

Содержание

1. Администрирование управляемых коммутаторов	3
Лабораторная работа № 1.	3
Знакомство с учебным стендом. Администрирование коммутаторов.	3
Лабораторная работа № 2.	5
Управление сетью с помощью протокола SNMP.	5
Лабораторная работа № 3.	6
Конфигурирование портов и работа с таблицей коммутации.	6
2. Технологии канального уровня	8
Лабораторная работа № 4.	8
Виртуальные локальные сети VLAN.	8
Лабораторная работа № 5.	9
Построение магистральных линий связи.	9
Лабораторная работа № 6.	10
Протокол IGMP.	10
Лабораторная работа № 7.	12
Алгоритмы связующего дерева Spanning Tree.	12
3. Технологии управления качеством сервиса.....	14
Лабораторная работа № 8.	14
Обеспечение качества передачи мультимедийного трафика с использованием протокола IEEE 802.1p.	14
Лабораторная работа № 9.	16
Технология QoS.	16
4. Безопасность	18
Лабораторная работа № 10.	18
Базовые механизмы безопасности коммутаторов.	18
Лабораторная работа № 11.	19
Безопасность на основе сегментации трафика.	19
Лабораторная работа № 12.	20
Безопасность на основе протокола IEEE 802.1x.	20
Лабораторная работа № 13.	23
Списки контроля доступа ACL.	23
Лабораторная работа № 14.	24
Технология виртуальных частных сетей.	24
Лабораторная работа № 15.	25
Технология Network Address Translation.	25
5. Технологии коммутации третьего уровня	26
Лабораторная работа № 16.	26
Основы коммутации третьего уровня.	26

6. Маршрутизация в глобальных сетях	28
Лабораторная работа № 17.	28
Статическая маршрутизация.	28
Лабораторная работа № 18.	29
Протокол маршрутизации EIGRP.	29
Лабораторная работа № 19.	32
Протокол маршрутизации OSPF-2.	32
Лабораторная работа № 20.	34
Протокол маршрутизации BGP.	34
7. Технологии Транспортного и Прикладного уровней	35
Лабораторная работа № 21.	35
Протоколы TCP и UDP.	35
Лабораторная работа № 22.	36
Динамическая конфигурация узла с использованием протокола DHCP.	36
Лабораторная работа № 23.	37
Настройка протокола DNS.....	37
8. Сетевые технологии операционной системы Linux	38
Лабораторная работа № 24.	38
Пользователи Linux и система PAM.	38
Лабораторная работа № 25.	39
Настройка межсетевого экрана в Linux.....	39
Лабораторная работа № 26.	40
Работа с файловым сервером в Linux.	40
Лабораторная работа № 27.	41
Настройка сервера Samba.	41
Лабораторная работа № 28.	42
Работа с сетевой файловой системой NFS.....	42

ВНИМАНИЕ:

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.

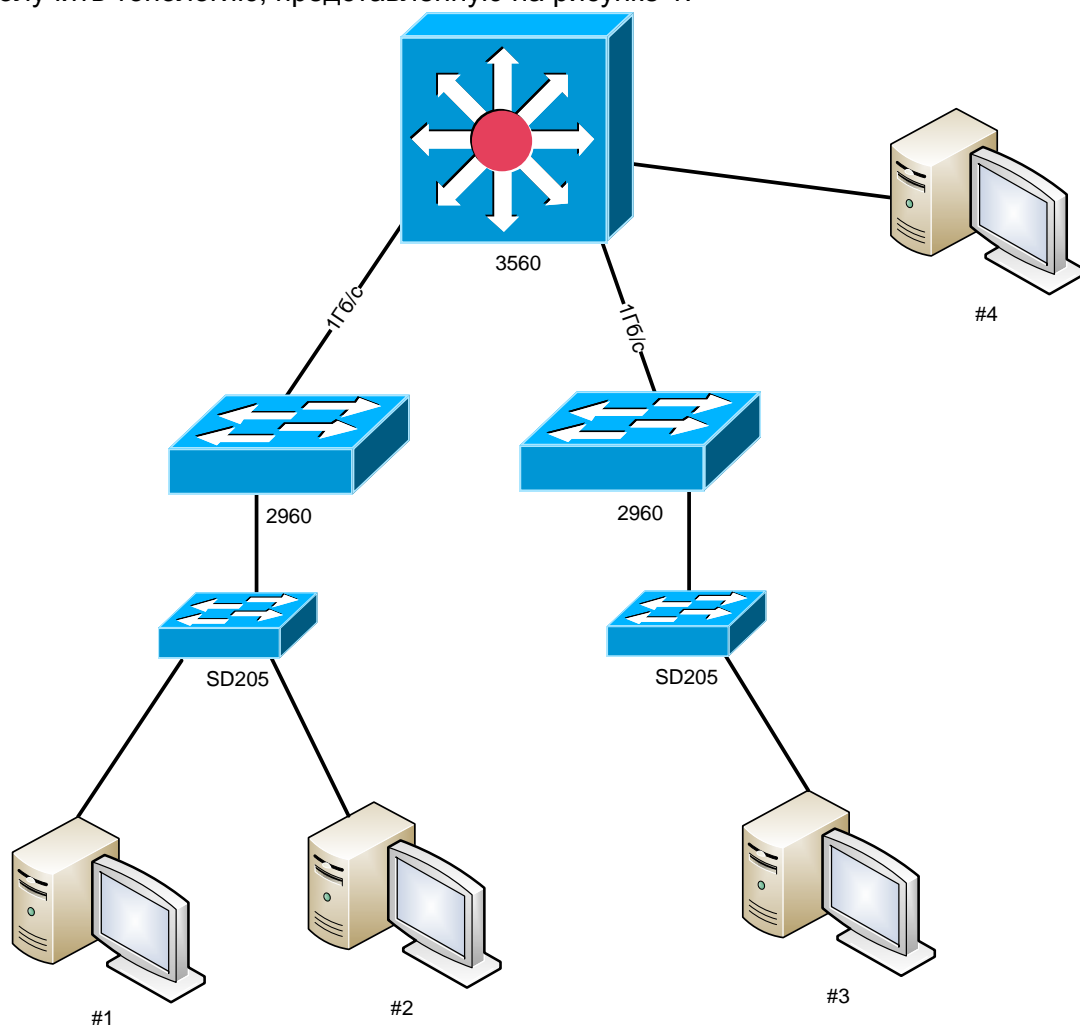


Рисунок 1. Топология коммутируемой сети.

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.

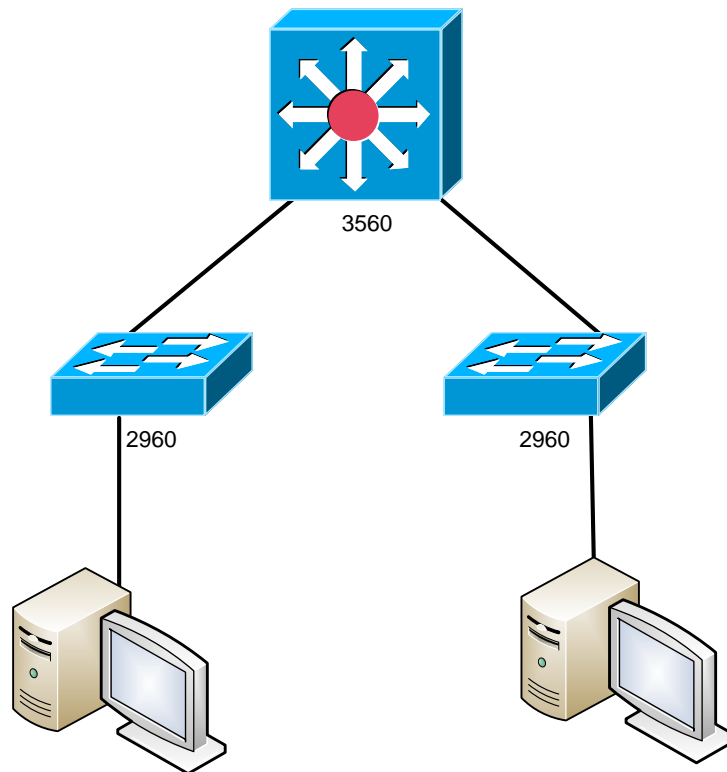


Рисунок 3. Топология коммутируемой сети.

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.

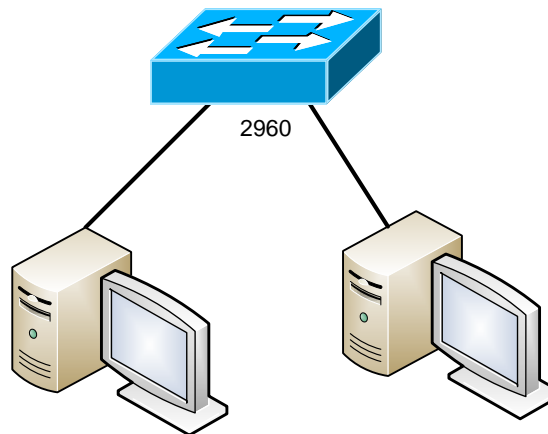


Рисунок 4. Топология коммутируемой сети.

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. Прodelайте действия пунктов 8-12 в обратную сторону.

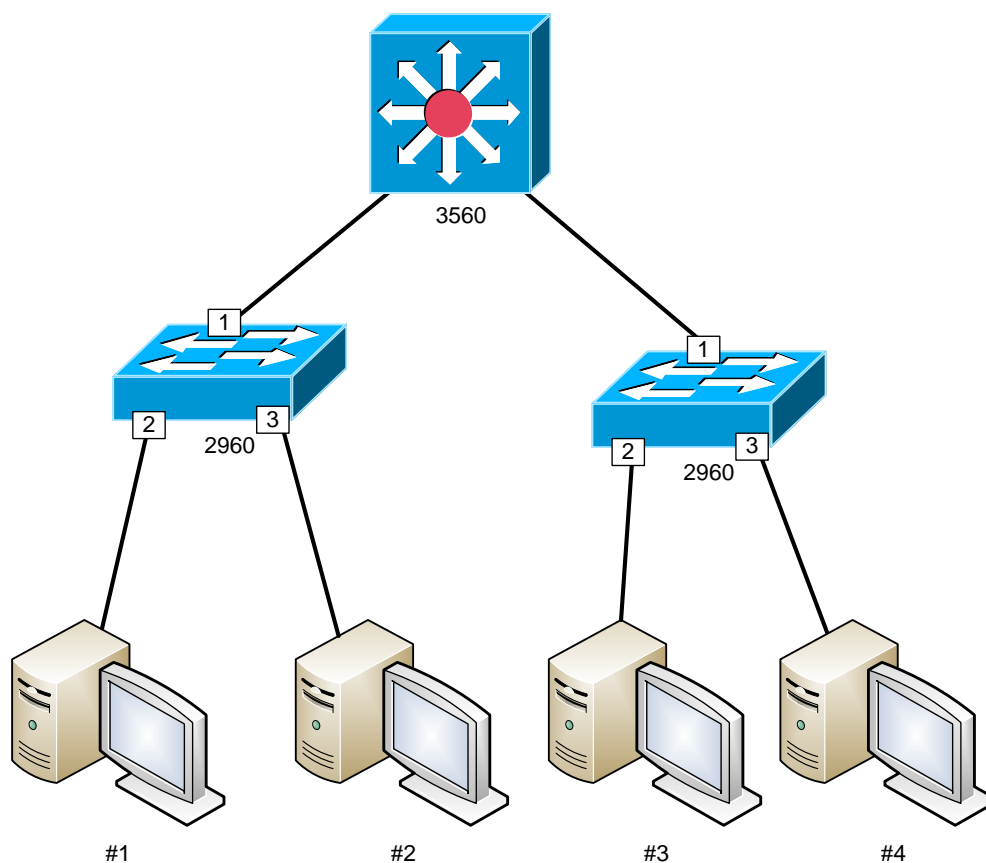


Рисунок 5.

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 соответствии 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.

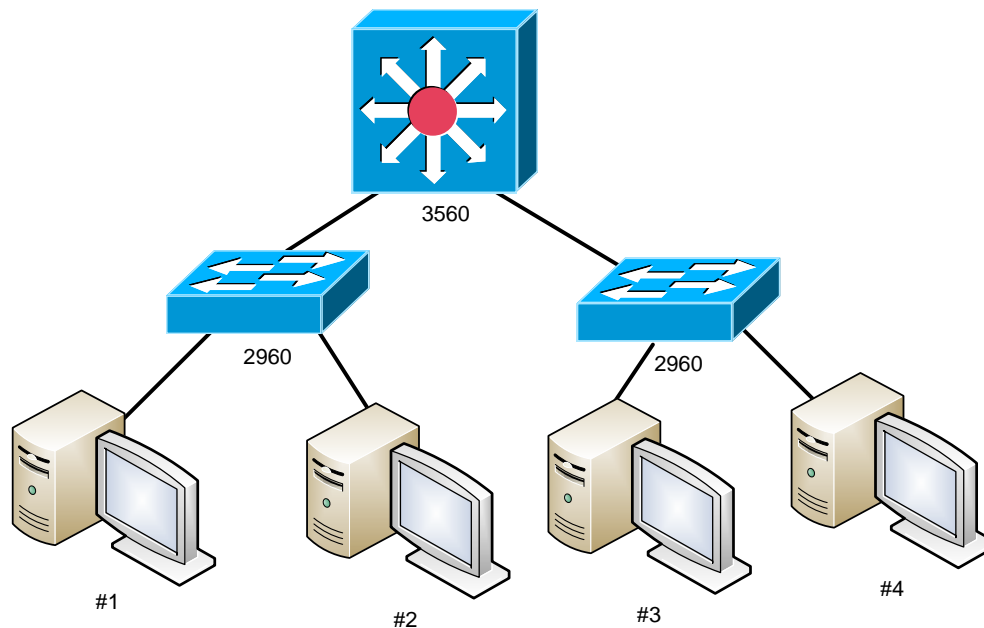


Рисунок 6. Коммутируемая топология для настройки виртуальных сетей VLAN.

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.

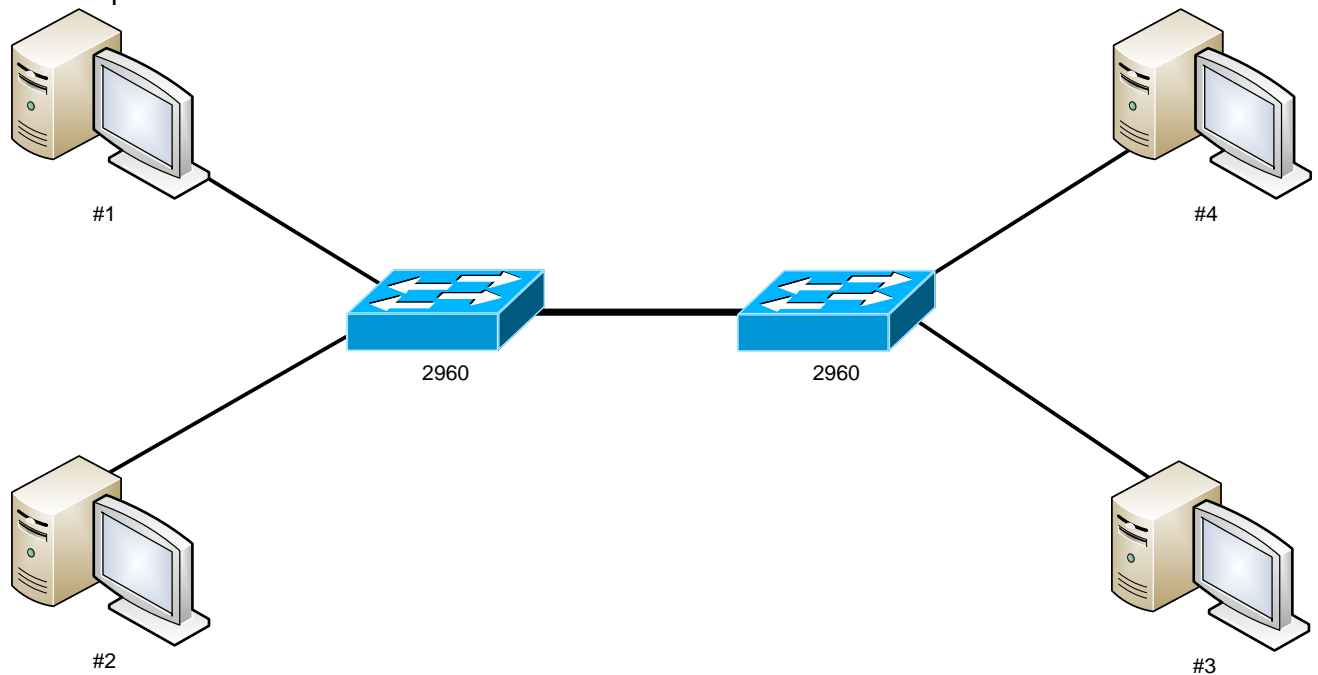


Рисунок 7. Топология коммутируемой сети.

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.

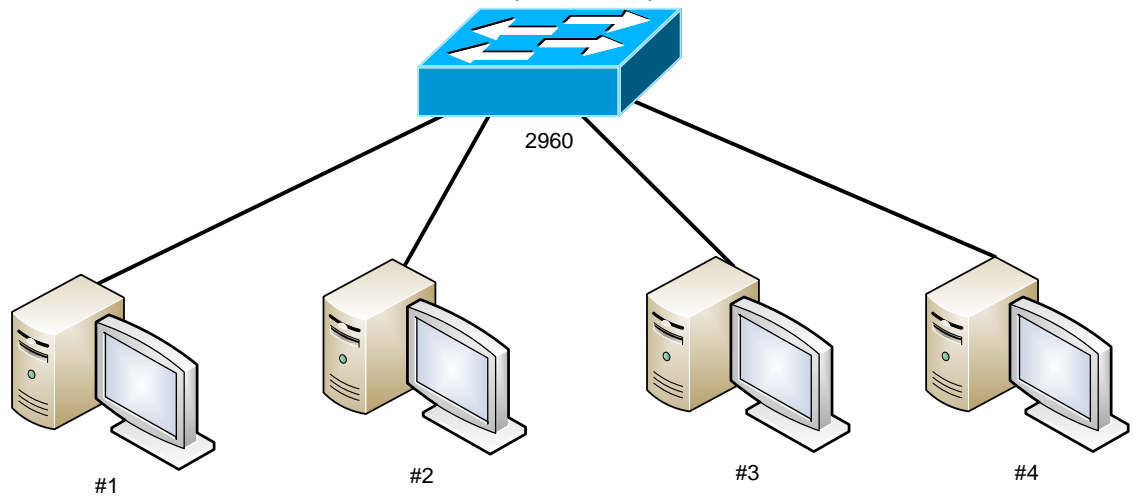


Рисунок 8.

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 медиапоток.
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 медиапоток от сервера 3, а машину 4 – от сервера 1.

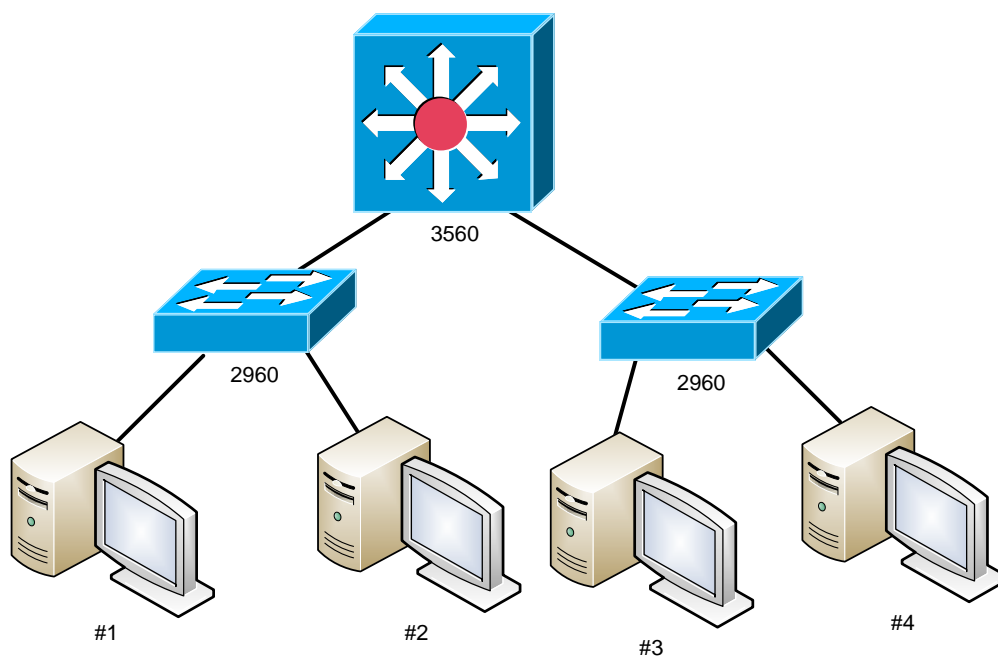


Рисунок 9.

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.

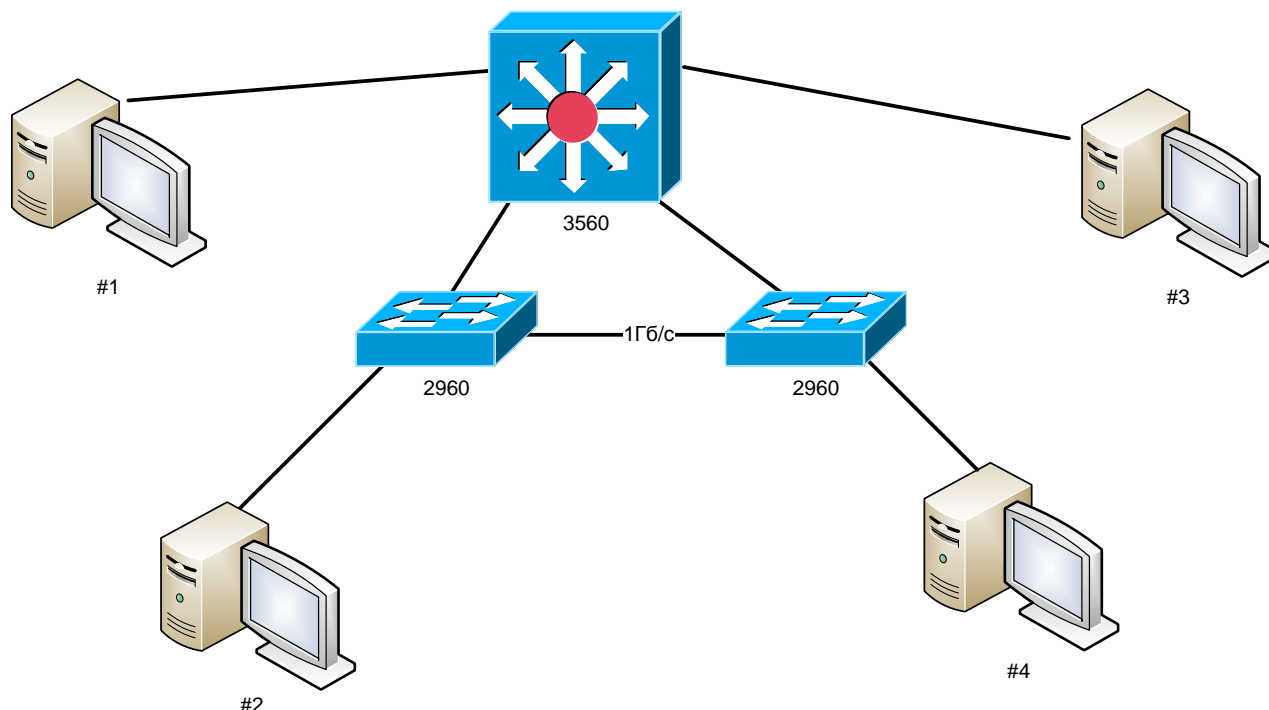


Рисунок 10. Топология коммутируемой сети.

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.

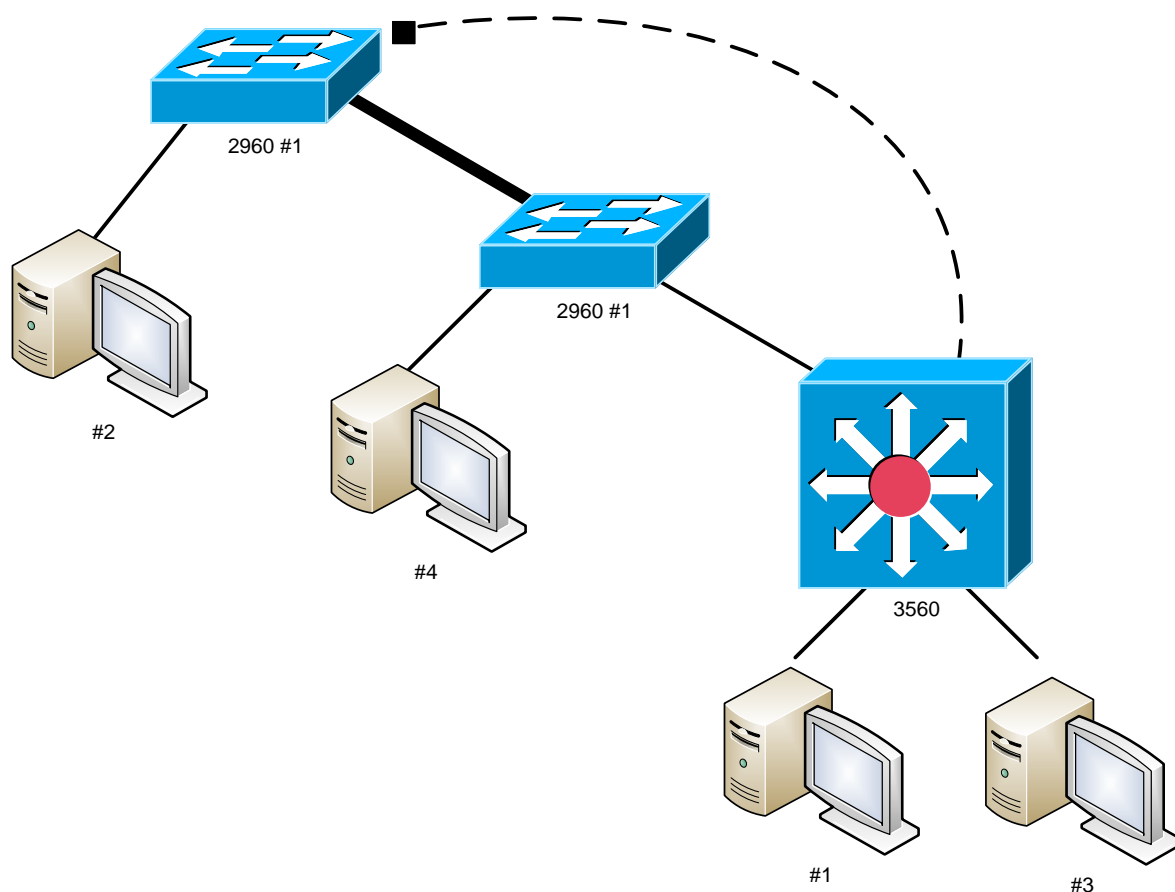


Рисунок 11. Топология сети после применения алгоритма STA.

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.

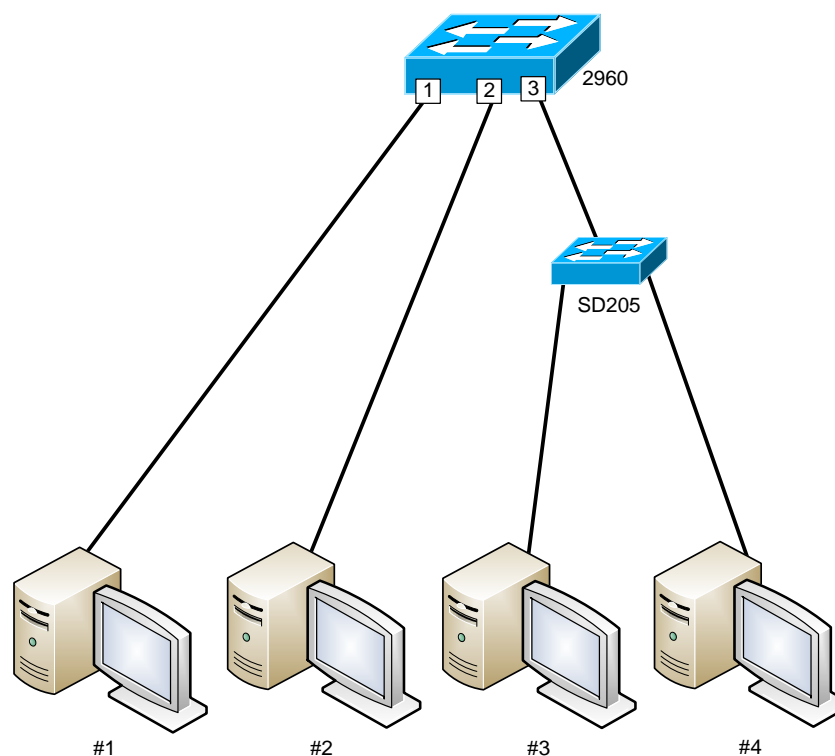


Рисунок 12.

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.
13. Сбросьте настройки коммутатора в фабричные и перезагрузите его.

Лабораторная работа № 9.**Технология QoS.**Цель работы:

Получить опыт работы с протоколами, определяющими QoS.

Порядок выполнения работы:

1. Соберите топологию, представленную на рисунке 13.

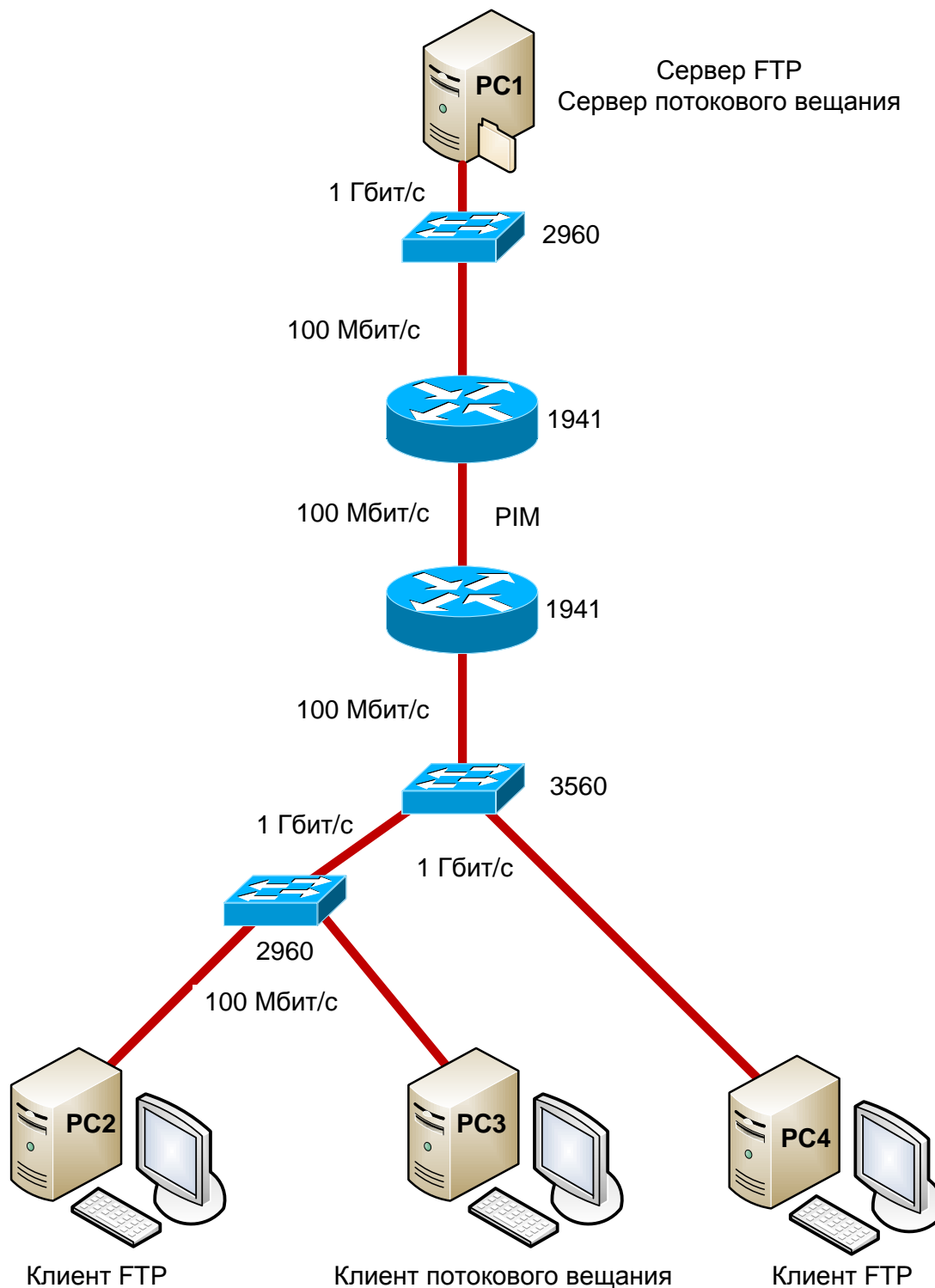


Рисунок 13.

2. Создайте 2 сети, настройте маршрутизацию между ними.
3. На PC1 запустите сервер FTP и сервер потокового вещания.

4. На коммутаторах настройте функцию IGMP Snooping, а на маршрутизаторах настройте протокол PIM.
5. Настройте PC3 в качестве клиента потокового вещания, обеспечьте передачу группового трафика между сетями.
6. Убедитесь, что видеопоток успешно принимается PC3. Наблюдайте за появлением разрывов в передаче видеопотока.
7. На PC2 и PC4 запустите одновременное скачивание файлов с PC1. Опишите процессы, происходящие с видеопотоком.
8. Остановите ftp-клиенты на PC2 и PC4 и приём видеопотока на PC4. Настройте функцию классификации трафика (CoS) на коммутаторах (алгоритм DiffServ). Классифицируйте мультимедийный трафик как более приоритетный, чем трафик FTP.
9. Запустите приём видеопотока. Убедитесь, что поток принимается без задержек.
10. На PC2 и PC4 запустите одновременное скачивание файлов с PC1. Посмотрите, появляются ли разрывы, если появляются, то сравните частоту их появления с вариантом без включения QoS, попробуйте перенастроить коммутаторы, чтобы минимизировать или устранить эти разрывы
11. На PC2 и PC3 с помощью tcpdump/Wireshark изучите входящие пакеты, обращайте внимание на поле CoS, опишите механизм обеспечения QoS по алгоритму DiffServ.

4. Безопасность

Лабораторная работа № 10.

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.

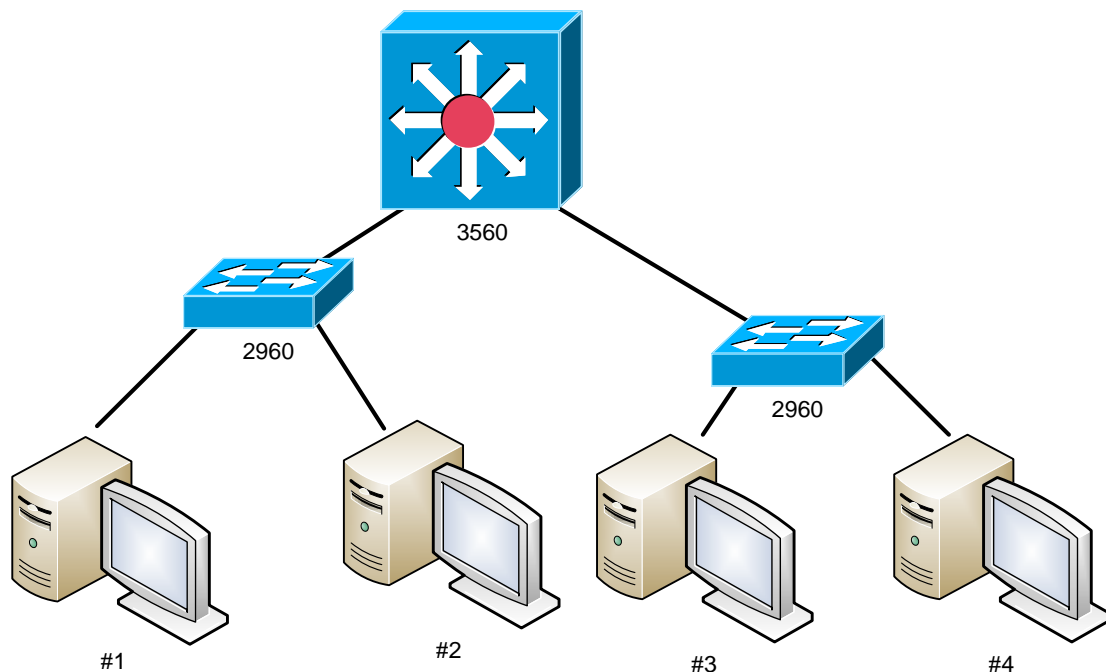


Рисунок 14.

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. Попробуйте 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 № 11.**Безопасность на основе сегментации трафика.**Цель работы:

Изучение механизма сегментации трафика.

Порядок выполнения работы:

1. Соберите топологию сети, представленную на рисунке 15.

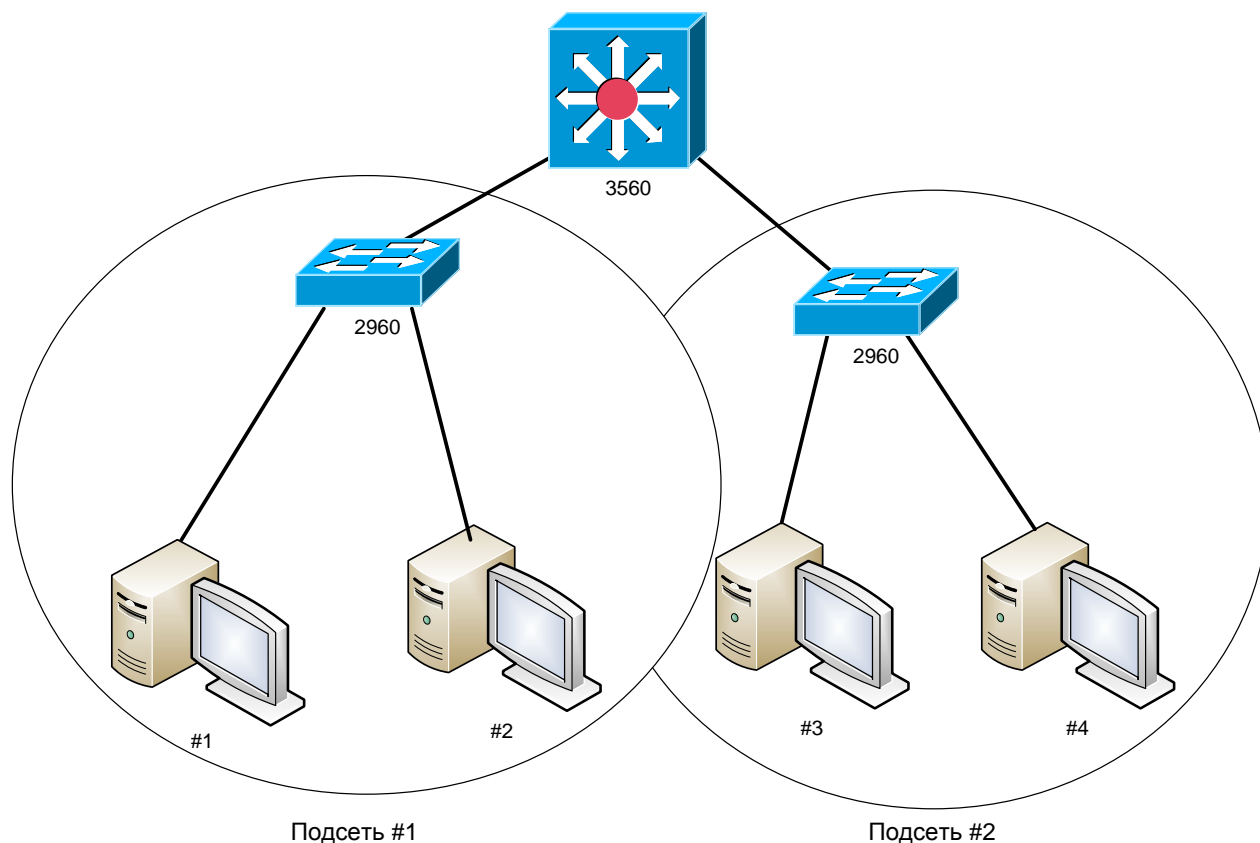


Рисунок 15. Топология коммутируемой сети.

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 заводские и перезагрузите его.

Лабораторная работа № 12.**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.

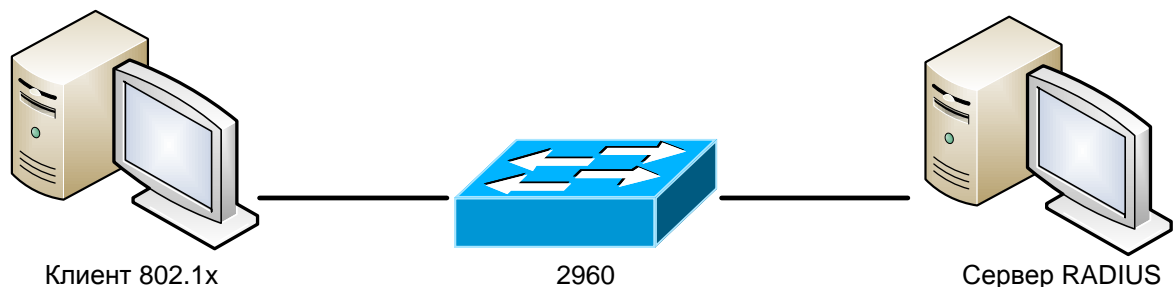


Рисунок 16. Топология коммутируемой сети.

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.

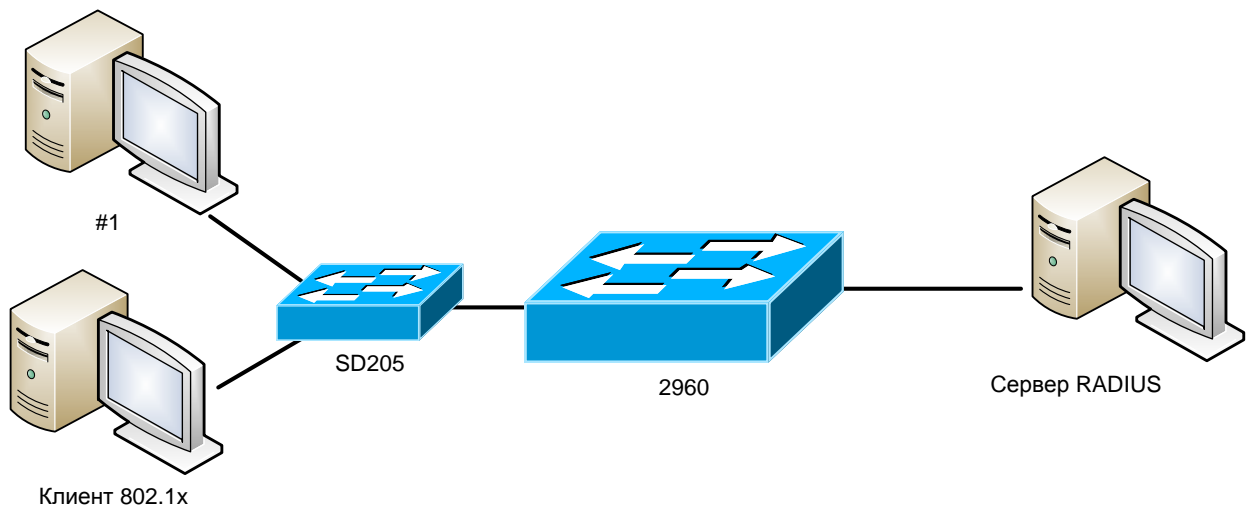


Рисунок 17. Топология коммутируемой сети.

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.

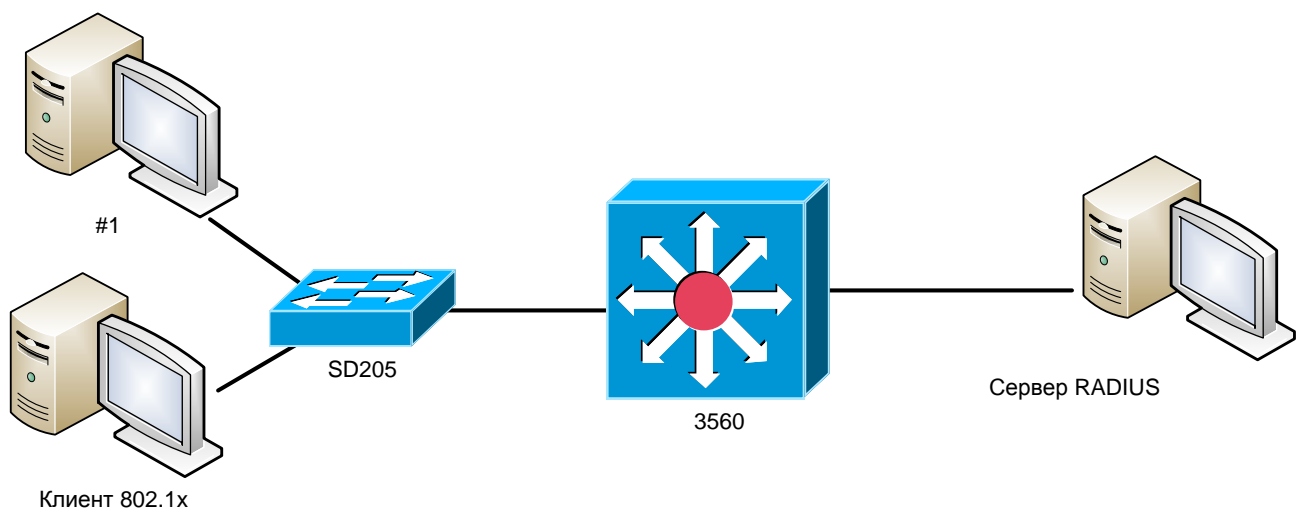


Рисунок 18. Топология коммутируемой сети.

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 иницируйте 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 № 13. Списки контроля доступа ACL.

Цель работы:

Изучение технологии Access Control Lists.

Порядок выполнения работы:

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

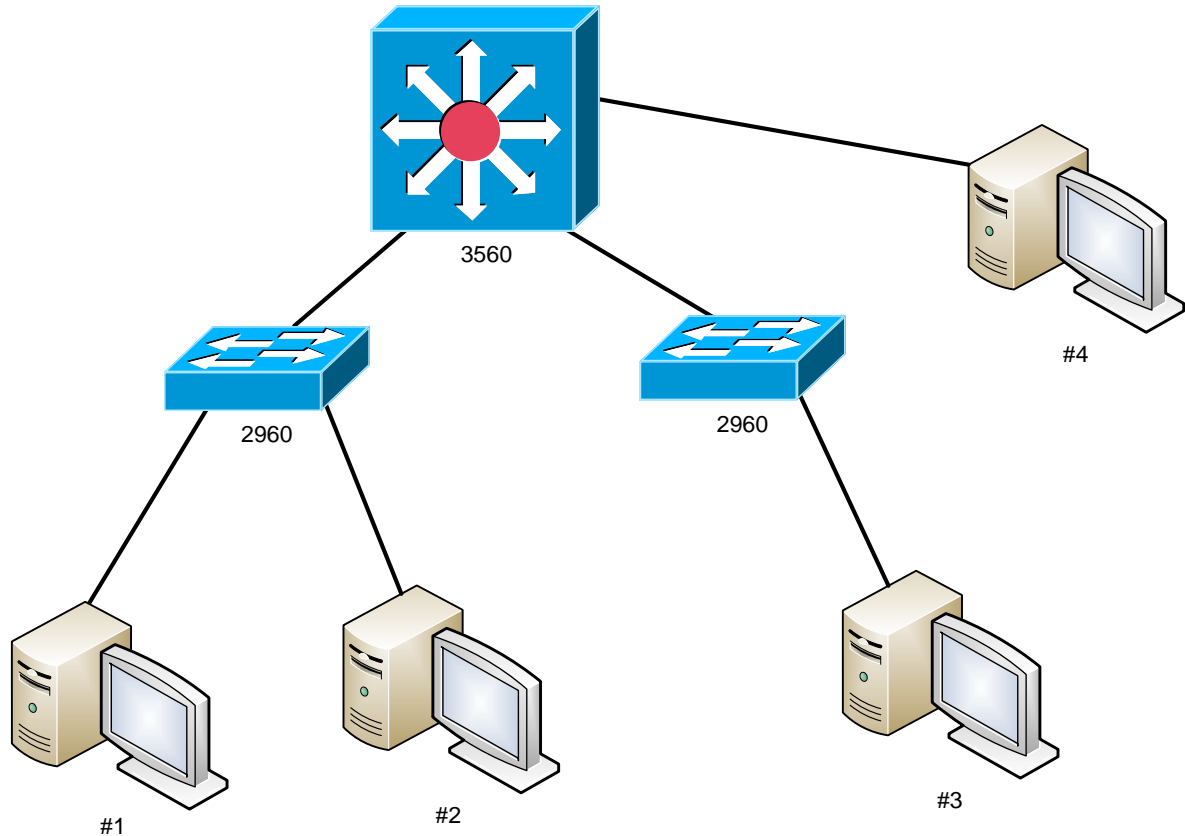


Рисунок 19. Топология коммутируемой сети.

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 «зеркалировался» на порт машины #4.
4. Проверьте созданные настройки.

Лабораторная работа № 15. Технология Network Address Translation.

Цель работы:

Изучение технологии NAT и способов её настройки в ОС Linux.

Порядок выполнения работы:

1. Соберите топологию сети, представленную на рисунке 22.

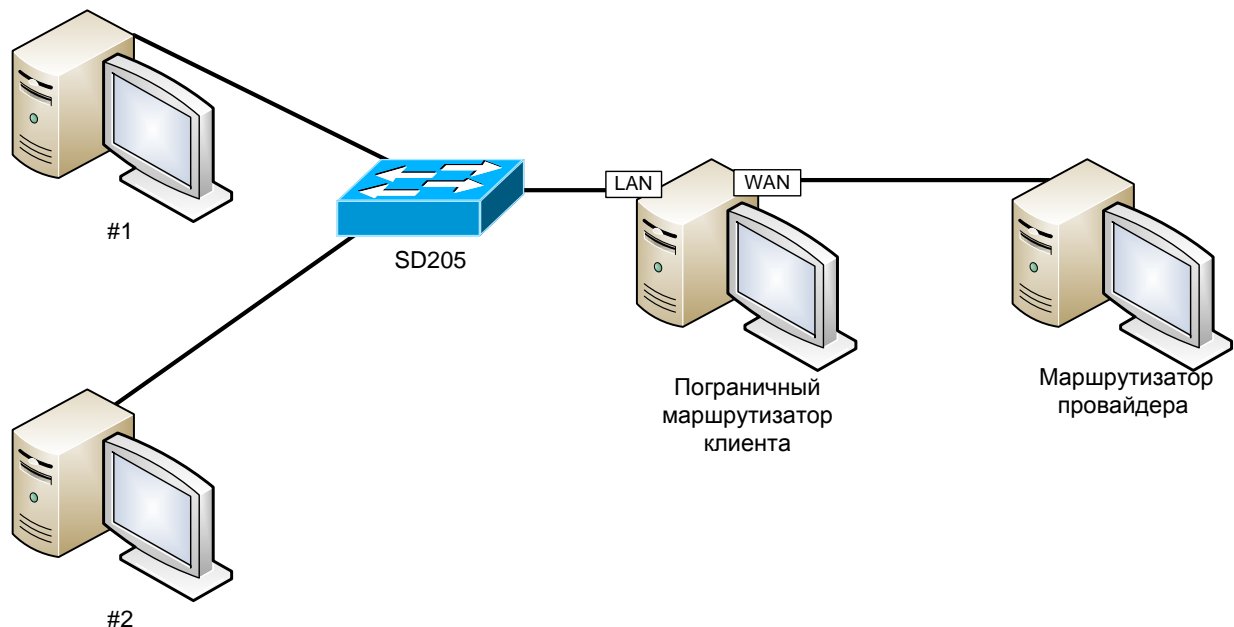


Рисунок 22.

2. Настройте компьютеры таким образом, чтобы рабочие станции #1, #2 и LAN-интерфейс маршрутизатор клиента принадлежали одной IP-подсети, а WAN-интерфейс маршрутизатор клиента и маршрутизатор провайдера – другой.
3. Настройте и запустите на маршрутизаторе провайдера веб-сервер.
4. Изучите главу 4.2.4 «Транслятор адресов» теоретического пособия.
5. Настройте NAT на пограничном маршрутизаторе клиента с использованием утилиты iptables.
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.

5. Технологии коммутации третьего уровня

Лабораторная работа № 16.

Основы коммутации третьего уровня.

Цель работы:

Изучение принципов работы коммутатора уровня 3.

Порядок выполнения работы:

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

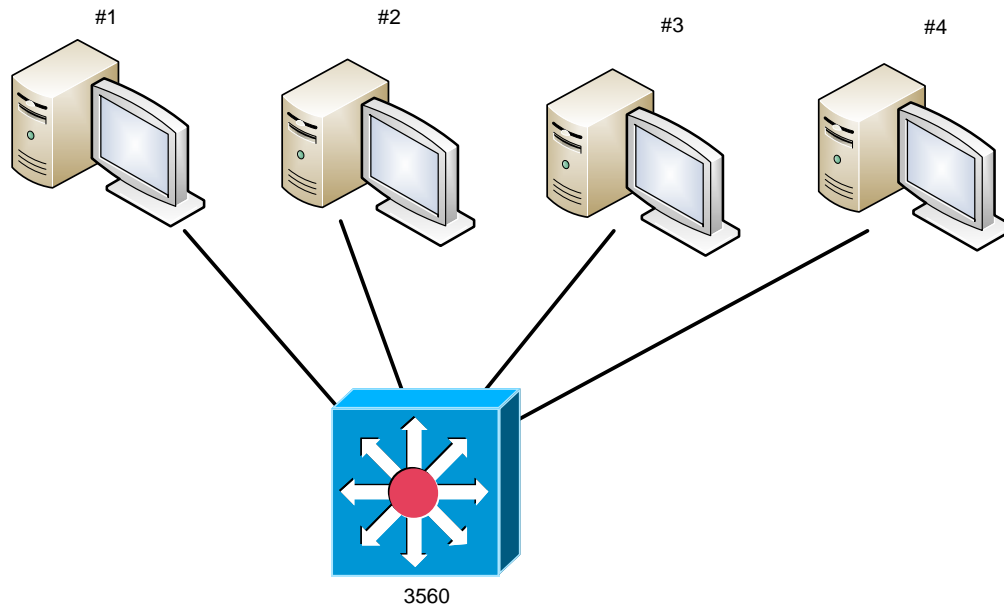


Рисунок 23. Топология коммутируемой сети.

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

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

3. Включите виртуальные сети в IP-подсети в соответствии 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.

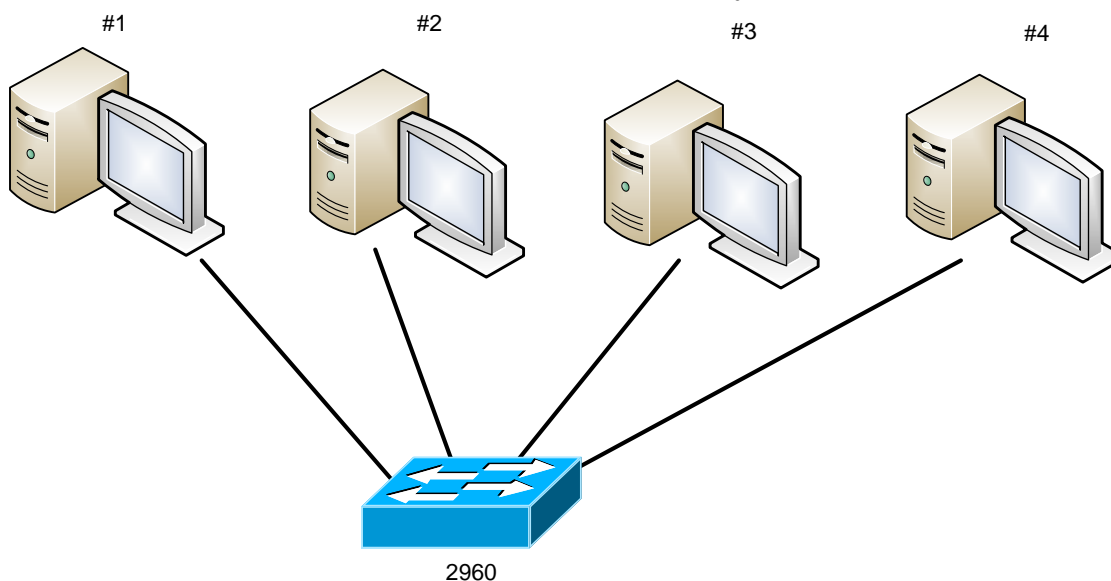


Рисунок 24. Топология коммутируемой сети.

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.

6. Маршрутизация в глобальных сетях

Лабораторная работа № 17.

Статическая маршрутизация.

Цель работы:

Получение навыков настройки программного маршрутизатора и построения статических маршрутов с использованием ОС Linux.

Порядок выполнения работы:

1. Соберите топологию сети, представленную на рисунке 25.

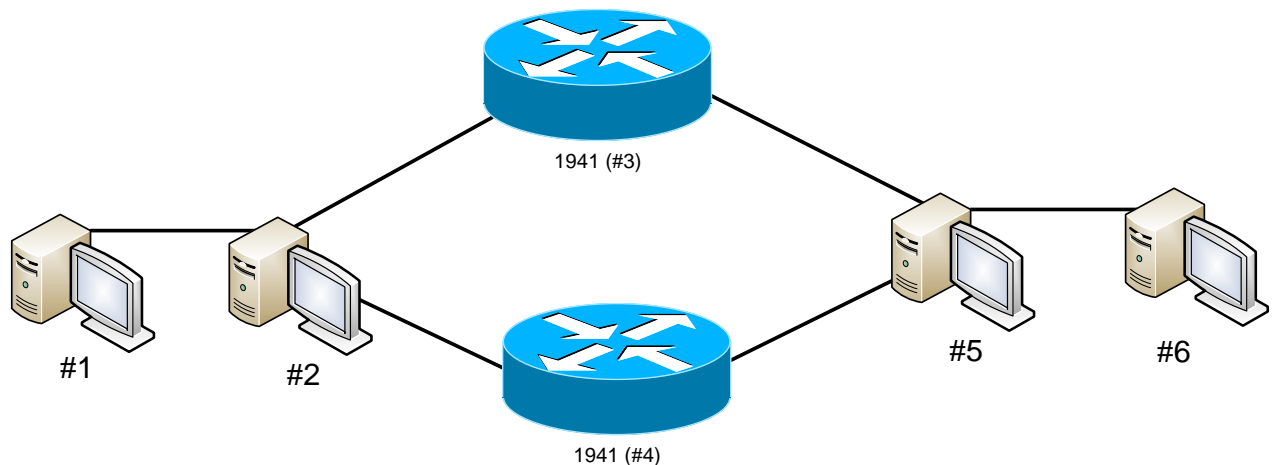


Рисунок 25.

2. Настройте произвольные IP-подсети класса C.
3. Настройте статические маршруты таким образом, чтобы трафик от машины 1 к машине 6 шёл по маршруту «1-2-3-5-6».
4. Разорвите связь между машиной 3 и 5.
5. Ответьте на следующие вопросы:
 - ✓ изменился ли маршрут прохождения трафика от машины 1 к машине 6?
 - ✓ изменились ли таблицы маршрутизации на машинах 2, 3 и 5?
6. Не восстанавливая связь между 3 и 5 машиной, измените таблицы маршрутизации на нужных машинах таким образом, чтобы трафик от машины 1 к машине 6 шёл по маршруту «1-2-4-5-6».
7. Сделайте выводы по поводу достоинств и недостатков статической маршрутизации.

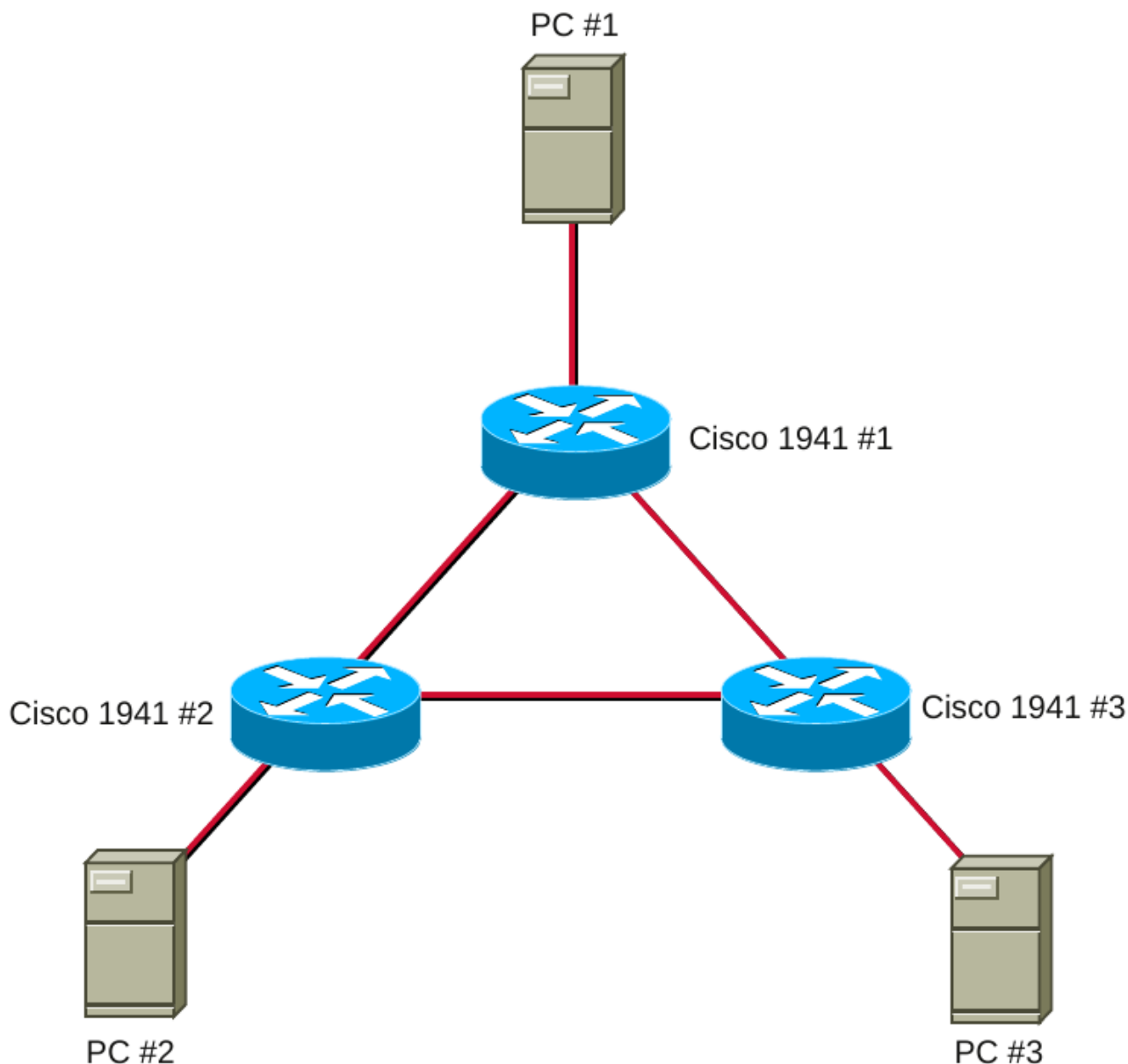
Лабораторная работа № 18.
Протокол маршрутизации EIGRP.

Цель работы:

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

Порядок выполнения работы:

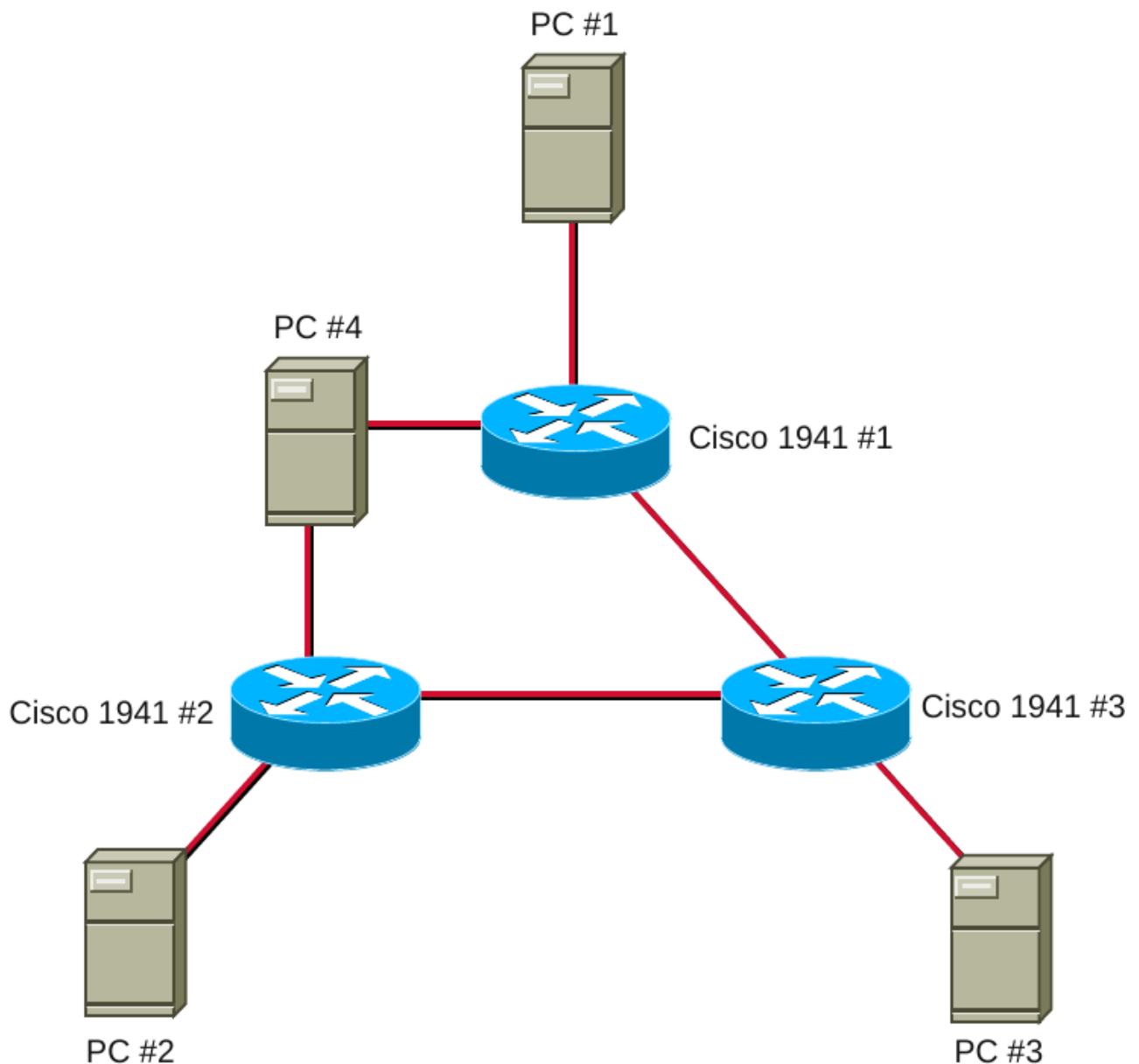
1. Соберите топологию



2. Настройте сетевые интерфейсы на компьютерах и маршрутизаторах
3. Настройте протокол EIGRP на маршрутизаторах
4. Дождитесь окончания процедур протокола и проверьте связность сети
5. Имитируйте разрыв сегмента сетевого кабеля между парой маршрутизаторов
6. Засеките время сходимости протокола
7. Изучите влияние таймеров hold и hello на скорость сходимости

Просмотр сообщений EIGRP

1. Соберите топологию



2. Настройте сетевые интерфейсы на компьютерах и маршрутизаторах
3. С помощью утилиты brctl соберите программный коммутатор из интерфейсов eth0 и eth1 на PC #4 следующим образом:

```
# brctl addbr br0  
# brctl addif br0 eth0  
# brctl addif br0 eth1
```
4. Настройте протокол EIGRP на маршрутизаторах
5. Дождитесь окончания процедур протокола и проверьте связность сети
6. Запустите прослушивание трафика на интерфейсе br0 программного коммутатора PC #4 с помощью tcpdump, изучите передающиеся между маршрутизаторами сообщения в нормальном режиме работы
7. Имитируйте разрыв сегмента сети между маршрутизаторами #2 и #3

8. Изучите передающиеся между маршрутизаторами сообщения при обнаружении неполадки в сети.

Сравнение скорости EIGRP и OSPF

1. Соберите топологию из первой части лабораторной работы
2. Настройте маршрутизаторы, протокол EIGRP на них и компьютеры
3. Дождитесь выполнения процедур протокола и проверьте связность сети
4. Имитируйте разрыв, измерьте время сходимости протокола EIGRP
5. Восстановите топологию
6. Отключите протокол EIGRP и настройте протокол OSPF на маршрутизаторах
7. Дождитесь выполнения процедур протокола и проверьте связность сети
8. Имитируйте разрыв, измерьте время сходимости протокола OSPF
9. Сделайте вывод о сходствах и различиях в процедурах настройки протоколов и о времени их сходимости

Лабораторная работа № 19. 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 27 (возможно использование коммутаторов).

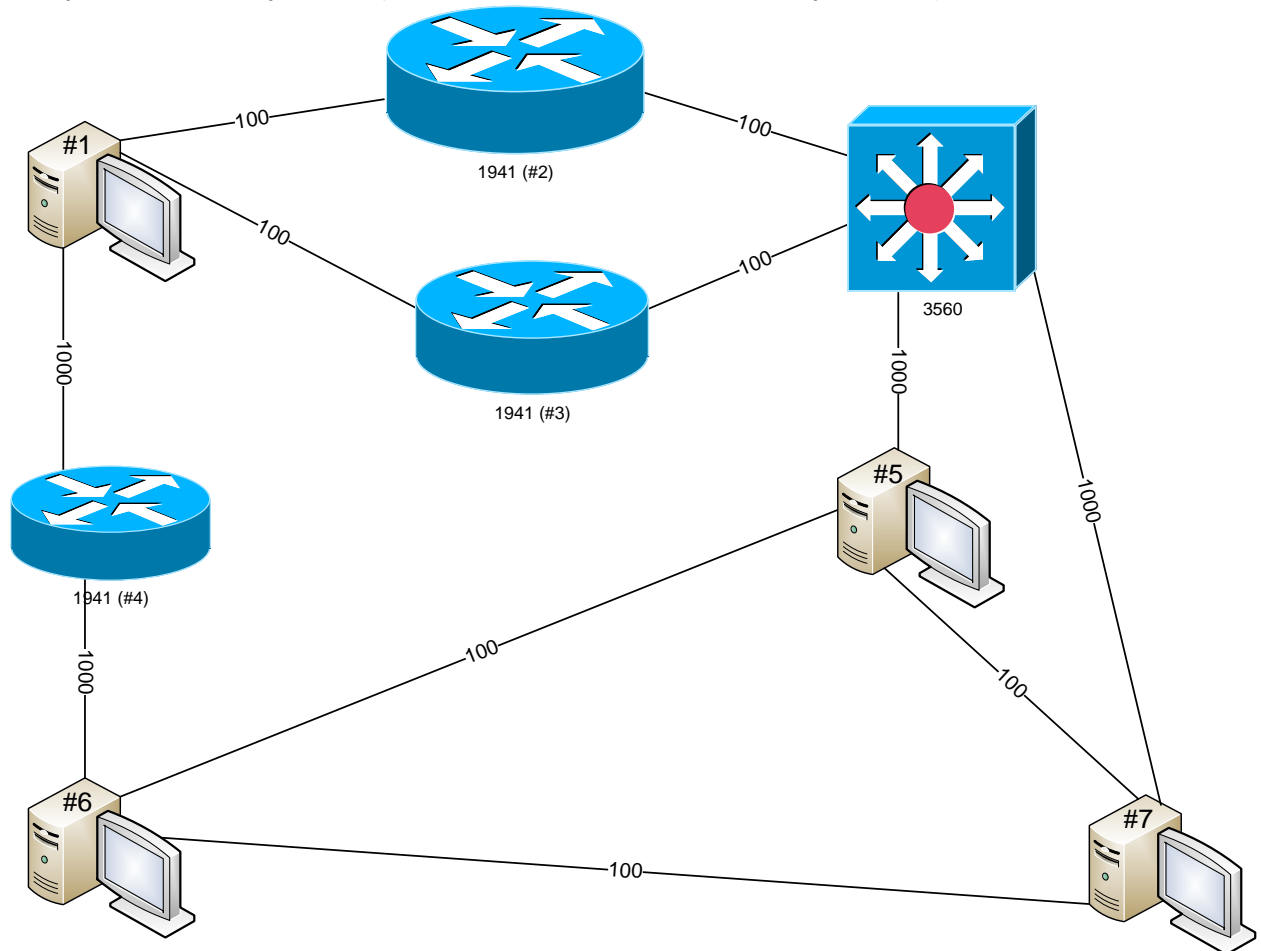


Рисунок 27. Топология коммутируемой сети.

2. Придумайте номера подсетей. На каждом из маршрутизаторов назначьте на сетевые интерфейсы IP-адреса в соответствии с подсетью, которой он принадлежит.
3. Изучите раздел 3.6 «Протокол маршрутизации OSPF» теоретического пособия.
4. Настройте протокол OSPF: на коммутаторе и маршрутизаторах – штатными средствами управления, на компьютерах – с использованием сервиса *quagga* (не забудьте включить функцию маршрутизации).
5. Проверьте работоспособность сети.
6. Рассчитайте стоимость для каждого интерфейса.
7. Осуществите взаимодействие между маршрутизаторами 1 и 7 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.

Лабораторная работа № 20. Протокол маршрутизации BGP.

Цель работы:

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

Порядок выполнения работы:

1. Соберите топологию сети, как указано на рисунке 28 (возможно использование коммутаторов).

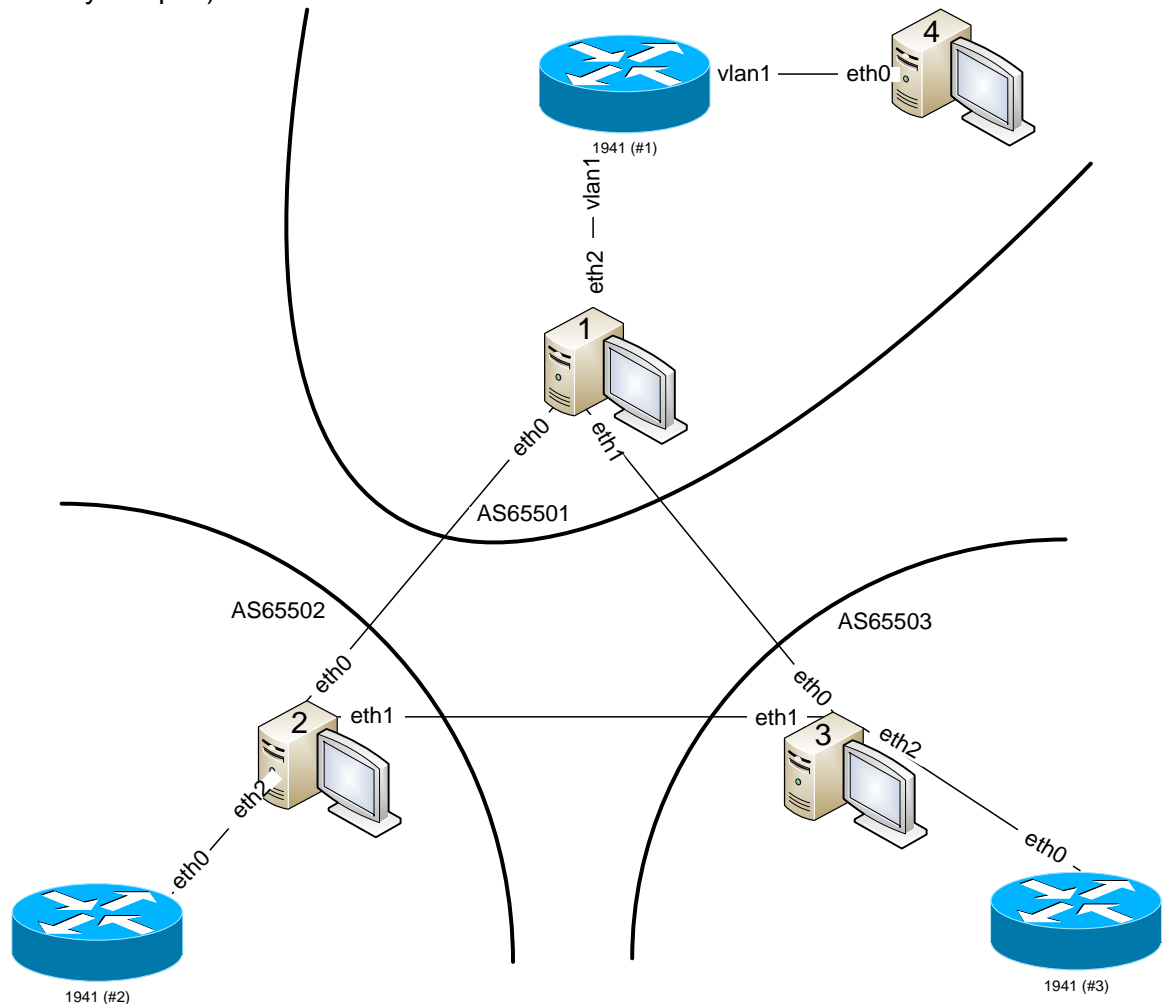


Рисунок 28. Топология коммутируемой сети.

2. Изучите раздел 3.7 «Протокол маршрутизации BGP» теоретического пособия.
3. Назначьте IP-адреса интерфейсам.
4. Настройте на каждом компьютере демон, реализующий протокол BGP (с использованием сервиса quagga). Номера автономных систем задайте в соответствии с рисунком 28.
5. Убедитесь в правильности настроек, просмотрев таблицы маршрутизации и таблицы состояния Quagga BGP.
6. Выполните трассировку маршрутов между всеми возможными парами устройств, запишите или запомните эти маршруты.
7. С помощью метрик сделайте маршрут между PC1 и PC2 более дорогим, чем между PC1 и PC3. Дождитесь схождения протокола и посмотрите, как изменились маршруты и изменились ли они вообще. Объясните изменение или отсутствие изменения маршрутов.
8. Настройками протокола добейтесь, чтобы маршрут от PC4 к RR3 пролегал через PC2.
9. Убедитесь, что маршрут между RR1 и RR3 кратчайший. Разорвите связь между PC1 и PC3. Измерьте время сходимости протокола.

7. Технологии Транспортного и Прикладного уровней

Лабораторная работа № 21.

Протоколы TCP и UDP.

Цель работы:

Изучение протоколов транспортного уровня стека TCP/IP.

Порядок выполнения работы:

1. Изучите разделы 3.8 «Протокол UDP» и 3.9 «Протокол TCP» теоретического пособия.
2. Осуществите взаимодействие двух машин с использованием протокола TCP. Например, на одной машине настройте веб-сервер и обратитесь к нему через веб-браузер на второй машине.
3. Используя утилиту `tcpdump` необходимо:
 - ✓ выделить фазы протокола TCP (установление соединения, обмен данными, разрыв соединения);
 - ✓ на примере одного пакета разобрать формат заголовка TCP-пакета.
4. Осуществите взаимодействие двух машин с использованием протокола UDP. Например, на одной машине запустите сервер VLC (видео-сервер), а на другой машине – приёмник (VLC плеер) /потокковые данные передаются с использованием протокола UDP/.
5. Используя утилиту `tcpdump` необходимо на примере одного пакета разобрать формат заголовка UDP-пакета.

Лабораторная работа № 22.**Динамическая конфигурация узла с использованием протокола DHCP.**Цель работы:

Изучение протокола DHCP и получение навыков настройки DHCP-сервера на базе ОС Linux.

Порядок выполнения работы:

1. Соберите топологию сети, представленную на рисунке 29.

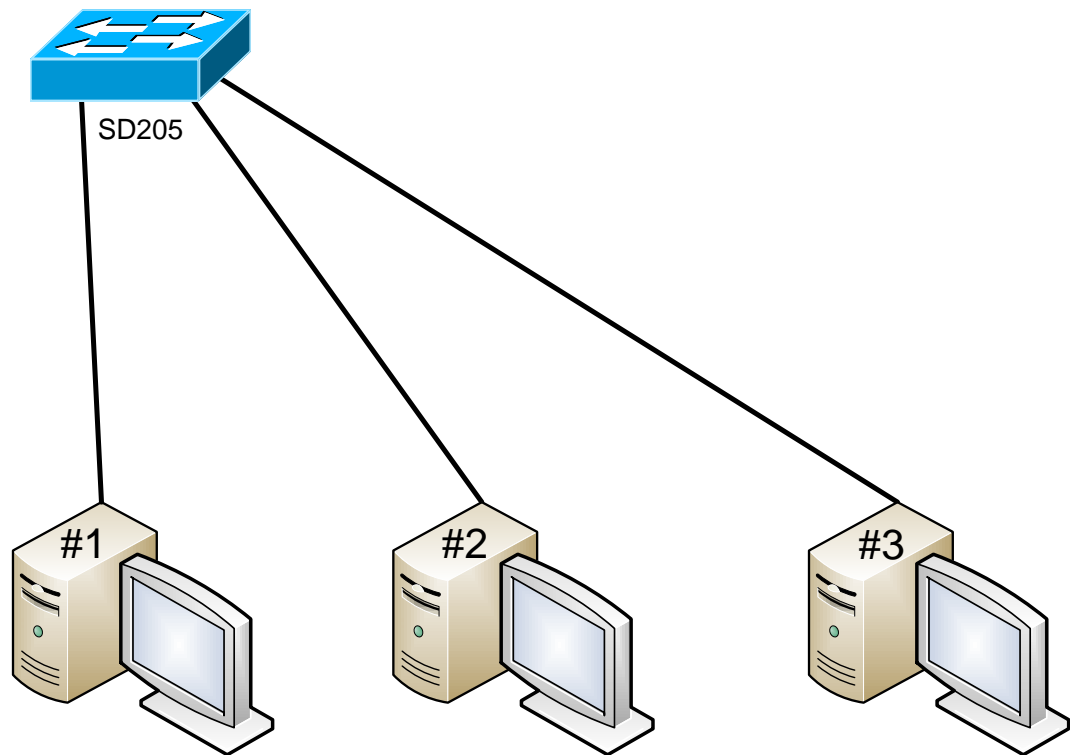


Рисунок 29.

2. Настройте машины 2 и 3 на динамическое получение сетевых настроек.
3. На сетевом интерфейсе машины 1 настройте две IP-подсети. То есть включите машину 1 в две IP-подсети 192.168.1.0/24 и 192.168.2.0/24.
4. Настройте DHCP-сервер на машине 1 таким образом, чтобы:
 - ✓ машина 2 получала произвольный IP-адрес (и соответствующие настройки) из подсети 192.168.1.0/24 через каждые 2 минуты;
 - ✓ машина 3 получала каждый раз постоянный IP-адрес (то есть настройте статическое распределение адреса).
5. Проверьте правильность сделанных настроек.
6. Ответьте на вопрос: какой IP-адрес назначается машине до получения сетевых настроек от DHCP-сервера.

Лабораторная работа № 23.**Настройка протокола DNS.**Цель работы:

Изучение системы DNS и получение навыков её настройки на базе ОС Linux.

Порядок выполнения работы:

1. Соберите топологию сети, представленную на рисунке 30.

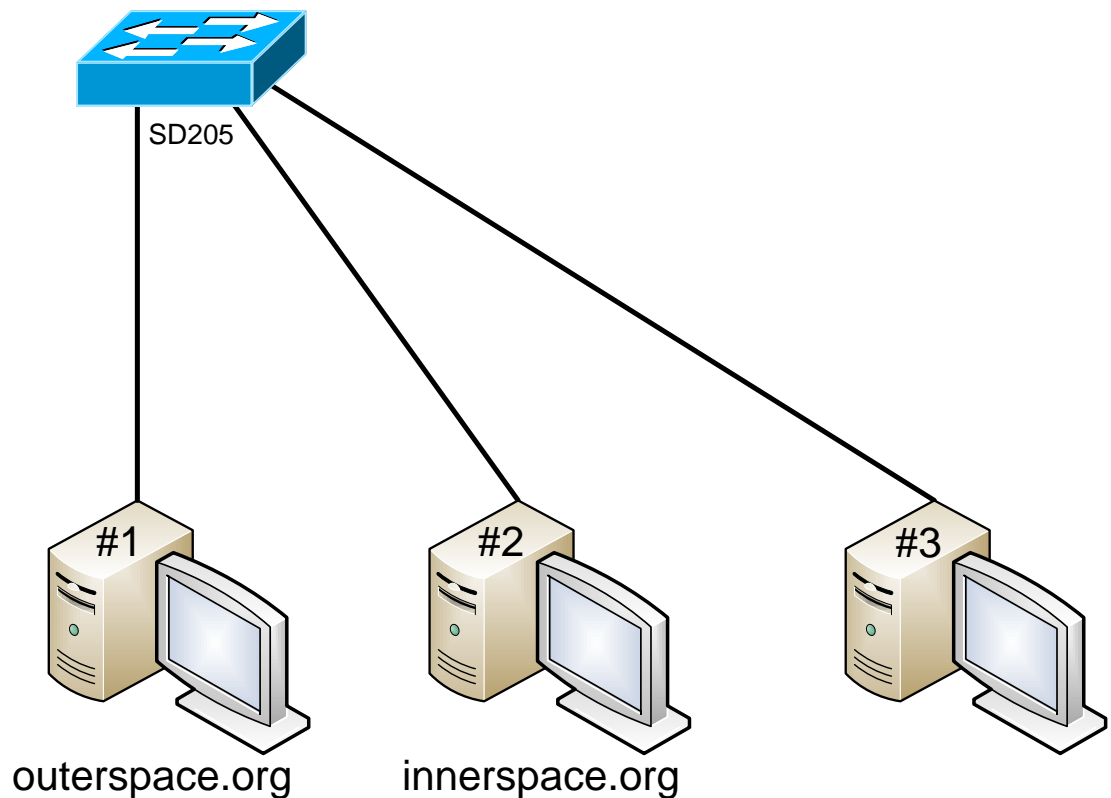


Рисунок 30.

2. Настройте на машине 1 DNS-сервер для поддержки зоны «outerspace.org».
3. Настройте на машине 2 DNS-сервер для поддержки зоны «innerspace.org». В качестве вышестоящего DNS-сервера укажите машину 1.
4. Создайте в каждой из зон несколько произвольных записей (например, www.innerspace.org).
5. Задаёте на машине 3 в качестве DNS-сервера машину 2.
6. Используя на машине 3 утилиту nslookup, разрешите имя «www.innerspace.org».
7. Проанализируйте полученный ответ, время отклика и журнал DNS-сервера на машине 2.
8. Используя на машине 3 утилиту nslookup, разрешите имя «www.outerspace.org».
9. Проанализируйте полученный ответ, время отклика и журналы DNS-серверов на машине 2 и 3.
10. На основе полученной информации ответьте на вопрос: каков маршрут прохождения последнего запроса клиента?

8. Сетевые технологии операционной системы Linux

Лабораторная работа № 24.

Пользователи Linux и система PAM.

Цель работы:

Изучение системы пользователей операционной системы Linux и получение навыков работы с ней.

Порядок выполнения работы:

1. Добавьте нового пользователя в систему с помощью команды `useradd`.
2. Добавьте нового пользователя в систему, непосредственно редактируя файл `/etc/passwd`.
3. Измените данные пользователя с помощью команд `usermod`, `chfn` или `chsh`. Посмотрите на изменения, произошедшие в файле `/etc/passwd`.
4. Создайте новую группу с помощью команды `groupadd`.
5. Создайте новую группу, непосредственно редактируя файл `/etc/group`.
6. Добавьте пользователя в новую группу несколькими способами.
7. Создайте каталог, смените группу-владельца и выставьте ему групповое право на запись. Зайдите от имени нового пользователя (либо воспользуйтесь `su`) и попробуйте создать файл в этом каталоге.
8. Удалите пользователя с помощью команды `userdel`.
9. Изучите документацию по `pam_nologin` (man `pam_nologin`) и запретите вход в систему не суперпользователям.
10. Изучите документацию по `pam_cracklib` (man `pam_cracklib`) и добавьте для файла `passwd` политику PAM, проверяющую мощность пароля. Создайте пользователя и поэкспериментируйте со слабыми паролями и параметрами `pam_cracklib`.

Лабораторная работа № 25. Настройка межсетевого экрана в Linux.

Цель работы:

Изучение утилиты iptables и получение навыков работы с ней.

Порядок выполнения работы:

1. Соберите топологию сети, представленную на рисунке 31.

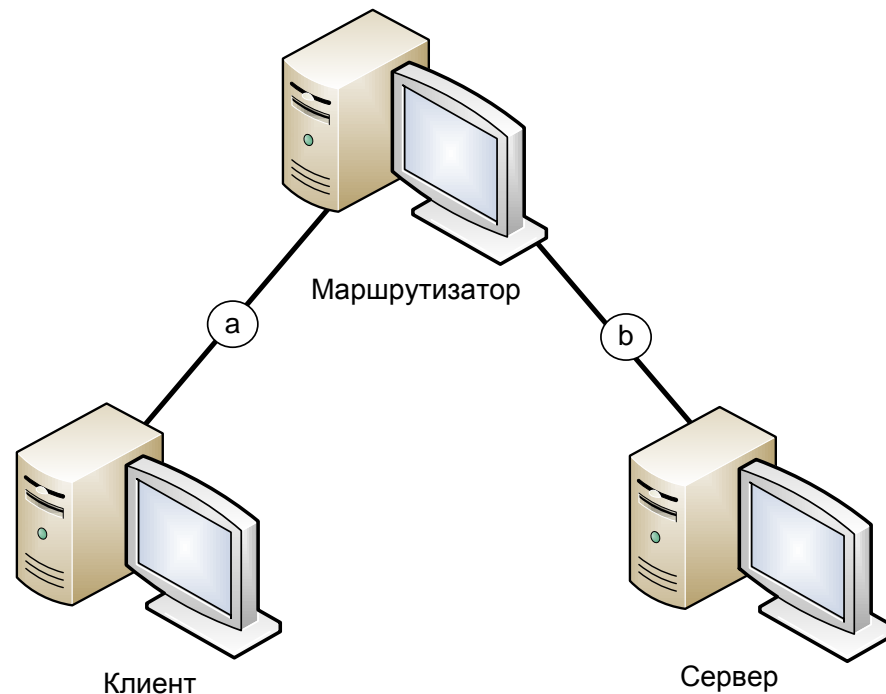


Рисунок 31.

2. Настройте рабочие станции таким образом, чтобы создать две различных IP-подсети: a и b (в соответствии с рисунком 31).
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 № 26.

Работа с файловым сервером в Linux.

Цель работы:

Изучение утилиты iptables и получение навыков работы с ней.

Порядок выполнения работы:

1. Запустите сервер ProFTP на 30 tcp-порту.
2. Ограничьте количество подключений к серверу равным 3.
3. Ограничьте файловое пространство пользователя его домашней папкой.
4. Проверьте выполненные настройки.

Лабораторная работа № 27.**Настройка сервера Samba.**Цель работы:

Изучение сервера Samba и получение навыков работы с ним.

Порядок выполнения работы:

1. Настройте публичный файловый сервер. Добавьте два общих каталога.
2. Измените права доступа к реальному каталогу в файловой системе и попробуйте получить доступ к ресурсу, соответствующему этому каталогу.
3. Добавьте несколько пользователей в базу Samba.
4. Распределите права на запись и чтение по созданным ресурсам. Проверьте работоспособность.
5. Изучите с помощью tcpdump протокол SMB.

Лабораторная работа № 28.**Работа с сетевой файловой системой NFS.**Цель работы:

Изучение файловой системы NFS и получение навыков работы с ним.

Порядок выполнения работы:

1. Настройте на сервер NFS на одной из машин. Экспортируйте каталоги /etc и какой-нибудь каталог, содержащий большой файл объёма, равного или примерно равного суммарному объёму содержимого /etc (объём можно вычислить командой `du -hs`, запущенной в /etc, создать файл произвольного размера командой `dd if=/dev/zero of=myfile bs=1M count=<размер в МБ>`, либо воспользоваться архиватором `tar`, запаковав каталог /etc в один файл).
2. Подключите оба каталога на один клиент.
3. Определите скорость копирования множества мелких файлов.
4. Определите скорость копирования одного большого файла аналогичного размера (скорость копирования можно определить командой `time cp -pR /mnt/nfs/etc /home/etc`. Для одиночного файла можно применить команду `time cp bigfile /dev/null`, чтобы исключить влияние дисковой подсистемы, либо можно использовать команды `find` и `cat` с перенаправлением в /dev/null).
5. Меняя параметры экспортирования (`no_subtree_check/subtree_check`, `async/sync`, `no_wdelay/wdelay`) и параметры монтирования (`rsize`, `wsize`, `noacl/acl`, `proto`), определите влияние этих параметров на скорость процесса чтения.
6. Экспортируйте ещё один каталог с сервера.
7. Подключите его на один клиент.
8. Проведите исследование скорости записи в зависимости от размера и количества файлов (множество больших и один маленький), параметров монтирования и параметров экспортирования.
9. Выполните действия 4-9 для 3 клиентов одновременно.
10. Для сравнения скорости работы протокола NFS запустите FTP-сервер и выполните чтение и запись множества маленьких файлов и одного крупного с помощью `rmvfyfs` и `wget`.
11. Сделайте вывод об оптимальном сочетании параметров и о влиянии каждого параметра из предложенных на процесс чтения и записи.