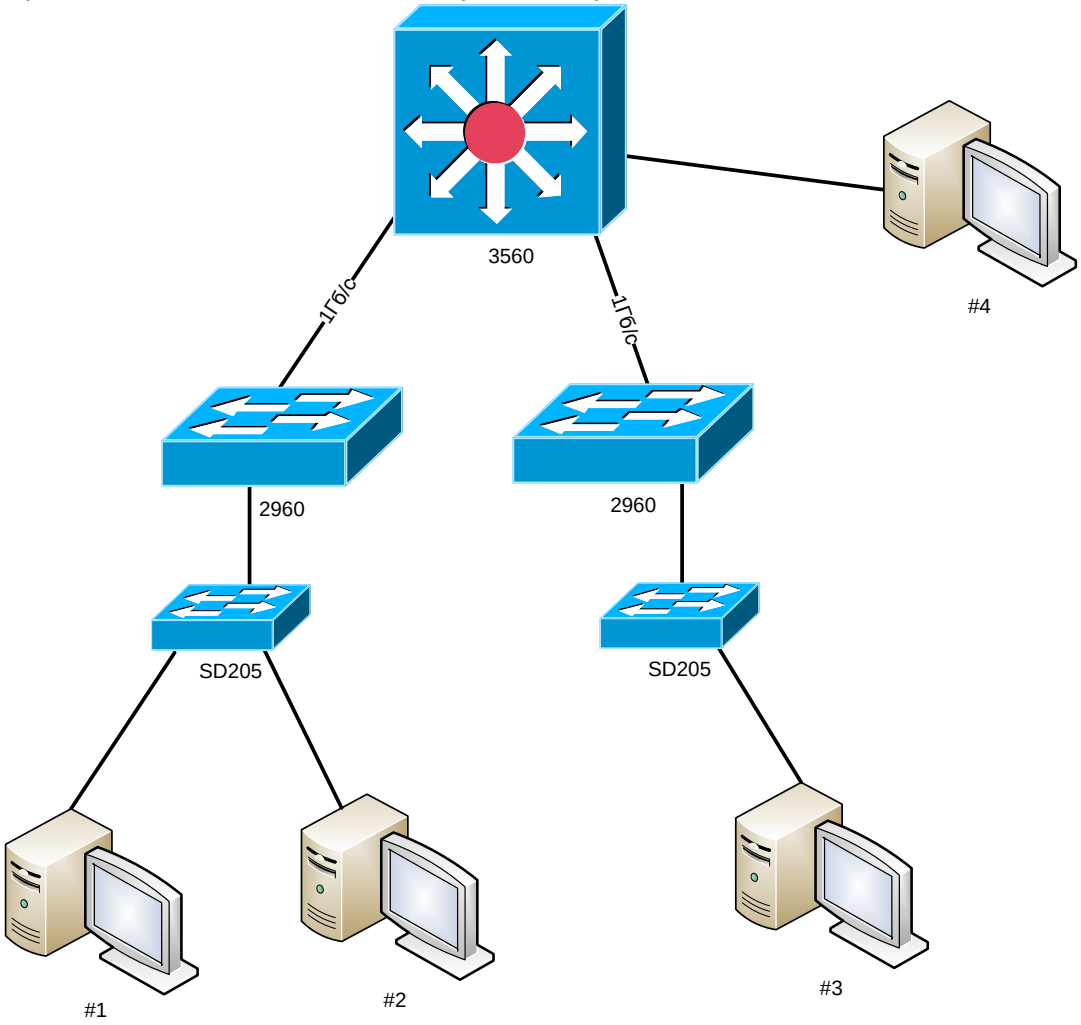

Рисунок 1. Топология коммутируемой сети.

Внимание: далее каждая бригада работает по отдельности со своим коммутатором Cisco 2960

3. Включите рабочие станции и зарегистрируйтесь на них (пользователь – root, пароль – qwerty).
4. Подключитесь к web-интерфейсу управления коммутатором. Зарегистрируйтесь на коммутаторе.

5. Определите MAC-адрес коммутатора и отметьте его на рисунке 1.
6. С помощью утилиты *ifconfig* определите параметры вашего узла. На рисунке отметьте MAC- и IP- адреса всех компьютеров.
7. С помощью утилиты *ping* проверьте связь каждой рабочей станции со всеми другими рабочими станциями созданной сети.
8. С помощью утилиты *arp* просмотрите таблицу ARP на каждой рабочей станции.
9. Назначьте коммутатору IP-адрес из диапазона свободных адресов IP-сети, в которой находятся рабочие станции. На рисунке 1 отметьте IP-адрес коммутатора.
10. С помощью системной утилиты коммутатора Ping проверить связь коммутатора с каждой машиной в сети.
11. Используя утилиту *tcpdump* на любой из машин в сети, убедиться в том, что до заданной машины доходят ICMP-запросы от коммутатора.

12. Создайте на коммутаторе пользователя со статусом «Admin».
13. Выйдите из системы (logout).
14. Зарегистрируйтесь на коммутаторе, используя учётную запись вновь созданного пользователя.
15. Создайте на коммутаторе пользователя со статусом «User».
16. Выйдите из системы (logout).
17. Зарегистрируйтесь на коммутаторе, используя учётную запись пользователя со статусом «User».
18. Попытайтесь выполнить любые действия, связанные с изменением текущих настроек коммутатора. Сделайте выводы об ограниченности прав пользователя со статусом «User».
19. Удалите все созданные Вами учётные записи пользователей.

20. Настройте на одном из компьютеров сервер syslog таким образом, чтобы он мог принимать информацию из сети и записывать её в один определённый файл.
21. Настройте коммутатор таким образом, чтобы он отправлял информацию о системных событиях на сервер журналирования.
22. Сохраните настройки, выйдите из системы и выключите питание коммутатора.
23. Включите питание коммутатора, зарегистрируйтесь на нём, а затем отключите и включите линию связи, подключенную к любому порту коммутатора.
24. При помощи утилиты tcpdump изучите диалог syslog-клиента и syslog-сервера.
25. Проанализируйте содержимое сообщения, полученного сервером журналирования.

26. Запустите на одном из компьютеров сервер DNS.
27. Создайте и настройте DNS-зону «lab.org».
28. На этом же компьютере настройте и запустите SMTP-сервер для зоны «lab.org».
29. Заведите на почтовом сервере следующие учётные записи пользователей: info@lab.org и switch@lab.org.
30. Настройте коммутатор таким образом, чтобы он отсылал информацию о системных событиях на созданные Вами почтовые адреса.
31. Используя почтового клиента «kmail» на втором компьютере, проверьте почту и убедитесь в работоспособности настроенного Вами механизма уведомления о системных событиях коммутатора через почтовые сообщения.
32. При помощи утилиты tcpdump изучите диалог smtp-клиента и smtp-сервера, pop3-клиента и pop3-сервера.

33. На двух компьютерах настройте сервер NTP.
34. Активируйте на коммутаторе клиента SNTP и настройте его на получение информации о времени с настроенных Вами серверов NTP через каждые 30 секунд.
35. При помощи утилиты tcpdump изучите диалог ntp-клиента и ntp-сервера.
36. Определите источник полученной информации о времени и сверьте системное время коммутатора.

37. Сбросьте настройки коммутатора в фабричные и перезагрузите его.

Лабораторная работа № 2.

Управление сетью с помощью протокола SNMP.

Цель работы:
Изучение способов мониторинга и управления сетью на основе протокола SNMP.

Порядок выполнения работы:

1. Постройте топологию сети, показанную на рисунке 3.

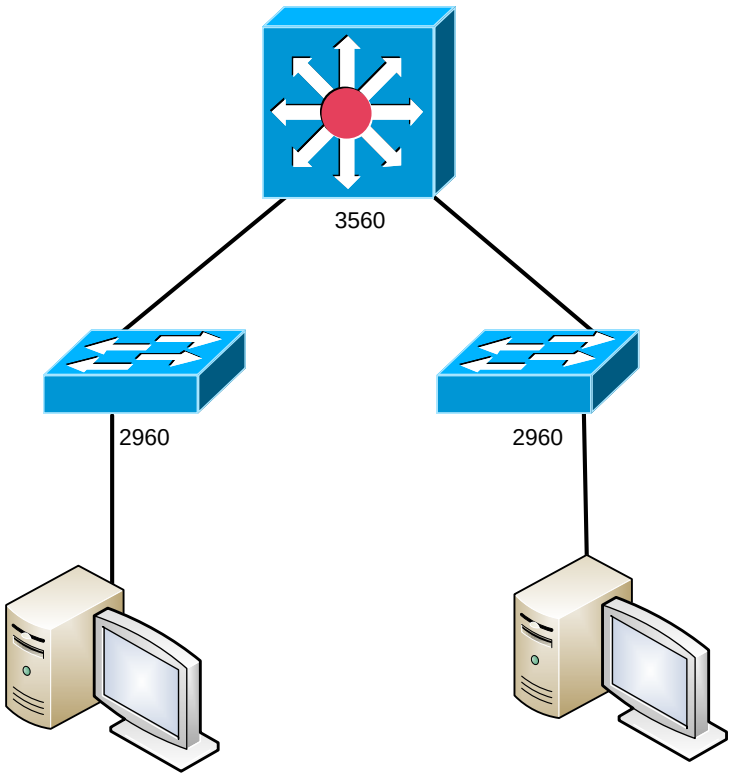

Рисунок 3. Топология коммутируемой сети.

2. Изучите раздел 3.10 «Протокол SNMP» теоретического пособия.
3. Настройте SNMP-протокол на коммутаторах.
4. Запустите утилиту iReasoning MIB Browser.
5. Загрузите базу MIB RFC-1213.
6. На обоих коммутаторах (2960 и 3560) 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).

Лабораторная работа № 3.

Конфигурирование портов и работа с таблицей коммутации.

Цель работы:
Получение навыков настройки портов коммутатора, изучение технологии зеркалирования портов (Port Mirroring) и принципов работы со статической таблицей перенаправления коммутатора.

Порядок выполнения работы:

1. Постройте топологию сети, показанную на рисунке 4.

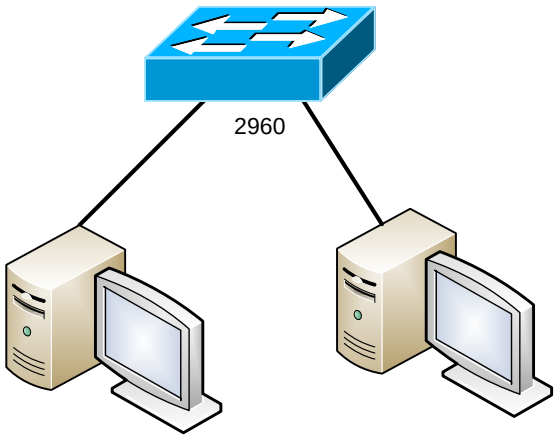

Рисунок 4. Топология коммутируемой сети.

2. Выключите один из портов коммутатора, к которому подключен один из компьютеров.
3. Попробуйте осуществить взаимодействие компьютеров. Сделайте выводы на основе полученного результата.

4. Настройте на коммутаторе зеркало для любого из портов, к которому подключен один из компьютеров.
5. Запустите на машинах, подключенных к порту-источнику и порту-приемнику (зеркалу), утилиту tcpdump. Активизируйте сетевую активность. Сравните результаты работы утилит на обеих машинах.

6. Силами двух бригад соберите топологию сети, представленную на рисунке 5. Все линия связи должны быть подключены к портам с пропускной способностью 100 Мбит/с. Обязательно соблюдайте нумерацию портов.
7. Установите пропускную способность портов коммутатора 2960, к которому подключены машины 3 и 4, равной 10 Мбит/с.
8. Настройте зеркало на коммутаторе 2960, к которому подключены машины 1 и 2, следующим образом: машина 1 – приёмник, машина 2 – источник.
9. «Пингуйте» (утилита ping) одновременно машину 2 с машин 3 и 4.
10. Запустите на машинах 1 и 2 утилиту tcpdump. Сравните результаты работы утилит на обеих машинах.
11. Проделайте действия пунктов 8-12 в обратную сторону.

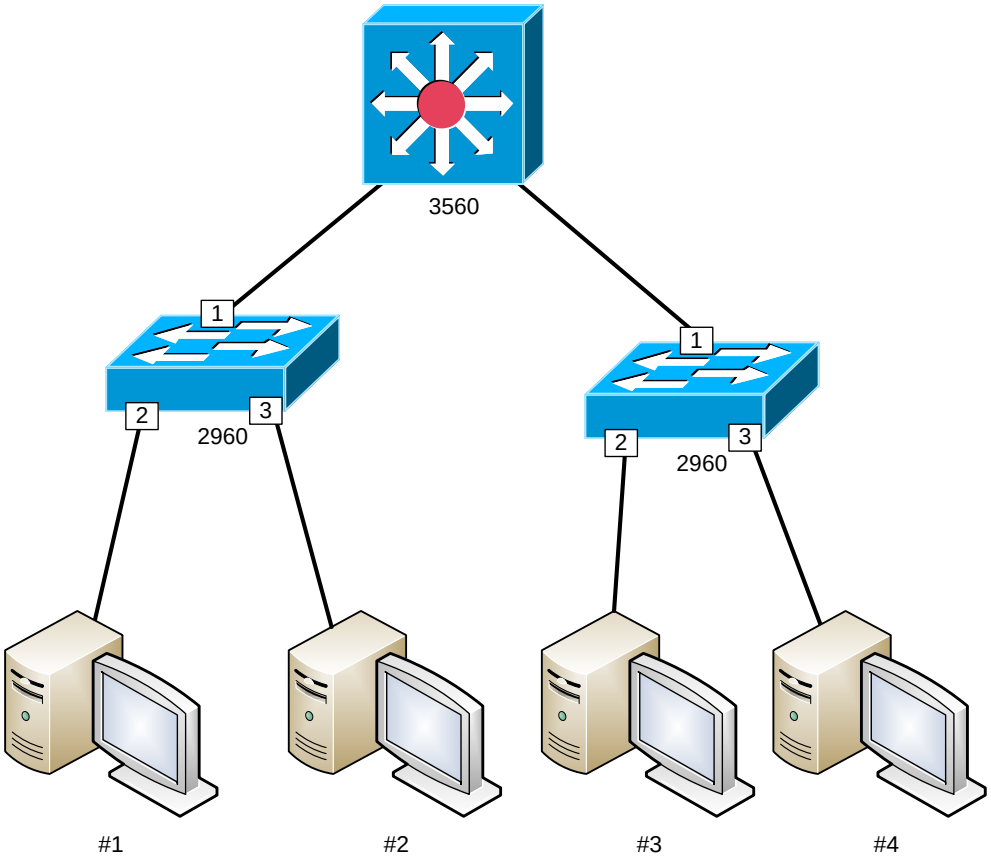

Рисунок 5.

12. Создайте в статической таблице перенаправления коммутатора 2960, к которому подключены машины 1 и 2, следующую некорректную запись: машина #4 подключена к порту 3. Вторая бригада должна сделать то же самое на своём коммутаторе – создать следующую некорректную запись: машина #1 подключена к порту 2.
13. Удалите из таблицы перенаправления все записи, полученные коммутатором в режиме самообучения.
14. «Пингуйте» машину #4 с машины #1 и машину #1 с машины #4.
15. На машинах #2 и #3 запустите утилиту tcpdump и убедитесь, что коммутатор перенаправляет пакеты в соответствие с созданными Вами некорректными записями в таблице коммутации.

16. Сбросьте настройки коммутатора в фабричные и перезагрузите его.

2. Технологии канального уровня

Лабораторная работа № 4.

Виртуальные локальные сети VLAN.

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 1.5 «Виртуальные сети. Сети на базе маркированных кадров» теоретического пособия.
2. Постройте топологию сети, представленную на рисунке 6.

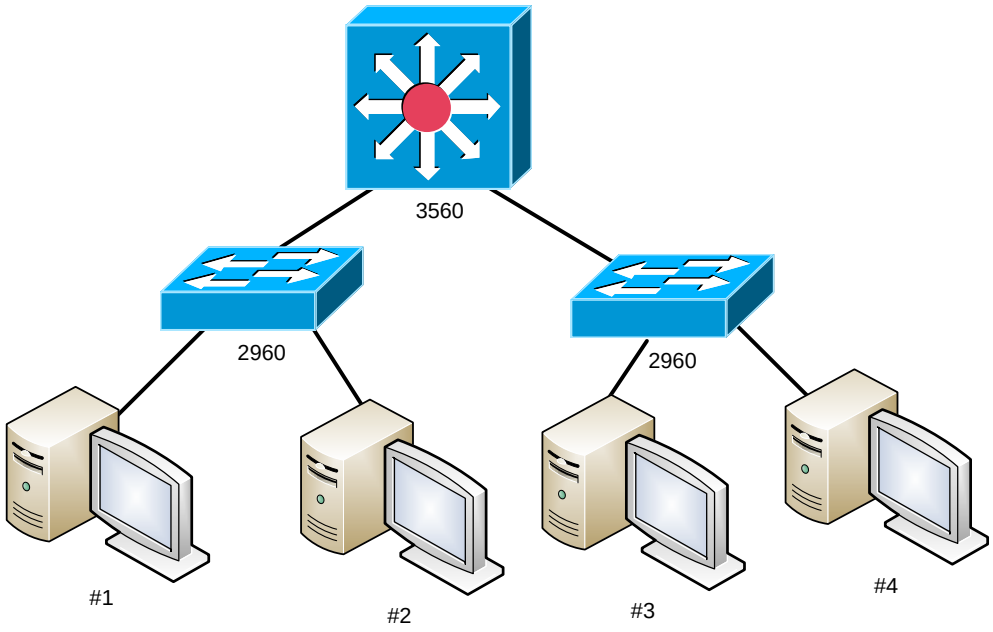

Рисунок 6. Коммутируемая топология для настройки виртуальных сетей VLAN.

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 коммутатора в фабричные и перезагрузите его.

Лабораторная работа № 5.

Построение магистральных линий связи.

Цель работы:
Изучение технологии агрегирования каналов связи (Link Aggregation, Trunking).

Порядок выполнения работы:

1. Постройте топологию сети, показанную на рисунке 7.
2. Одновременно запустите процессы передачи файла с машины 1 на машину 3 и с машины 2 на машину 4. Определите время передачи (*подсказка: удобнее пользоваться утилитой ftp, которая автоматически определяет время передачи*).
3. Изучите раздел 1.4 «Объединение портов в магистральные линии связи» теоретического пособия.

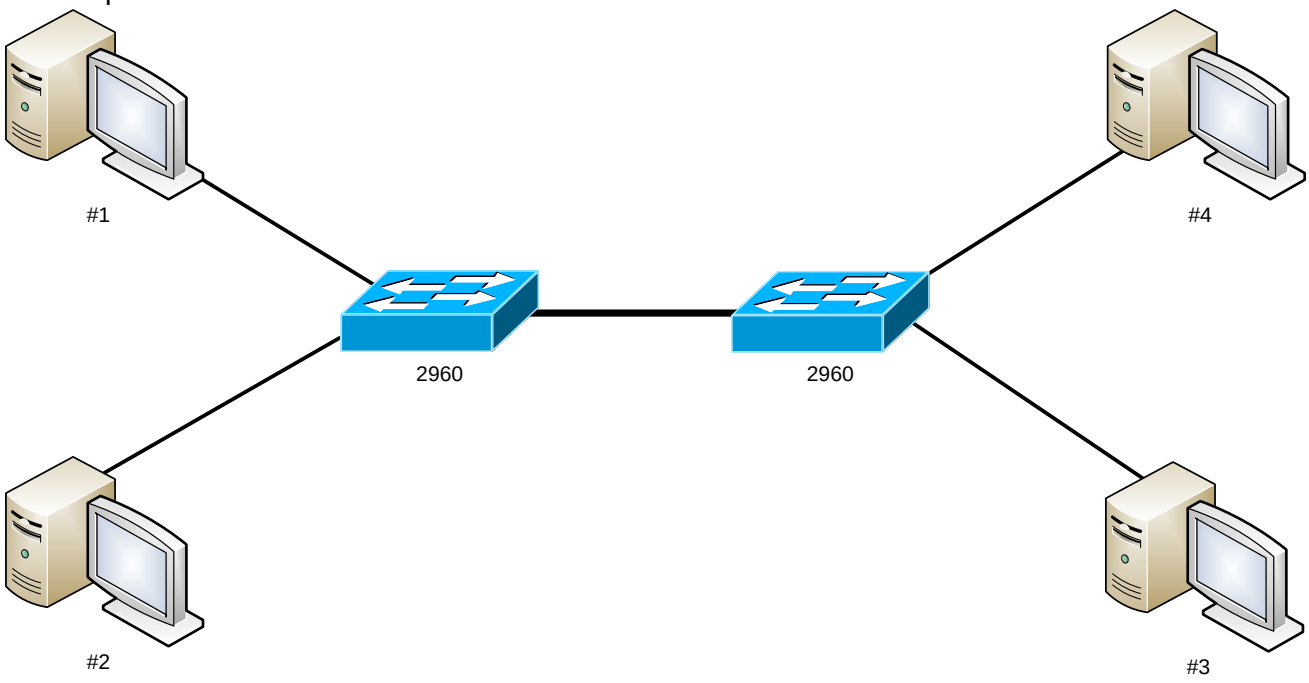

Рисунок 7. Топология коммутируемой сети.

4. Создайте магистраль между коммутаторами, включающую 2 порта.
5. Одновременно запустите процессы передачи файла с машины 1 на машину 3 и с машины 2 на машину 4. Определите время передачи и сравните его со временем, полученным в пункте 10.
6. Удалите созданную магистраль и соедините коммутаторы через гигабитные порты.
7. Одновременно запустите процессы передачи файла с машины 1 на машину 3 и с машины 2 на машину 4. Определите время передачи и сравните его с предыдущими полученными значениями. Сделайте вывод.

Лабораторная работа № 6.

Протокол IGMP.

Цель работы:
Изучение протокола IGMP и способов его настройки на коммутаторах и маршрутизаторах.

Порядок выполнения работы:

1. Постройте топологию сети, показанную на рисунке 8.

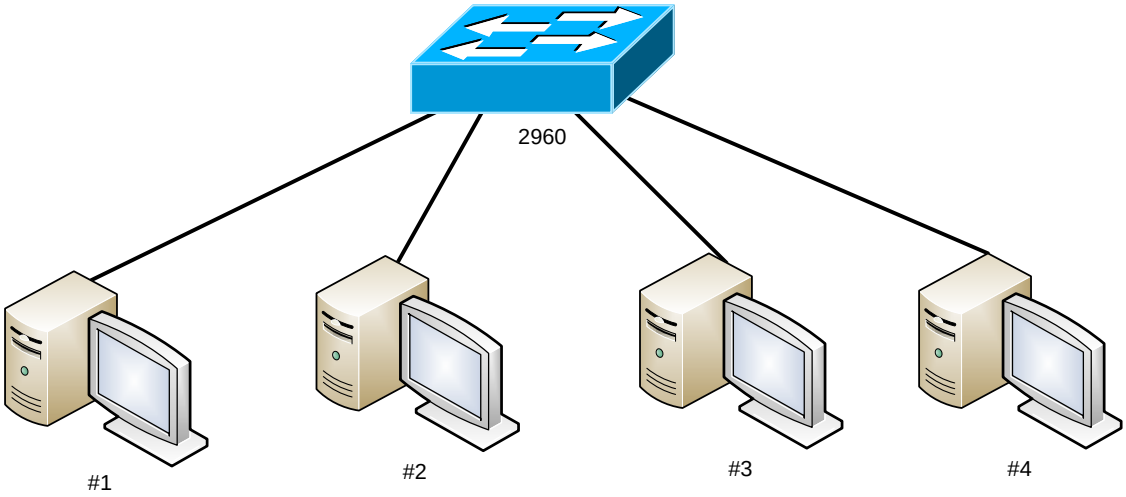

Рисунок 8.

2. Изучите раздел 3.2 «Протокол IGMP» теоретического пособия.
3. Создайте на коммутаторе дополнительную виртуальную сеть «Multicast», которая включает машины 1 и 3.
4. Для VLAN «Multicast» включите поддержку протокола IGMP.
5. Запустите на машине 1 сервер вещания медиапотока.
6. Сделайте попытку принять данный поток со всех остальных машин.
7. Ответьте, какие машины в итоге получают медиапоток, а какие – нет.
8. С помощью утилиты tcpdump отследите пути распространения мультикаст-трафика в сети.

9. Постройте топологию сети, показанную на рисунке 9.
10. Создайте две IP-подсети на коммутаторе 3560 и настройте протокол IGMP для каждой подсети.
11. На обоих коммутаторах 2960 настройте протокол IGMP, используя функцию IGMP Snooping.
12. Запустите на машинах 1 и 3 сервера вещания. Настройте машину 2 на получения медиапотока от сервера 3, а машину 4 – от сервера 1.

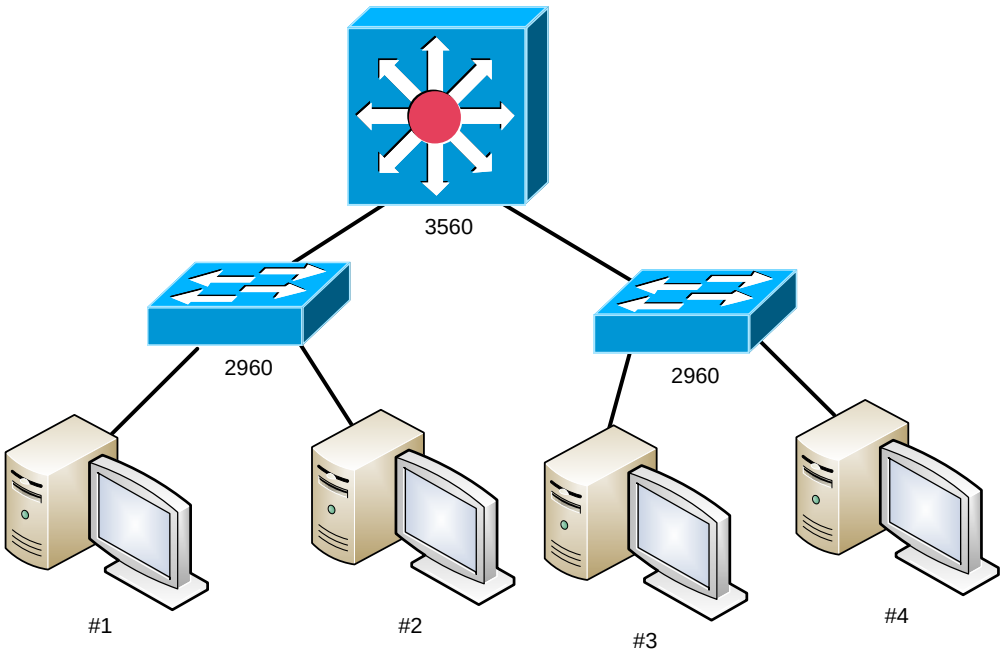

Рисунок 9.

13. Убедитесь в том, что сеть функционирует правильно.
14. Используя средства мониторинга коммутатора 3560 выясните, какие IGMP-группы присутствуют в сети и кто в них входит.

15. Сбросьте настройки коммутаторов в фабричные и перезагрузите их.

Лабораторная работа № 7.

Алгоритмы связующего дерева Spanning Tree.

Цель работы:
Изучение алгоритма Spanning Tree и Rapid Spanning Tree. Получение навыков построения сети с поддержкой резервных линий связи.

Порядок выполнения работы:

1. Изучите раздел 1.6 «Протоколы связующего дерева» теоретического пособия.
2. Соберите сеть с топологией, представленной на рисунке 10.

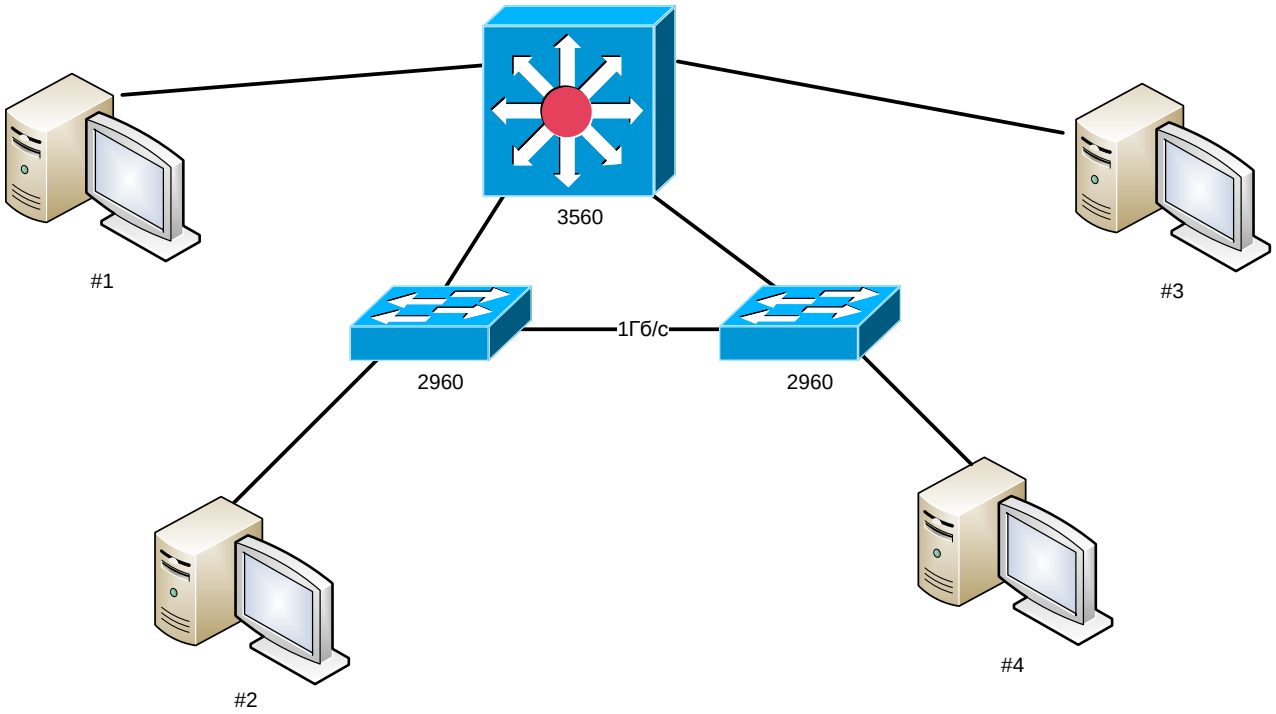

Рисунок 10. Топология коммутируемой сети.

3. Активизируйте на всех коммутаторах протокол Spanning Tree.
4. Настройте приоритеты коммутаторов и портов таким образом, чтобы получить сеть, показанную на рисунке 11 (пунктиром показана резервная связь)
5. С помощью системы мониторинга убедитесь, что через порт коммутатора 2960 #1, отмеченного черным квадратом, трафик не идет. Проверьте остальные задействованные в работе порты. Результаты мониторинга сохраните.
6. Имитируйте сбой в сети, нарушив соединение, выделенное на рисунке 8 жирной линией. В соответствии с алгоритмом Spanning Tree сеть должна быть переконфигурирована. Убедитесь в этом с помощью системы мониторинга коммутаторов. Определите время сходимости сети. Результаты сохраните.

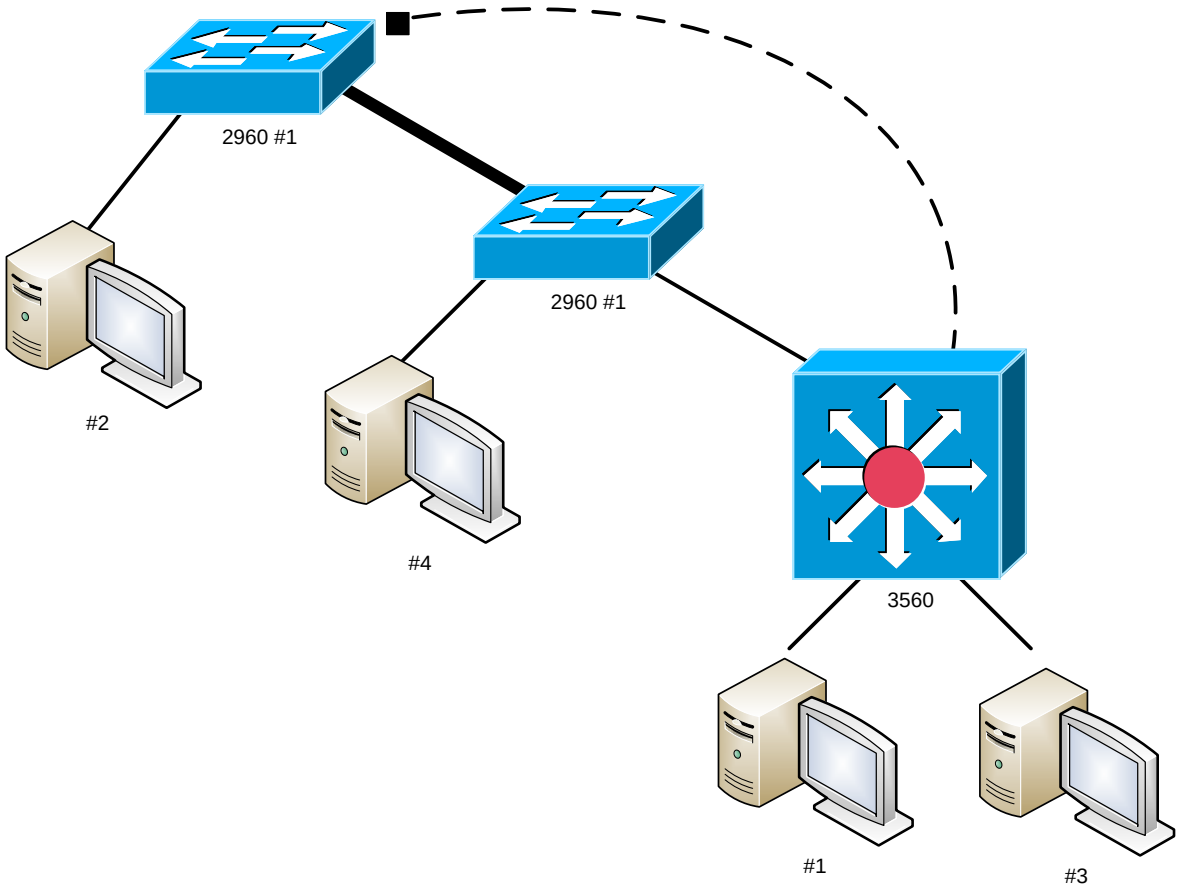

Рисунок 11. Топология сети после применения алгоритма STA.

7. Активизируйте на всех коммутаторах протокол Rapid Spanning Tree.
8. Повторите действия пунктов 4-6.
9. Сравните времена сходимости, полученные при использовании двух протоколов: STP и RSTP. Сделайте выводы.

10. Сбросьте настройки коммутатора в фабричные и перезагрузите его.

3. Технологии управления качеством сервиса

Лабораторная работа № 8.

Обеспечение качества передачи мультимедийного трафика с использованием протокола IEEE 802.1p.

Цель работы:
Получить навык работы с технологией CoS и протоколом IEEE 802.1p путём улучшения качества передачи видеопотока параллельно с потоком передачи файла.

Суть работы:
На собранной топологии сети запустить два процесса передачи данных: видеопоток и поток передачи файла. Оценить качество передачи видеоданных – оно будет низким. Настроить технологию CoS на коммутаторе таким образом, чтобы дать больший приоритет потоку видеоданных. Провести эксперимент заново и убедиться, что качество передачи видеопотока увеличилось.

Порядок выполнения работы:

1. Соберите топологию сети, представленную на рисунке 12.

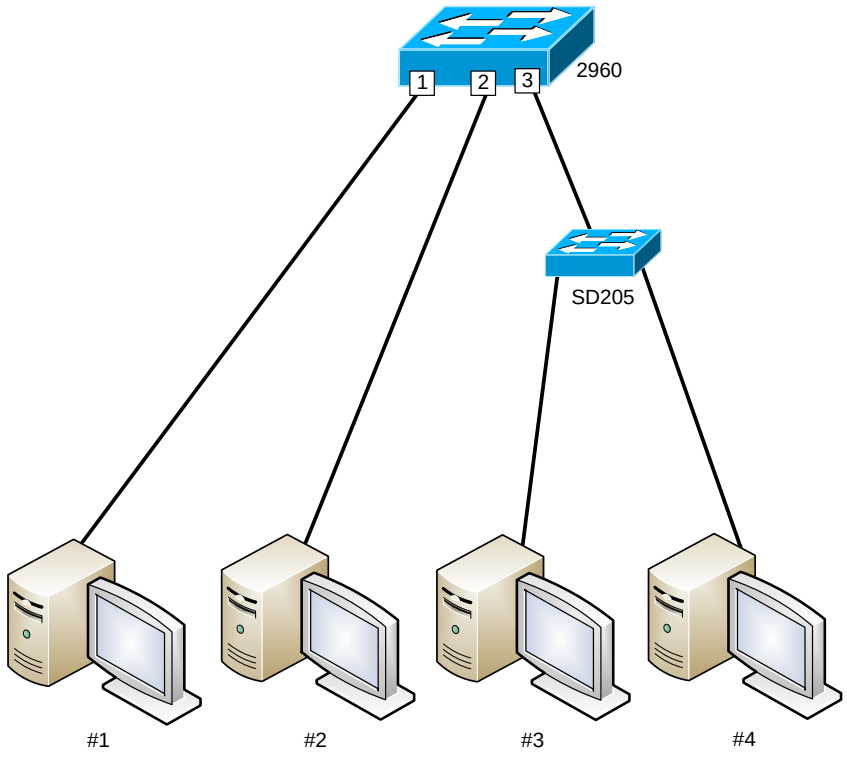

Рисунок 12.

2. Изучите раздел 1.7 «Технология QoS» теоретического пособия.
3. Установите пропускную способность 3-го порта равной 512 Кбит/с.
4. Запустите два потока передачи данных (видео-ролик находится в /root/Desktop/Media):
   - ✓ машина #1 – сервер видеовещания (с использованием VLC-плеера);
   - ✓ машина #2 – FTP-сервер;
   - ✓ машина #3 – клиент, принимающий видеоданные;
   - ✓ машина #4 – FTP-клиент, принимающий файл размером 1Гб из каталога /srv/ftp/.
5. Определите качества передачи видео и время передачи файла.

6. Настройте коммутатор таким образом, чтобы классификация входящего трафика осуществлялась на основе поля 802.1p.

7. Назначьте каждому потоку приоритет: видеопоток от машины #1, поступающий на 1-ый порт, должен иметь более высокий приоритет, чем файловый поток от машины #2, поступающий на 2-ой порт.
8. Настройте коммутатор таким образом, чтобы более приоритетный трафик попадал в выходную очередь Q3, менее приоритетный трафик – в очередь Q1.
9. Снова запустите два потока передачи данных и определите качества передачи видео и время передачи файла.

10. Настройте алгоритм обработки выходных очередей на WRR.
11. Снова запустите два потока передачи данных и определите качества передачи видео и время передачи файла.
12. Сделайте выводы на основе полученных результатов.

Сбросьте настройки коммутатора в фабричные и перезагрузите его.

4. Безопасность

Лабораторная работа № 9.

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 14.

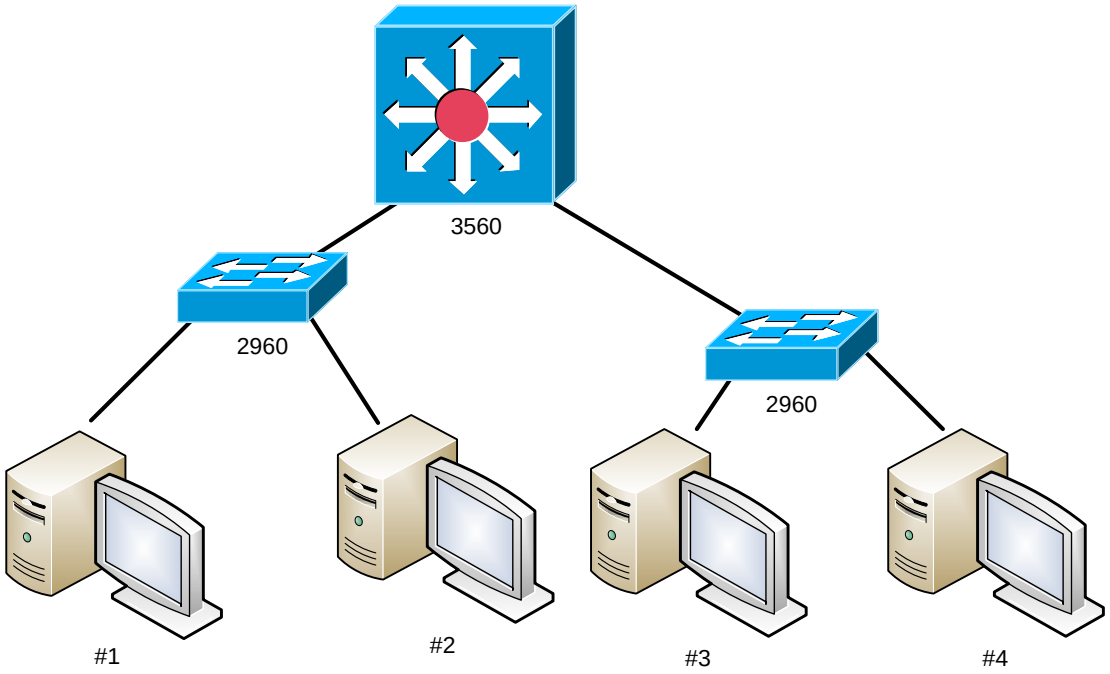

Рисунок 14.

2. Настройте коммутаторы 2960 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 2960 таблицу коммутации в режиме Permanent.
8. Попытайтесь осуществить взаимодействие с 4-ым компьютером. Объясните полученный результат.

9. Сбросьте блокировку таблиц коммутации.
10. Используя технологию IP Source Guard, настройте на коммутаторах 2960 фильтры таким образом, чтобы в сети могли работать только машины #1 и #3.

11. Сбросьте настройки коммутатора в фабричные и перезагрузите его.

Лабораторная работа № 10.

Безопасность на основе сегментации трафика.

Цель работы:
Изучение механизма сегментации трафика.

Порядок выполнения работы:

1. Соберите топологию сети, представленную на рисунке 15.

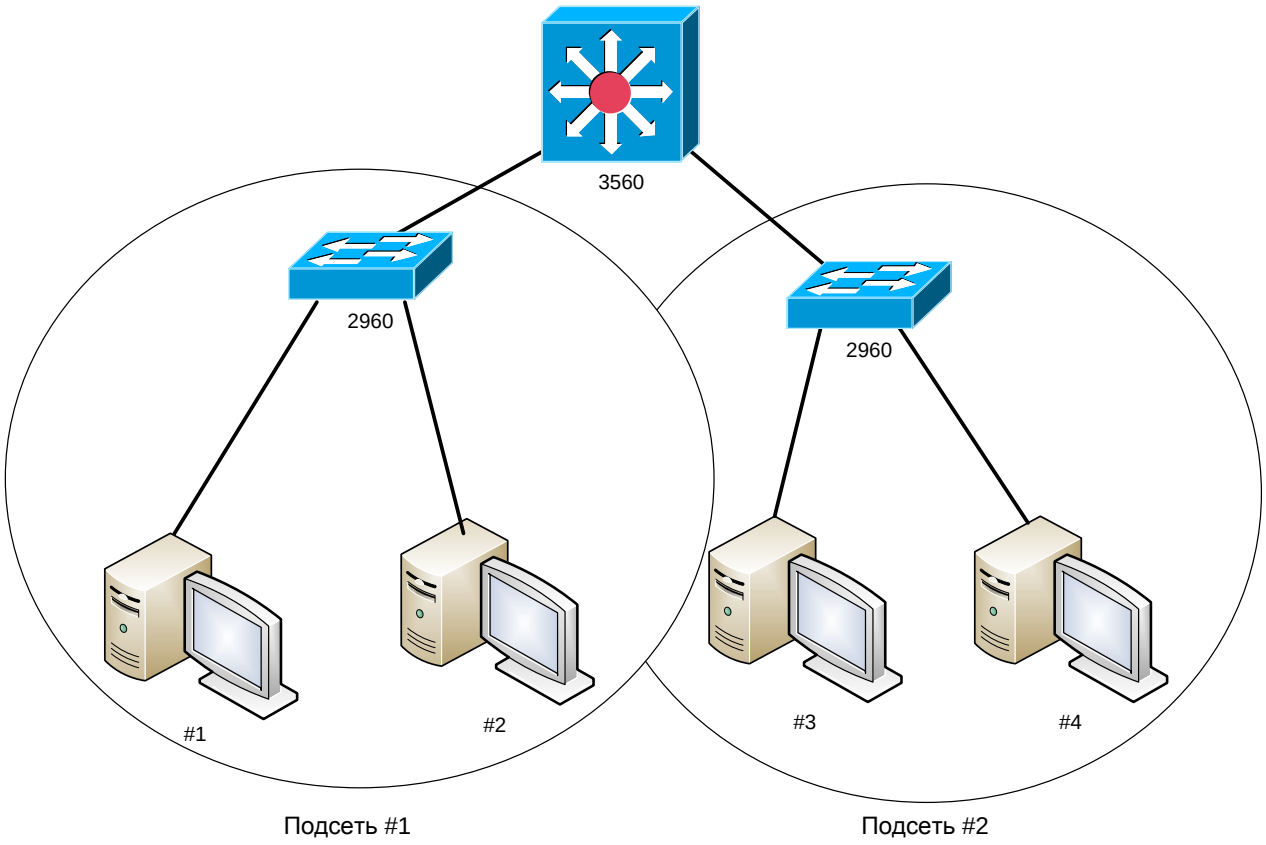

Рисунок 15. Топология коммутируемой сети.

2. Создайте IP-подсети, как это показано на рисунке 15. Назначьте каждому компьютеру IP-адрес из собственной подсети.

3. Изучите раздел 2.6 «Сегментация трафика» теоретического пособия.
4. Организуйте на каждом из коммутаторов 2960 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. Подтвердите правильность сделанных настроек.

6. Сбросьте настройки коммутатора в фабричные и перезагрузите его.

Лабораторная работа № 11.

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.

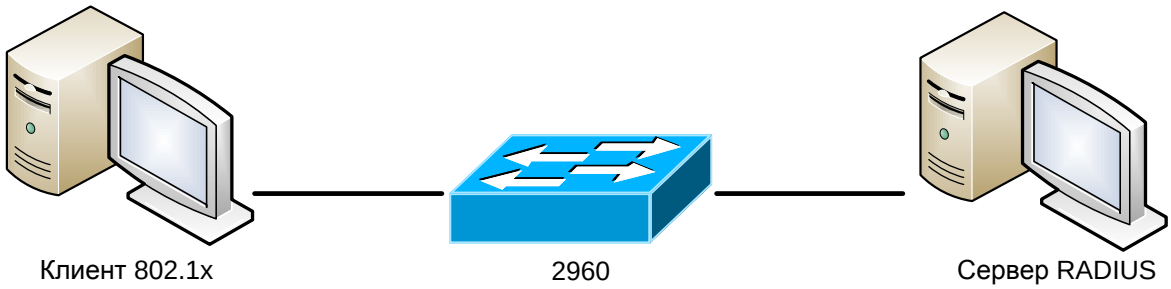

Рисунок 16. Топология коммутируемой сети.

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.

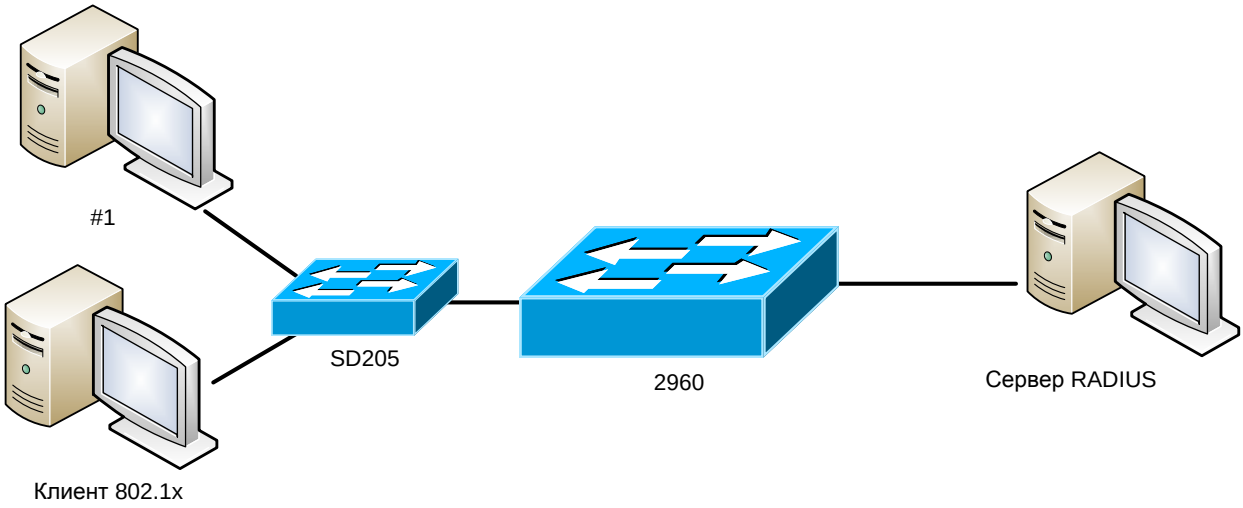

Рисунок 17. Топология коммутируемой сети.

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.

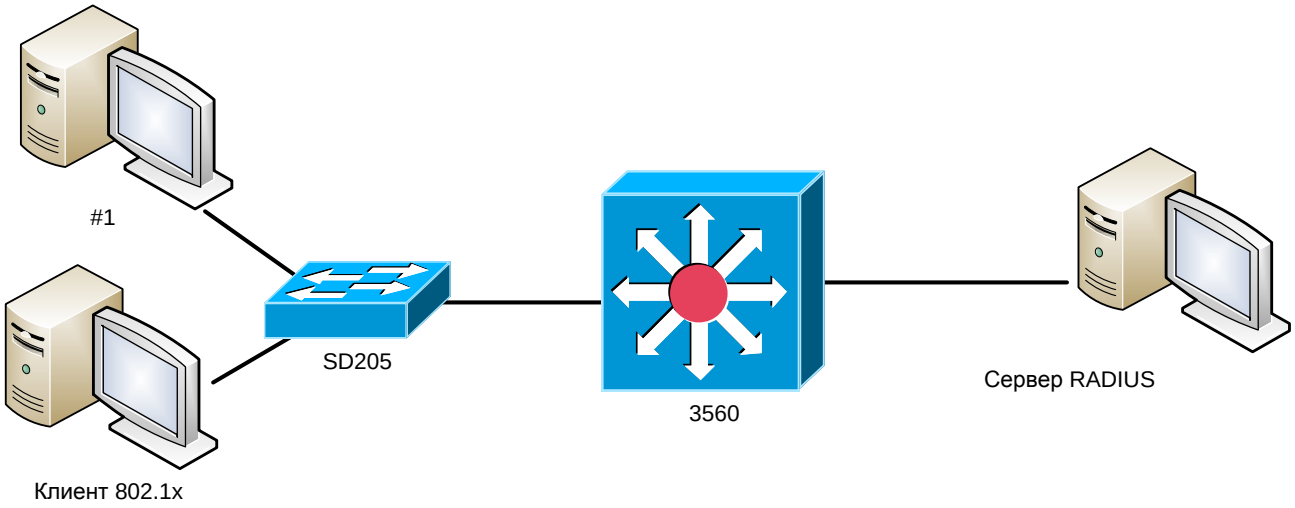

Рисунок 18. Топология коммутируемой сети.

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 № 12.

Списки контроля доступа ACL.

Цель работы:
Изучение технологии Access Control Lists.

Порядок выполнения работы:

1. Соберите сеть с топологией, представленной на рисунке 19.

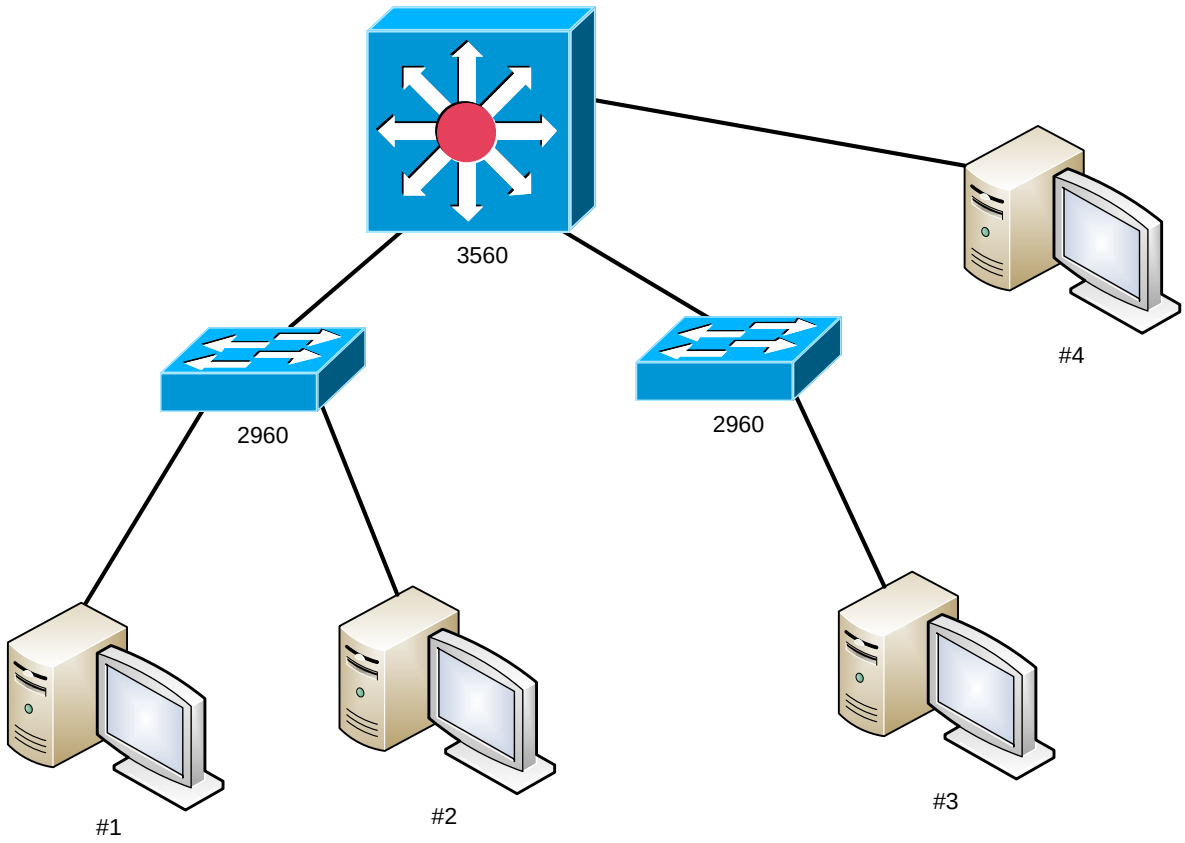

Рисунок 19. Топология коммутируемой сети.

2. Изучите раздел 2.5 «Списки контроля доступа» теоретического пособия.
3. Настройте списки контроля доступа таким образом, чтобы:
   - ни один из коммутаторов 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.

5. Технологии коммутации третьего уровня

Лабораторная работа № 13.

Основы коммутации третьего уровня.

Цель работы:
Изучение принципов работы коммутатора уровня 3.

Порядок выполнения работы:

1. Соберите сеть с топологией, представленной на рисунке 23.

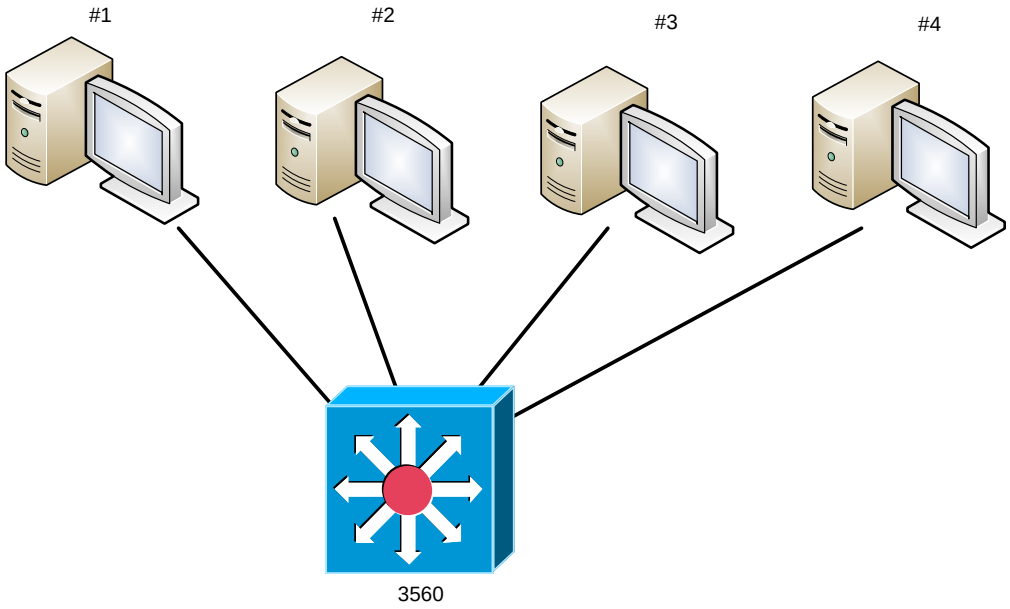

Рисунок 23. Топология коммутируемой сети.

2. Включите машины в виртуальные сети в соответствие со следующей таблицей:

Номер машины	Номер VLAN
1	1
2	2
3	2
4	3

3. Включите виртуальные сети в IP-подсети в соответствие со следующей таблицей:

Номер VLAN	IP-подсеть
1	192.168.1.0/24
2	192.168.2.0/24
3	192.168.3.0/24

4. Назначьте каждой машине IP-адрес из подсети, в которую она входит.
5. Проверить взаимодействие между всеми машинами.
6. С помощью утилиты traceroute выясните маршрут между любыми двумя машинами из разных подсетей.

7. Просмотрите содержимое ARP таблицы на коммутаторе и выясните MAC-адреса машин по их IP-адресу.

8. Запустите FTP-сервер на машине № 3.
9. Используя протокол FTP, скачайте с машины №3 на машину № 1 следующие файлы, находящиеся в каталоге /srv/ftp/*: 20Mb, 200Mb, 500Mb, 1Gb*. Заполните следующую таблицу:

Файл	Время передачи, мс
20Mb	
200Mb	
500Mb	
1Gb	

10. Соберите сеть с топологией, представленной на рисунке 24.

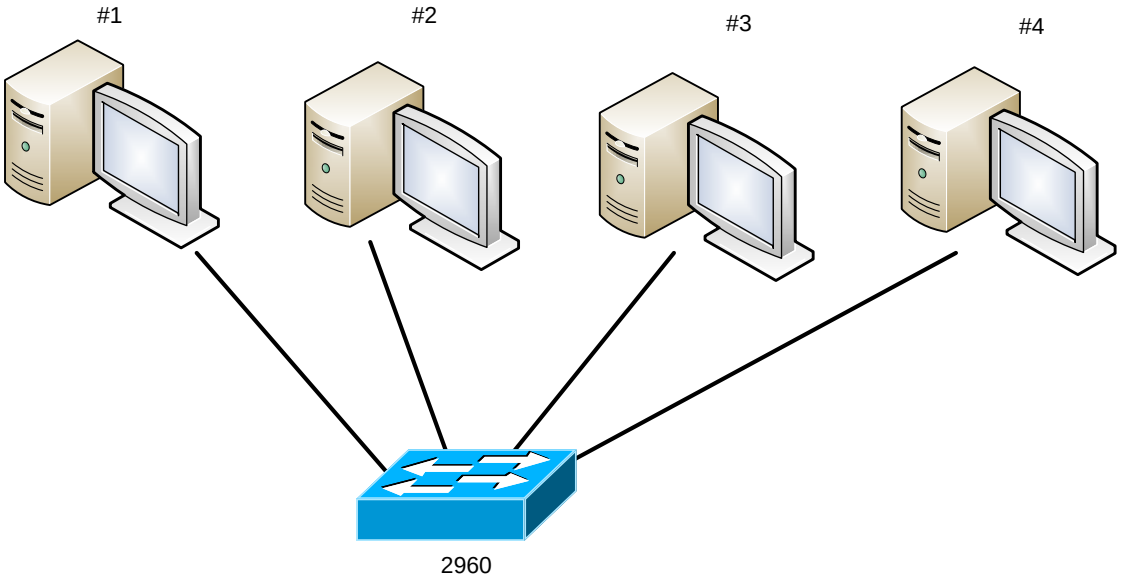

Рисунок 24. Топология коммутируемой сети.

11. Повторите действия пункта 9 и заполните следующую таблицу:

Файл	Время передачи, мс
20Mb	
200Mb	
500Mb	
1Gb	

12. Сравните времена скачивания одного и того же файла для сетей, построенных на различных принципах (уровнях) коммутации. Сделайте выводы.

13. Сбросьте настройки коммутатора в фабричные и перезагрузите его.

Лабораторная работа № 14.

Протокол маршрутизации OSPF-2.

Цель работы:

Изучить протокол OSPF. Получить практические навыки в построения маршрутизирующих сетей на базе протокола OSPF.

Порядок выполнения работы:

1. Соберите топологию сети и установите пропускную способность каналов такой, как указано на рисунке 23.

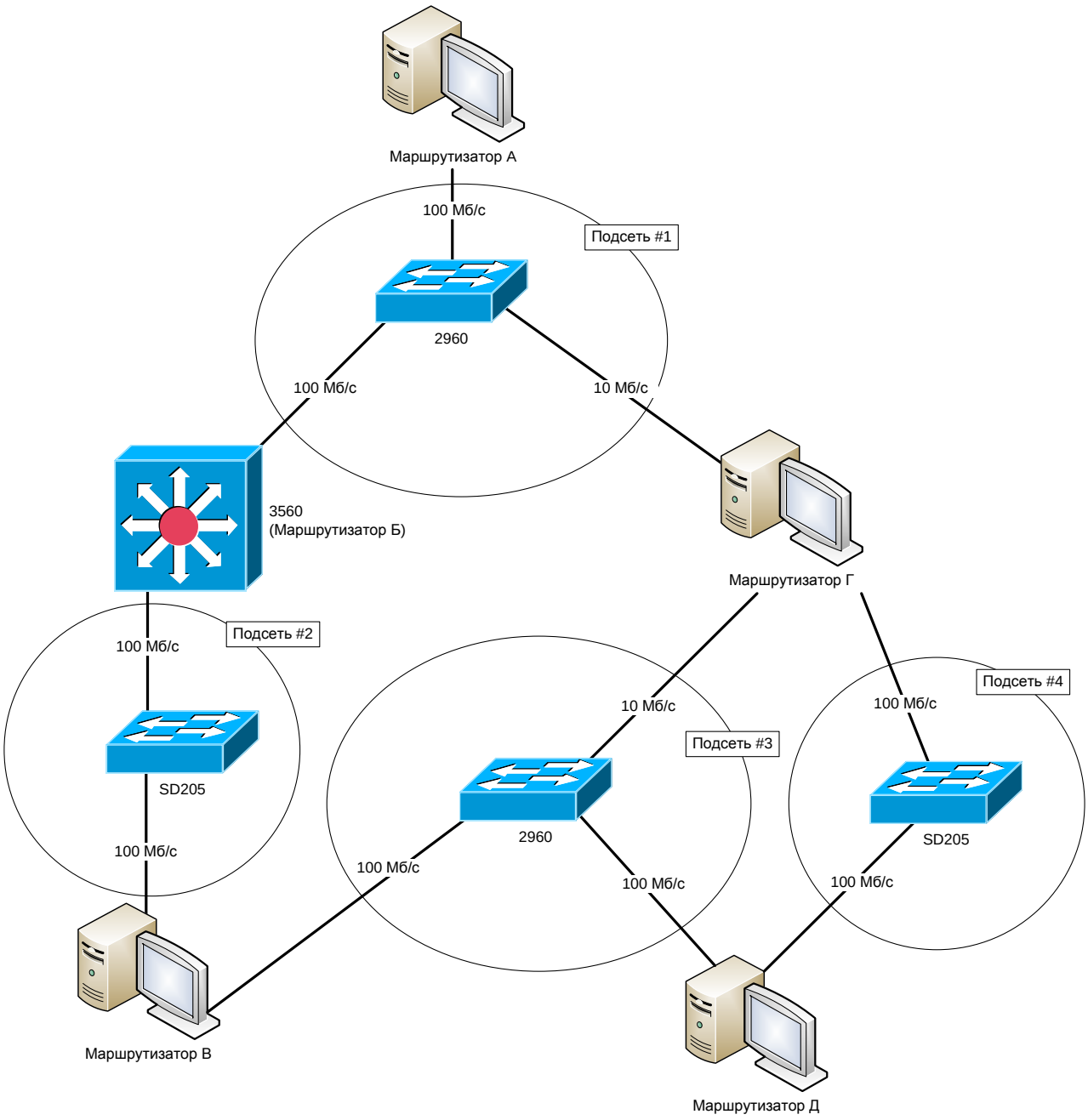

Рисунок 23. Топология коммутируемой сети.

2. Придумайте номера подсетей. На каждом из маршрутизаторов назначьте на сетевые интерфейсы IP-адреса в соответствие с подсетью, которой он принадлежит.

3. Изучите раздел 3.6 «Протокол маршрутизации OSPF» теоретического пособия.
4. Настройте протокол OSPF: на маршрутизаторе Б – штатными средствами управления коммутатором, на остальных маршрутизаторах – с использованием сервиса *quagga* (не забудьте включить функцию маршрутизации).
5. Проверьте работоспособность сети.

6. Рассчитайте стоимость для каждого интерфейса.
7. Осуществите взаимодействие между маршрутизаторами А и Д и выясните, по какому маршруту проходят пакеты.
8. Имитируйте сбой в сети на активном маршруте. Определите новый маршрут следования пакетов и время сходимости протокола OSPF в данном случае.

9. Определите, как изменилась таблица маршрутизации на клиенте, программных и аппаратном маршрутизаторах.
10. С помощью утилиты tcpdump изучите процессы, происходящие в сети, в которой используются протокол динамической маршрутизации OSPF-2.
11. Используя утилиту telnet, изучите процессы, происходящие внутри демона маршрутизации. Сравните таблицы маршрутизации ядра операционной системы и демона динамической маршрутизации.

12. Сбросьте настройки коммутатора в фабричные и перезагрузите его.