Федеральное агентство связи

Федеральное государственное образовательное бюджетное учреждение высшего профессионального образования

ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ

ЭЛЕКТРОННАЯ БИБЛИОТЕЧНАЯ СИСТЕМА

Самара

ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ

Федеральное государственное образовательное бюджетное учреждение
высшего профессионального образования

Поволжский государственный университет телекоммуникаций и информатики

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ СЕТЕЙ НА МАРШРУТИЗАТОРАХ И КОММУТАТОРАХ

Методические указания к лабораторным работам

для специальностей:
210404 – Многоканальные телекоммуникационные системы
210406 – Сети связи и системы коммутации
210401 – Физика и техника оптической связи
210403 – Защищенные системы связи
090106 – Информационная безопасность телекоммуникационных систем
200600 – Фотоника и оптоинформатика

Составитель: Н.Н. Васин

Самара
ИУНЛ ПГУТИ
2011

УДК 681.3
УДК 004.722
ББК 32.973.202я7

Обеспечение безопасности сетей на маршрутизаторах и коммутаторах: Методические указания по проведению лабораторных работ / Васин Н.Н. – Самара: ФГОБУВПО ПГУТИ, 2011. – 24 с.

Комплекс лабораторных работ посвящен конфигурированию паролей и сетевых фильтров (списков доступа) на маршрутизаторах, а также конфигурированию безопасности портов коммутатора, созданию виртуальных локальных сетей. В методических указаниях приведены схемы сетей, адреса устройств, порядок выполнения лабораторной работы, примеры конфигурирования устройств.

Рецензент:
Росляков А.В. – д.т.н., профессор, зав. кафедрой АЭС ПГУТИ

Федеральное государственное образовательное бюджетное учреждение высшего профессионального образования

Поволжский государственный университет телекоммуникаций и информатики

2011

Лабораторная работа № 1.
Формирование паролей на маршрутизаторе

Схема сети лабораторной работы приведена на рис.1.1, адреса – в табл.1.1.

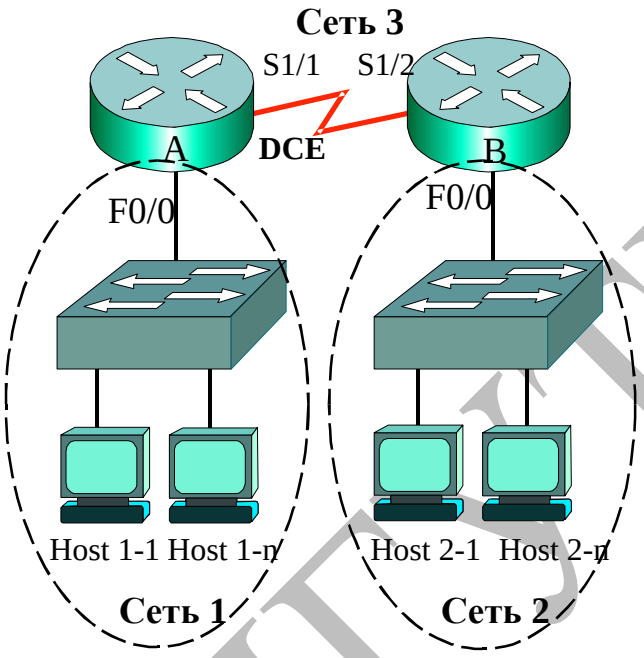

Рис. 1.1. Схема сети

Таблица 1.1

Адреса сетей и интерфейсов маршрутизаторов

	IP-адрес сети	Интерфейсы	IP-адрес интерфейса
Сеть 1	192.168.10.0/24	F0/0	192.168.10.1
Сеть 2	192.168.20.0/24	F0/0	192.168.20.1
Сеть 3	200.30.30.0/24	S1/1	200.30.30.11
		S1/2	200.30.30.12

1. **Сконфигурировать адреса всех интерфейсов маршрутизаторов согласно табл.1.1.**

2. **Сконфигурировать адреса конечных узлов сети**

Host 1-1 – 192.168.10.11, Host 1-n – 192.168.10.18, Host 2-1 – 192.168.20.21, Host 2-n – 192.168.20.29.

3. На маршрутизаторах **A и B сконфигурировать протокол маршрутизации RIP.** По командам **ping, sh run, s hip route** проверить работоспособность сети, при необходимости отладить сеть.

4. Установка пароля на консольный вход

На маршрутизаторе A сконфигурировать имя и пароль консольного порта:

Router(config)#**hostname Router_A**
Router_A(config)#**line console 0**
Router_A(config-line)#**password cis-1**
Router_A(config-line)#**login**

Проверить работоспособность пароля, для чего используя команды **exit** выйти из режима конфигурирования и вновь войти.

Что при этом происходит? Сравнить с маршрутизатором B, где пароль не установлен.

5. Защита входа в привилегированный режим

На маршрутизаторе A сконфигурировать два пароля:

Router_A(config)#**enable password cis-2**
Router_A(config)#**enable secret cis-3**

Проверить работоспособность паролей, для чего используя команду **exit** выйти в пользовательский режим и вновь войти в привилегированный.
Какой пароль позволяет войти в привилегированный режим? Почему?

Посмотреть текущую конфигурацию (sh run). Прокомментировать информацию об установленных паролях. В какой форме представлены пароли?

6. Удаленный доступ

На маршрутизаторе B сконфигурировать имя:

Router(config)#**hostname Router_B**
Router_B(config)#

По команде **telnet** реализовать удаленный доступ в маршрутизатор A:

Router_B#**telnet 192.168.10.1**

Что при этом происходит? Почему?

7. **Защита удаленного доступа**

На маршрутизаторе А сконфигурировать пароль на виртуальные линии:

Router_A(config)#**line vty 0 4**
Router_A(config-line)#**password cis-4**
Router_A(config-line)#**login**

По команде **telnet** реализовать удаленный доступ с маршрутизатора В в маршрутизатор А:

Router_B#**telnet 192.168.10.1**

Что при этом происходит? Почему?

В режиме удаленного доступа **изменить имя маршрутизатора А** на R-A. Завершить удаленный доступ. **Проверить, что имя изменено**.

8. **Реализовать удаленный доступ в маршрутизатор А с конечного узла Host 2-n**.

Внести изменения в конфигурацию маршрутизатора А, использовав команду:

R-A(config)#**service password-encription**

Проверить текущую конфигурацию. Прокомментировать информацию об установленных паролях. В какой форме представлены пароли?

Выйти из режима удаленного доступа.

На маршрутизаторе А отменить команду **service password-encription**. **Прокоментировать текущую конфигурацию**.

9. **Сохранить текущую конфигурацию!!!**

R-A#**copy run start**

10. **Восстановление утерянного пароля**

Если пользователь позабыл пароль, то пароль **enable password** можно восстановить, а пароль **enable secret** можно заменить новым. Это реализуется только при физическом доступе к маршрутизатору через консольный порт

(console). При загрузке маршрутизатора необходимо обойти проверку паролей за счет изменения значения **конфигурационного регистра**.

11. Проверить значение конфигурационного регистра по команде:

R-A#**show version**
…
Configuration register is 0x2102

12. Выключить и вновь включить маршрутизатор

В течение 1 минуты, когда производится проверка (тестирование) аппаратных средств маршрутизатора, нажать клавишу **Break** на клавиатуре. При этом маршрутизатор переходит в режим
rommon 1>

13. Ввести команду

rommon 1>**confreg 0x2142**,

которая позволяет при загрузке конфигурационного файла обойти проверку паролей.

14. Следующая команда

rommon 2>**reset**

запустит процесс перезагрузки, который завершится вопросом:

Continue with configuration dialog? [yes/no]:

на который нужно ответить отрицательно – no**.**

Маршрутизатор готов к переконфигурированию!
Проверить текущую конфигурацию! Прокомментировать ее.

Router>**ena**

Router#**sh run**

15. Для сохранения прежней конфигурации, хранящейся в памяти NVRAM, выполнить команду:

Router#**copy start run**
…
R-A#

16. Проверить текущую конфигурацию!

R-A#**sh run**

17. Внести необходимые изменения в текущую конфигурацию. Изменить пароли, запомнить их!

18. Вернуть прежнее значение конфигурационного регистра

R-A(config)#**config-register 0x2102**

19. Сохранить текущий конфигурационный файл

R-A#**copy run start**

Лабораторная работа № 2

Конфигурирование списков доступа

Необходимо сконфигурировать стандартные списки доступа по защите Сети 1 (рис. 2.1).

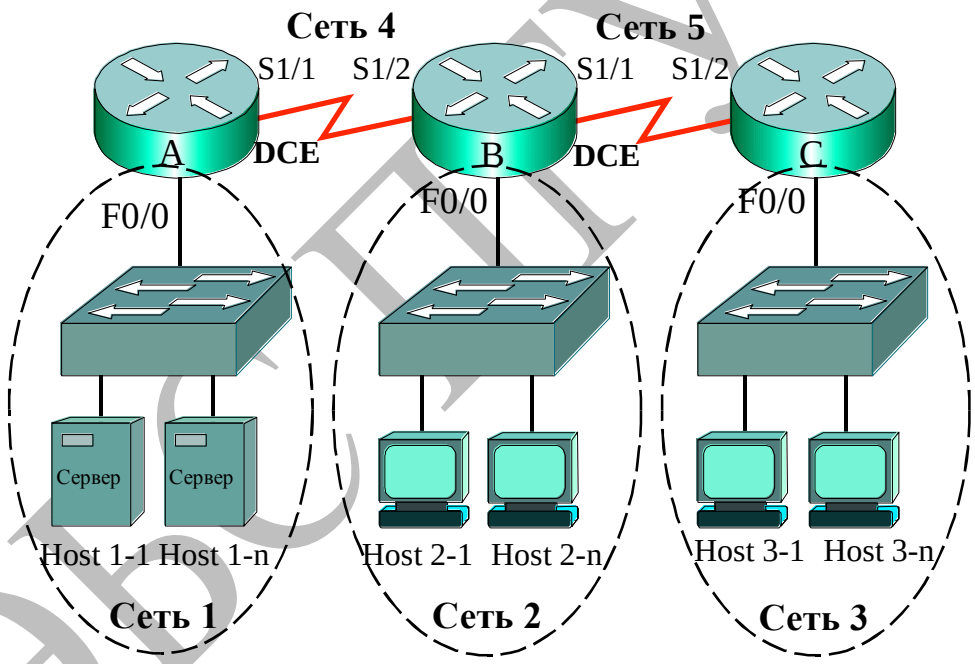

Рис. 2.1. Схема сети

Сконфигурировать адреса в соответствии с табл. 2.1, сконфигурировать протокол RIP.
Проверить работоспособность сети!!!

Таблица 2.1

Адреса сетей и интерфейсов маршрутизаторов

	IP-адрес сети	Интерфейсы	IP-адрес интерфейса

Сеть 1	192.168.10.0/24	F0/0	192.168.10.1
Сеть 2	192.168.20.0/24	F0/0	192.168.20.1
Сеть 3	192.168.30.0/24	F0/0	192.168.30.1
Сеть 4	200.40.40.0/24	S1/1	200.40.40.11
		S1/2	200.40.40.12
Сеть 5	200.50.50.0/24	S1/1	200.50.50.11
		S1/2	200.50.50.12

Адреса конечных узлов:
Host 1-1 – 192.168.10.11, Host 1-n – 192.168.10.24, Host 2-1 – 192.168.20.11, Host 2-n – 192.168.20.24, Host 3-1 – 192.168.30.11, Host 3-n – 192.168.30.24.

Задание 1. Необходимо, чтобы серверы Сети 1 были доступны только узлу Host 2-1 Сети 2 с адресом 192.168.20.11, а все остальные узлы Сети 2 и Сети 3 не имели бы доступа в Сеть 1. Список доступа следует установить на интерфейс F0/0 маршрутизатора Router_A. Номер списка доступа (10) выбирается из диапазона 1 – 99. Адреса сетей, а также названия и адреса интерфейсов приведены в табл. 2.1.

Создание и установка списка доступа производится по командам:

Router_A(config)#**access-list 10 permit 192.168.20.11**

Router_A(config)#**int f0/0**

Router_A(config)#**ip access-group 10 out**

Согласно созданной конфигурации ко всем исходящим из маршрутизатора пакетам через интерфейс F0/0 будет применяться список доступа:
permit 192.168.20.11 – присутствует в списке в явном виде,

deny any – присутствует неявно в конце каждого списка доступа.

Некоторые версии операционных систем IOS маршрутизаторов требуют в обязательном порядке использование масок WildCard при задании адресов узлов и сетей, либо расширения **host** при задании адресов узлов.

Проверить работоспособность списка доступа!

Задание 2. Серверы Сети 1 должны быть доступны всем узлам Сети 2 и узлу Host 3-1 Сети 3 с адресом 192.168.30.11, остальные узлы Сети 3 не должны иметь доступа. Список доступа установить на интерфейс F0/0 Router_A. В списке доступа имеются адреса сети и отдельного узла, поэтому необходимо использовать маску WildCard. Нулевые значения маски WildCard означают требование обработки соответствующих разрядов адреса, а единичные значения – игнорирование соответствующих разрядов адреса при функционировании списка доступа. Таким образом, маска **0.0.0.0** предписывает

анализ и обработку всех разрядов адреса, т.е. в этом случае будет обрабатываться адрес каждого узла. Маска **0.0.0.255** показывает, что обрабатываться будет только сетевая часть адреса класса С.
Следовательно, список доступа будет следующим:

Router_A(config)#**access-list 11 permit 192.168.30.11 0.0.0.0**

Router_A(config)#**access-list 11 permit 192.168.20.0 0.0.0.255**

Router_A(config)#**int f0/0**

Router_A(config)#**ip access-group 11 out**

Согласно созданной конфигурации ко всем исходящим из маршрутизатора пакетам через интерфейс f0/0 будет применяться список доступа:
permit 192.168.30.11 – разрешение узлу с инвертированной маской WildCard **0.0.0.0**,
permit 192.168.20.0 – разрешение сети с инвертированной маской WildCard **0.0.0.255**,
deny any – присутствует неявно в конце списка доступа.

Записи **192.168.30.11 0.0.0.0** полностью соответствует другой вариант – **host 192.168.30.11**, который также предписывает обрабатывать адрес только одного узла. **Проверить данный вариант**!

Задание 3. В Сети рис.2.1 необходимо установить список доступа, который:

1. блокирует рабочей станции 192.168.20.11 Сети 2 доступ в Сеть1;
2. блокирует рабочей станции 192.168.30.24 Сети 3 доступ в Сеть1;

Для этого создается список доступа:

Router_A(config)#**access-list 12 deny host 192.168.20.11**

Router_A(config)#**access-list 12 deny host 192.168.30.24**

Router_A(config)#**access-list 12 permit any**

Router_A(config)#**int f0/0**

Router_A(config-if)#**ip access-group 12 out**

Данный список блокирует доступ в Сеть 1 только двум рабочим станциям 192.168.20.11 и 192.168.30.24, а всем остальным – доступ разрешен. Если бы отсутствовала третья строка списка доступа, то ни одна станция из других сетей не могла бы попасть в Сеть 1.

Проверить работоспособность списка доступа!

Задание 4. Используя исходные данные **Задания 3**, сформировать список доступа в виде именованного (имя ACL):

Router_A(config)#**ip access-list standard ACL**
Router_A(config)#**deny host 192.168.20.11**
Router_A(config)#**deny host 192.168.30.24**
Router_A(config)#**permit any**
Router_A(config)#**int f0/0**
Router_A(config-if)#**ip access-group ACL out**

Проверить работоспособность списка доступа!

Задание 5. На маршрутизаторе А (рис.2.1) необходимо установить расширенный список доступа, который:

1. блокирует рабочим станциям Сети 2 доступ в Сеть1 по **telnet**;
2. разрешает рабочим станциям Сети 2 доступ в Сеть1 по другим протоколам, например, по команде **ping** протокола ICMP.

Для этого необходимо сконфигурировать пароли на маршрутизаторе А:

Router_A(config)#**line vty 0 15**
Router_A(config-line)#**password cisco-1**
Router_A(config-line)#**login**
Router_A(config-line)#**exit**
Router_A(config)#**enable secret cisco-2**

Выполнить удаленный доступ к маршрутизатору Router_A с конечного узла 192.168.20.11:

PC>**telnet 192.168.10.1**
…
Password:
Router_A>**ena**
Password: (*ввести пароль*)
Router_A#**conf t**

Изменить конфигурацию маршрутизатора, например, изменить имя:

Router_A(config)#**hostname R_A**
R_A(config)#

Выполнить команду:

PC>**ping 192.168.10.1**

Прокомментировать результаты выполнения команд telnet и **ping!**

Сформировать список доступа, блокирующий рабочим станциям Сети 2 доступ в Сеть1 по **telnet** и разрешающий доступ в Сеть1 по команде **ping.:**

R_A(config)#**access-list 102 deny tcp 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255 eq 23**
R_A(config)#**access-list 102 permit ip any any**
R_A(config)#**int s1/1**
R_A(config-if)#**ip access-group 102 in**

Выполнить удаленный доступ к маршрутизатору R_A (адрес 192.168.10.1) с конечного узла 192.168.20.11.

PC>**telnet 192.168.10.1**

Выполнить команду PC>**ping 192.168.10.1**

Прокомментировать результаты выполнения команд telnet и **ping!**

Лабораторная работа № 3
Конфигурирование безопасности коммутатора

Лабораторная работа выполняется для сети (рис.3.1), адреса – в табл. 3.1.

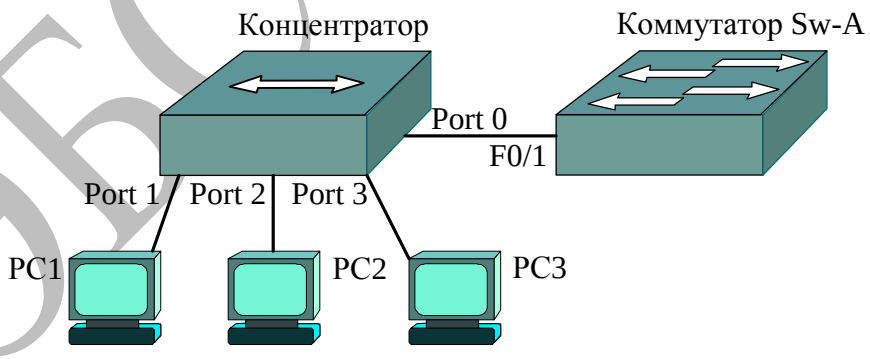

Рис.3.1. Схема сети

Таблица 3.1

Адреса сетей и интерфейсов маршрутизаторов

Устройство		Адрес	Маска	Шлюз
PC1	NIC	10.1.10.21	255.255.255.0	10.1.10.11
PC2	NIC	10.1.10.22	255.255.255.0	10.1.10.11

PC3	NIC	10.1.10.23	255.255.255.0	10.1.10.11
S1	Vlan 101	10.1.10.11	255.255.255.0	10.1.10.1

1. Собрать схему сети рис.3.1.

2. Сконфигурировать адресную информацию на компьютерах PC1, PC2, PC3 согласно табл. 3.1.

3. Выполнить последовательность команд:

Switch>**en**
Switch#**sh run**
Switch#**sh start**
Switch#**sh vlan brief**
Switch#**sh int vlan 1**
Switch#**sh ip int vlan 1**
Switch#**sh int f0/1**

Обратить внимание на состояние устройств и интерфейсов (включен – **up** или выключен **down**), их IP-адреса и MAC-адреса, к каким виртуальным сетям **vlan** приписаны порты коммутатора.

4. Сконфигурировать имя коммутатора и пароли на нем:

Switch(config)#**hostname Sw-A**
Sw-A(config)#**line console 0**
Sw-A(config-line)#**password cisco-1**
Sw-A(config-line)#**login**
Sw-A(config-line)#**line vty 0 15**
Sw-A(config-line)#**password cisco-2**
Sw-A(config-line)#**login**
Sw-A(config-line)#**exit**
Sw-A(config)#**enable secret cisco-3**

5. Используя команды **exit**, вернуться в пользовательский режим. Затем вновь войти в привилегированный режим. Объяснить действие паролей. Проверить пароли по команде **sh run**. Какие пароли представлены в открытой форме, а какие криптографированы? Как зашифровать пароли на консольной и виртуальных линиях?

Выполнить шифрование всех паролей. Произвести проверку!

6. Сконфигурировать IP-адрес на коммутаторе для управления с удаленного устройства. По умолчанию управляющей является виртуальная локальная сеть vlan 1, на которую и выполняют атаки хакеры. Поэтому в качестве управляющей рекомендуется использовать виртуальную сеть с другим

номером, например vlan 101, на интерфейс которой устанавливается адрес шлюза по умолчанию (10.1.10.11) компьютеров PC1, PC2, PC3.

Sw-A(config)#**vlan 101**
Sw-A(config-vlan)#**exit**
Sw-A(config)#**int vlan 101**
Sw-A(config-if)#**ip add 10.1.10.11 255.255.255.0**
Sw-A(config-if)#**no shutdown**

7. Выполнить команды верификации:

Sw-A#**sh vlan brief**
Sw-A#**sh int vlan 101**

Прокомментировать полученные результаты.

8. Приписать порт f0/1 к vlan 101:

Sw-A(config)#**int f0/1**
Sw-A(config-if)#**switchport access vlan 101**

9. Установить шлюз по умолчанию:

Sw-A(config)#**ip default-gateway 10.1.10.1**

10. Выполнить команды верификации:

Sw-A#**sh run**
Sw-A#**sh vlan brief**
Sw-A#**sh int vlan 101**
Sw-A#**sh mac-address-table**

Прокомментировать полученные результаты.
11. С компьютера PC1 выполнить удаленный доступ к коммутатору:

PC1>**telnet 10.1.10.11**

12. С компьютера PC1 в режиме удаленного доступа произвести изменение конфигурации коммутатора, например, изменить имя коммутатора на S1.

13. Завершить сеанс удаленного доступа, используя команды **exit**.

14. Убедиться в изменении конфигурации коммутатора, войдя в режим конфигурирования коммутатора CLI.

15. Выполнить команду:

S1#**sh mac-address-table**

Команду повторить через 5 минут.

Объяснить полученный результат.

16. Определить физические адреса сетевых карт компьютеров по команде **ipconfig /all** для компьютеров PC1, PC2 и PC3. **Записать** MAC-адреса..

17. Сконфигурировать статическую запись в таблице маршрутизации, приписав MAC-адрес компьютера PC1 к порту Fa0/1 коммутатора:

S1(config)#**mac-address-table static** *Mac-адрес* **vlan 101 interface fastethernet 0/1**

Проверить таблицу коммутации.

18. Удалить статическую запись из таблицы коммутации. Проверить таблицу коммутации.

Конфигурирование безопасности порта коммутатора

19. Сконфигурировать безопасность порта f0/1:

S1(config)#**int f0/1**
S1(config-if)#**switchport mode access**
S1(config-if)#**switchport port-security**

Задать количество безопасных адресов, равное 1:

S1(config-if)#**switchport port-security maximum 1**

Установить режим безопасных адресов **sticky**:

S1(config-if)#**switchport port-security mac-address sticky**

Установить режим реагирования на нарушение безопасности **shutdown**:

S1(config-if)#**switchport port-security violation shutdown**

20. Проверить текущую конфигурацию и таблицу коммутации по командам **show running-configuration** и **show mac-address-table.** Прокомментировать полученные результаты.

21. Выполнить команду **ping 10.1.10.11** с компьютера PC1. Вновь проверить таблицу коммутации и прокомментировать полученный результат.

22. Выполнить команду **ping 10.1.10.11** с компьютера PC2. Порт коммутатора должен выключиться**.**

23. Выполнить команду **show port-security int f0/1** и прокомментировать полученный результат.

24. Включить порт f0/1 коммутатора. После того, как загорится зеленый индикатор, выполнить команду **ping 10.1.10.11** с компьютера PC1.

25. Выполнить команду **show port-security int f0/1**.

26. Увеличить количество безопасных адресов до 2:

S1(config-if)#**switchport port-security maximum 2**

27. Выполнить команду **ping 10.1.10.11** с компьютеров PC1, PC2.

28. Выполнить команды **show mac-address-table** и **show port-security int f0/1** и прокомментировать полученный результат.

29. Выполнить команду **ping 10.1.10.11** с компьютера PC3. Прокомментировать результат.

Лабораторная работа № 4
Конфигурирование виртуальных локальных сетей

Статическое конфигурирование виртуальных сетей сводится к назначению портов коммутатора на каждую виртуальную локальную сеть VLAN, через использование командной строки CLI.

1. Создать схему лабораторной работы, включающую три виртуальных локальных сети (рис. 4.1) на коммутаторе Sw_A, подключив PC0 к порту f0/1, PC1 – к порту f0/2, PC2 – к порту f0/3, PC3 – к порту f0/4, PC4 – к порту f0/5, PC5 – к порту f0/6:

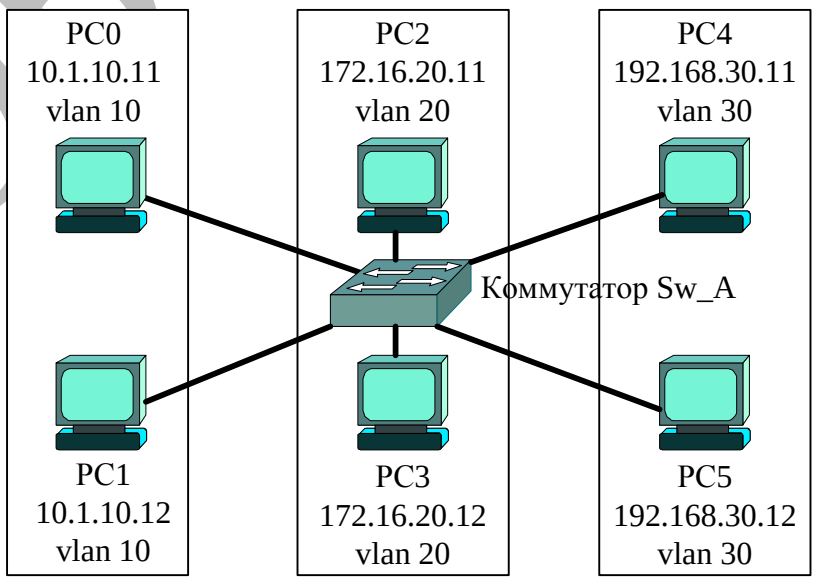

Рис. 4.1. Виртуальные локальные сети

2. Согласно схеме рис.4.1 и Таблице 4.1сконфигурировать на конечных узлах (персональных компьютерах PC0 – PC5) IP-адреса, маски и шлюзы по умолчанию.

Таблица 4.1

Конфигурация конечных узлов виртуальных локальных сетей

VLAN №	Узел	Адрес узла	Маска	Шлюз
Vlan 10	PC0 PC1	10.1.10.11 10.1.10.12	255.255.255.0	10.1.10.1
Vlan 20	PC2 PC3	172.16.20.11 172.16.20.12	255.255.255.0	172.16.20.1
Vlan 30	PC4 PC5	192.168.30.11 192.168.30.12	255.255.255.0	192.168.30.1

Таким образом, каждая виртуальная локальная сеть имеет свой IP-адрес.

3. По команде **sh vlan brief** посмотреть состояние виртуальных сетей и интерфейсов коммутатора. Прокомментировать результат.

4. Сконфигурировать на коммутаторе три виртуальных локальных сети:

Sw-A(config)#**vlan 10**
Sw-A(config-vlan)#**vlan 20**
Sw-A(config-vlan)#**vlan 30**

5. По команде **sh vlan brief** проанализировать изменения конфигурации.

6. Назначить виртуальные сети на определенные интерфейсы (приписать интерфейсы к созданным виртуальным сетям), используя пару команд **switchport mode access**, **switchport access vlan***№*. Ниже приведен пример указанных операций для сети рис.4.1.

Sw-A(config)#**int f0/1**
Sw-A(config-if)#**switchport mode access**
Sw-A(config-if)#**switchport access vlan 10**
Sw-A(config-if)#**int f0/2**
Sw-A(config-if)#**switchport mode access**
Sw-A(config-if)#**switchport access vlan 10**
Sw-A(config-if)#**int f0/3**

Sw-A(config-if)#**switchport mode access**

Sw-A(config-if)#**switchport access vlan 20**

Sw-A(config-if)#**int f0/4**

Sw-A(config-if)#**switchport mode access**

Sw-A(config-if)#**switchport access vlan 20**

Sw-A(config-if)#**int f0/5**

Sw-A(config-if)#**switchport mode access**

Sw-A(config-if)#**switchport access vlan 30**

Sw-A(config-if)#**int f0/6**

Sw-A(config-if)#**switchport mode access**

Sw-A(config-if)#**switchport access vlan 30**

7. Произвести верификацию полученной конфигурации с помощью команды **show vlan brief**. Прокомментировать результат.

8. Скопировать конфигурационный файл в энергонезависимую память коммутатора по команде:

Sw-A #**copy running-config startup-config**

9. Для отмены неверного назначения виртуальной сети на интерфейс, например, ошибочное назначение виртуальной сети vlan 20 на интерфейс F0/2, используется команда:

Sw-A(config)#**int f0/2**
Sw-A(config-if)#**no switchport access vlan**

Также можно просто приписать интерфейс f0/2 к другой виртуальной сети, например, к vlan 10:

Sw-A(config)#**int f0/2**
Sw-A(config-if)#**switchport mode access**
Sw-A(config-if)#**switch access vlan 10**

10. Проверка работоспособности сети производится по командам ping, (tracert). Проверить соединение PC0 с PC1 и другими компьютерами:

PC0>**ping 10.1.10.12**

PC0>**ping 172.16.20.12**

PC0>**ping 192.168.30.12**

11. Если к сети присоединить дополнительный узел PC6, адрес которого 192.168.30.101 (рис.4.2), т.е. адрес его сети совпадает с адресом сети vlan 30, но узел PC6 не приписан ни к одной из виртуальных сетей, то он не сможет реализовать соединения с узлами существующих виртуальных сетей.
Проверить! Результат показать преподавателю.

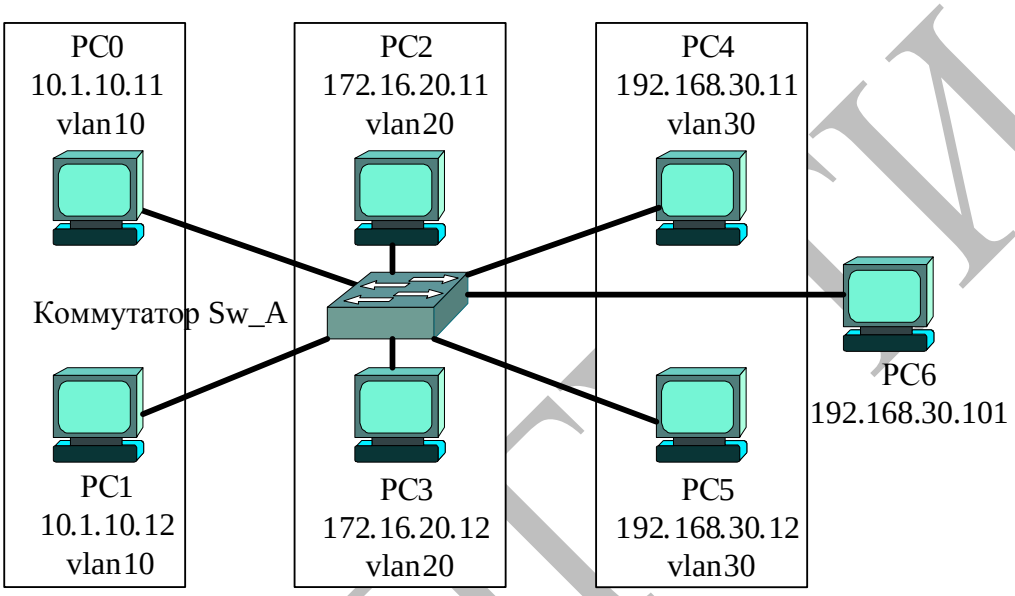

Рис.4.2. Функционирование виртуальных локальных сетей

Формирование виртуальных локальных сетей на нескольких коммутаторах

12. Собрать схему сети рис.4.3.

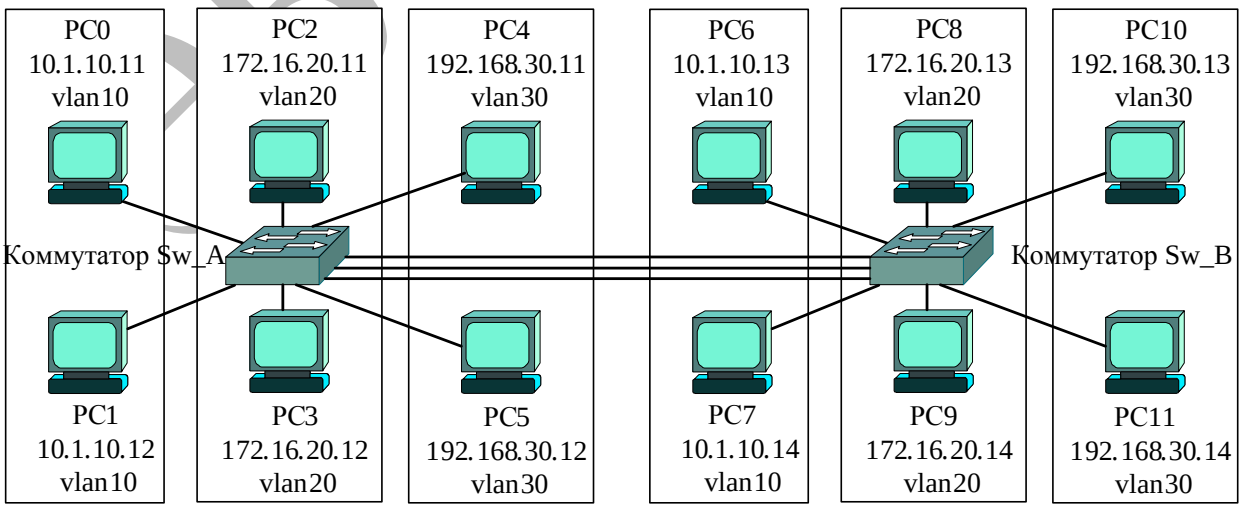

Рис.4.3. VLAN на двух коммутаторах

Согласно схеме рис.4.3 сконфигурировать на конечных узлах (персональных компьютерах PC6 – PC11) IP-адреса, маски и шлюзы по умолчанию. Приписать интерфейсы второго коммутатора Sw_B к vlan 10, vlan 20, vlan 30. Приписать интерфейсы, соединяющие коммутаторы между собой, например f0/7, f0/8, f0/9, к vlan 10, vlan 20, vlan 30.

13. Проверить работоспособность сети. По команде **ping** проверить соединение PC0 с PC1 и другими компьютерами:

PC0>**ping 10.1.10.12**
PC0>**ping 10.1.10.13**
PC0>**ping 10.1.10.14**

PC0>**ping 172.16.20.12**

PC0>**ping 192.168.30.12**

Объяснить результаты!

Маршрутизация между виртуальными локальными сетями

14. Поскольку каждая виртуальная локальная сеть представляет собой широковещательный домен, т.е. сеть со своим IP-адресом, то для связи между сетями необходима маршрутизация Уровня 3. Поэтому к коммутатору необходимо присоединить маршрутизатор (рис.4.4).

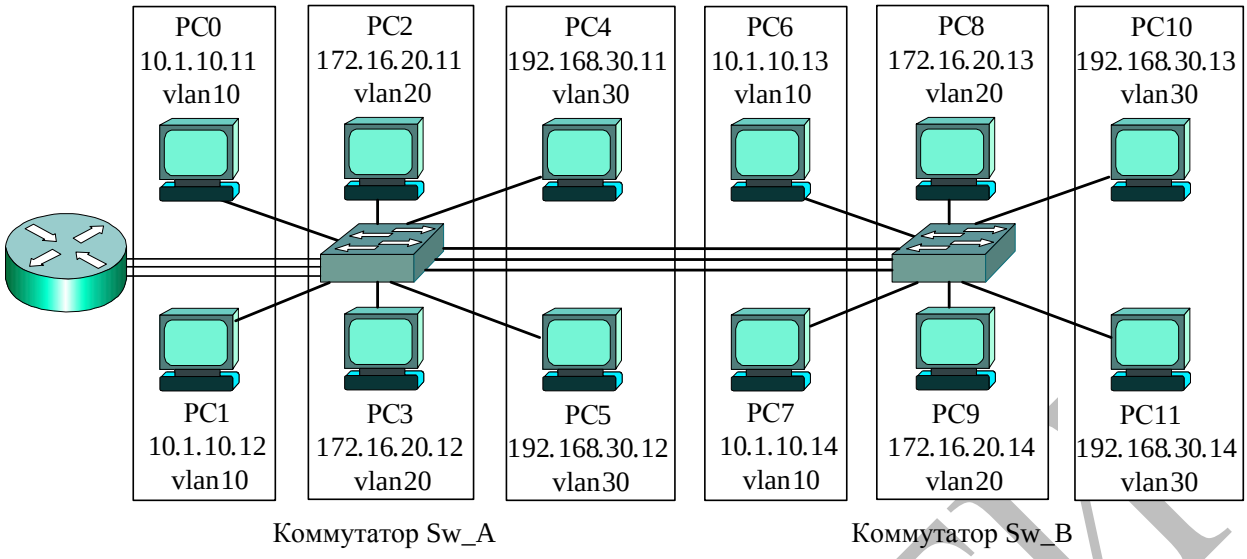

Рис.4.4. Связь между сетями через маршрутизатор

15. Для соединения с маршрутизатором в схеме дополнительно задействованы три интерфейса коммутатора Sw_A: F0/11, F0/12, Ff0/13.При этом порт F0/11 приписан к сети vlan 10, порт F0/12 – к vlan 20, порт F0/13 – к vlan 30.

Sw_A(config)#**int f0/11**
Sw_A(config-if)#**switchport access vlan 10**
Sw_A(config-if)#**int f0/12**
Sw_A(config-if)#**switchport access vlan 20**
Sw_A(config-if)#**int f0/13**
Sw_A(config-if)#**switchport access vlan 30**

16. На маршрутизатор серии 2811 установите дополнительные интерфейсы локальных сетей, например, NM-2FE2W. Таким образом, на маршрутизаторе будут функционировать 4 интерфейса локальных сетей: F0/0, F0/1, F1/0, F1/1.

17. На маршрутизаторе используются три интерфейса F0/0, F0/1, F1/0 (по числу виртуальных сетей), которые сконфигурированы следующим образом:

Router>**ena**
Router#**conf t**
Router(config)#**int f0/0**
Router(config-if)#**ip add 10.1.10.1 255.255.255.0**

Router(config-if)#**no shut**

Router(config-if)#**int f0/1**

Router(config-if)#**ip add 172.16.20.1 255.255.255.0**

Router(config-if)#**no shut**

Router(config)#**int f1/0**

Router(config-if)#**ip add 192.168.30.1 255.255.255.0**

Router(config-if)#**no shut**

18. По команде **shiproute** посмотреть таблицу маршрутизации:

```
Router#shiproute
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.10.0 is directly connected, FastEthernet0/0
     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.20.0 is directly connected, FastEthernet0/1
C    192.168.30.0/24 is directly connected, FastEthernet1/0
```

Из таблицы маршрутизации следует, что все три сети (10.1.10.0, 172.16.20.0, 192.168.30.0) являются непосредственно присоединенными и, следовательно, могут обеспечивать маршрутизацию между сетями. «Прозвонка» с узла 10.1.10.11 узлов сетей 172.16.20.0, 192.168.30.0 должна дать положительный результат.

19. Проверить работоспособность сети. По команде **ping** проверить соединение PC0 со всеми другими компьютерами сети. **Результат показать преподавателю**.

Недостатком такого метода организации межсетевых соединений является необходимость использования дополнительных интерфейсов коммутатора и маршрутизатора, число которых равно количеству виртуальных сетей. От этого недостатка свободно **транковое** соединение, когда совокупность физических каналов между двумя устройствами может быть

заменена одним агрегированным каналом, включающим несколько логических соединений.

Конфигурирование транковых соединений

20. Собрать схему сети рис.4.5. При транковом соединении коммутатора и маршрутизатора три физических канала между ними (рис. 4.4) заменяются одним агрегированным каналом (рис. 4.5).

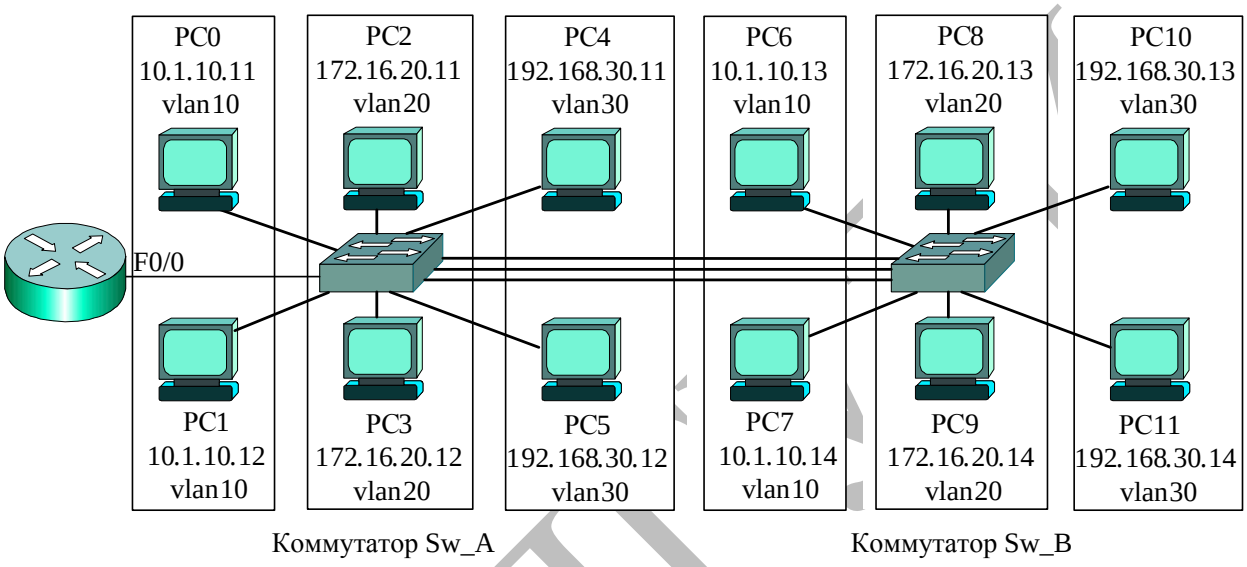

Рис.4.5. Транковое соединение коммутатора и маршрутизатора

Для создания транкового соединения на коммутаторе задействован интерфейс F0/10, а на маршрутизаторе – F0/0.

21. Конфигурирование коммутатора будет следующим:

```
Sw_A>ena
Sw_A#conf t
Sw_A(config)#vlan 10
Sw_A(config-vlan)#vlan 20
Sw_A(config-vlan)#vlan 30
Sw_A(config-vlan)#int f0/1
Sw_A(config-if)#switchport mode access
Sw_A(config-if)#switchport access vlan 10
Sw_A(config-if)#int f0/4
Sw_A(config-if)#switchport access vlan 10
Sw_A(config-if)#int f0/2
Sw_A(config-if)#switchport access vlan 20
Sw_A(config-if)#int f0/5
Sw_A(config-if)#switchport access vlan 20
Sw_A(config-if)#int f0/3
```

Sw_A(config-if)#**switchport access vlan 30**
Sw_A(config-if)#**int f0/6**
Sw_A(config-if)#**switchport access vlan 30**
Sw_A(config-if)#**int f0/10**
Sw_A(config-if)#**switchport mode trunk**
Sw_A(config-if)#^Z

22. По команде **sh int f0/10 switchport** можно посмотреть состояние интерфейса:

Sw_A#**sh int f0/10 switchport**
Name: Fa0/10
Switchport: Enabled
Administrative Mode: **trunk**
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
. . .
Sw_A#

Из распечатки следует, что порт F0/10 находится в режиме Trunk.

23. Конфигурирование маршрутизатора сводится к тому, что на его интерфейсе F0/0 формируются субинтерфейсы F0/0.10, F0/0.20, F0/0.30. На указанных субинтерфейсах конфигурируется протокол Dot 1q для виртуальных сетей 10, 20, 30. Последовательность команд необходимо завершить включением интерфейса **no shut**.

Router>**ena**
Router#**conf t**
Router(config-if)#**int f0/0.10**
Router(config-subif)#**encapsulation dot1q 10**
Router(config-subif)#**ip add 10.1.10.1 255.255.255.0**
Router(config-subif)#**int f0/0.20**
Router(config-subif)#**encapsulation dot1q 20**
Router(config-subif)#**ip add 172.16.20.1 255.255.255.0**
Router(config-subif)#**int f0/0.30**
Router(config-subif)#**encapsulation dot1q 30**
Router(config-subif)#**ip add 192.168.30.1 255.255.255.0**

Router(config-subif)#**int f0/0**
Router(config-if)#**no shut**
24. Результат конфигурирования проверяется по команде **sh ip route**:

Router#**sh ip route**

…

Gateway of last resort is not set

  10.0.0.0/24 is subnetted, 1 subnets
C 10.1.10.0 is directly connected, FastEthernet0/0.10
  172.16.0.0/24 is subnetted, 1 subnets
C 172.16.20.0 is directly connected, FastEthernet0/0.20
C   192.168.30.0/24 is directly connected, FastEthernet0/0.30
Router#

Из таблицы маршрутизации следует, что сети 10.1.10.0, 172.16.20.0, 192.168.30.0 являются непосредственно присоединенными. Поэтому маршрутизатор способен обеспечить маршрутизацию между сетями.

25. Проверить работоспособность сети. По команде **ping** проверить соединение всех компьютеров сети между собой. **Результат показать преподавателю**.

26. Сформировать транковое соединение между коммутаторами (рис.4.6)

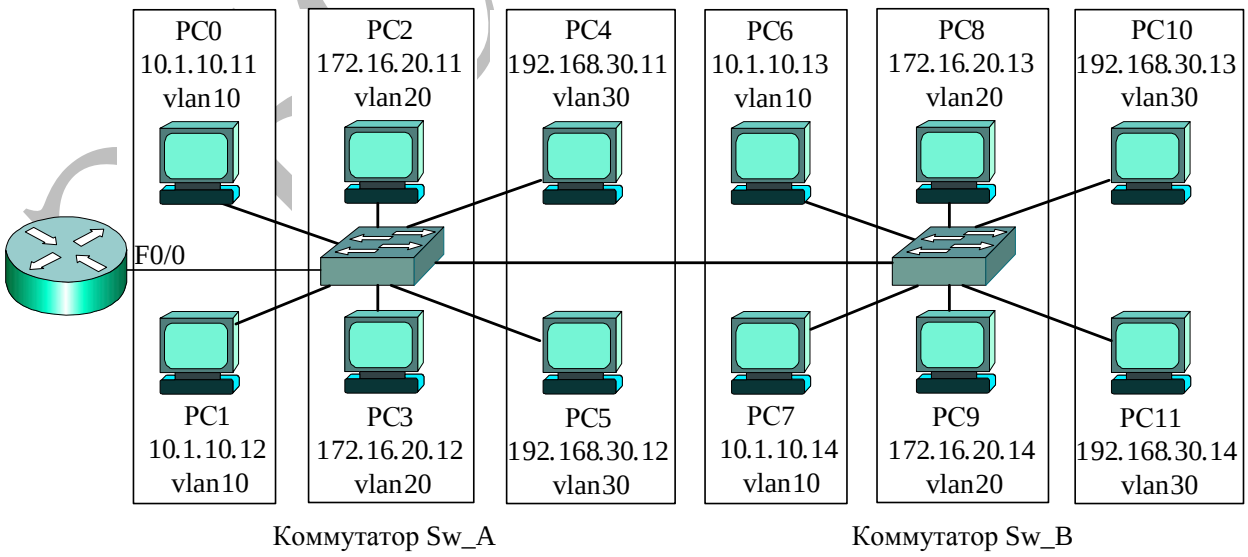

Рис.4.6. Транковое соединение коммутаторов

27. Проверить работоспособность сети. По команде **ping** проверить соединение всех компьютеров сети между собой. **Результат показать преподавателю**.

Список литературы

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. СПб: Издательство «Питер» - 2011. – 944 с.
2. Васин Н.Н. Основы сетевых технологий на базе коммутаторов и маршрутизаторов: Учебное пособие – М.: Интуит,: БИНОМ. 2011. – 270 с.
3. Васин Н.Н. Сети и системы передачи информации на базе коммутаторов и маршрутизаторов (Конспект лекций): Учебное пособие. – Самара: ПГУТИ, 2010. 362 с.
4. Васин Н.Н. Сети и системы передачи информации на базе коммутаторов и маршрутизаторов CISCO: Учебное пособие. – Самара: ПГАТИ, 2008. 236 с.
5. Васин Н.Н., Ротенштейн И.В. Основы конфигурирования маршрутизаторов. Методические указания к лабораторным работам. – Самара: ПГУТИ. 2011. – 37 с.