Федеральное государственное бюджетное образовательное учреждение высшего образования
Поволжский государственный университет телекоммуникаций и информатики
(ПГУТИ)

Васин Н.Н.

Технологии пакетной коммутации и маршрутизации

Методические указания по выполнению курсовой работы

Для студентов направления подготовки бакалавров
11.03.02 – Инфокоммуникационные технологии и системы связи,

Самара, ПГУТИ
2021

УДК 004.7

Н.Н. Васин

Технологии пакетной коммутации и маршрутизации: Методические указания по выполнению курсовой работы / Васин Н.Н. – Самара: ПГУТИ, ИУНЛ, 2021. – 19 с.

Методические указания по выполнению курсовой работы предназначены для студентов направления подготовки бакалавров 11.03.02 – Инфокоммуникационные технологии и системы связи, в рамках учебного курса «Технологии пакетной коммутации и маршрутизации».

В ходе выполнения курсовой работы моделируется схема сети с коммутацией пакетов, конфигурируются сетевые устройства распределенной составной сети, реализованной на коммутаторах, маршрутизаторах и конечных узлах. В методических указаниях приведены индивидуальные задания на выполнение курсовой работы, порядок выполнения задания, примеры конфигурирования устройств.

Рецензент:
Карташевский В.Г. – д.т.н., профессор, зав. кафедрой ИБ

Поволжский государственный университет телекоммуникаций и информатики

2021

Задание на курсовую работу

1. В среде Packet Tracer сформируйте схему сети (рис. 1). Используйте маршрутизаторы серии 2911, коммутаторы – серии 2960.

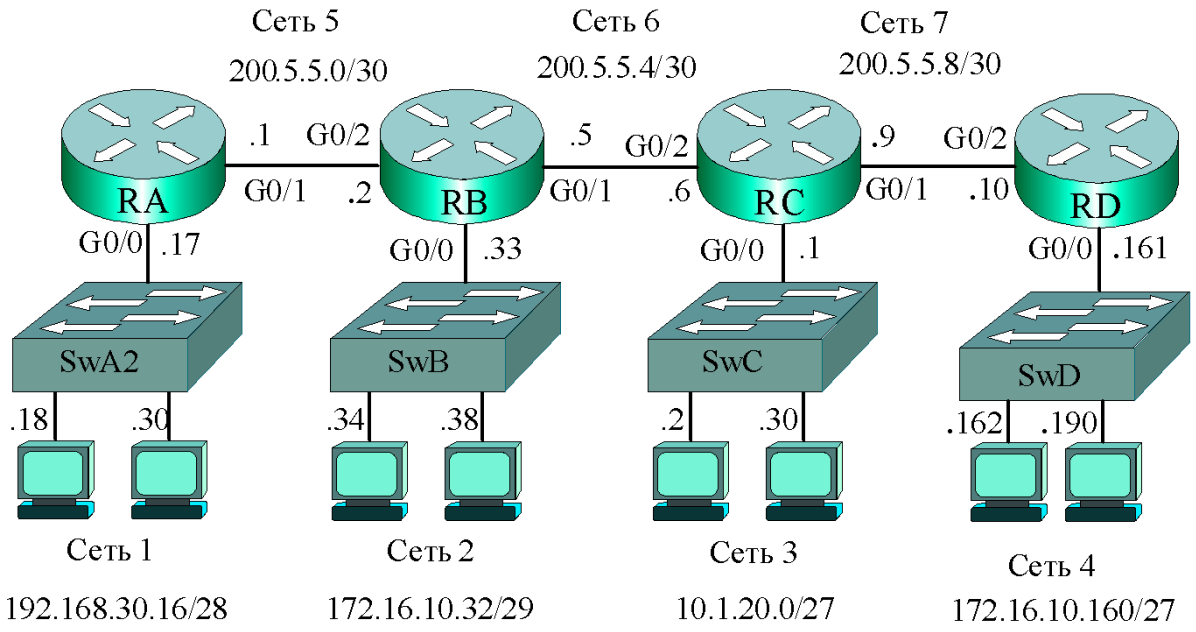

Рис.1. Составная сеть

2. Индивидуальные задания приведены в табл. 1, там же заданы адреса сетей и префиксы.

3. Согласно заданию распределите адреса между всеми устройствами. Первый адрес в сети задайте шлюзу по умолчанию (`Default` Gateway).

4. Сконфигурируйте интерфейсы всех маршрутизаторов. Процесс конфигурирования отразите в пояснительной записке.

5. На маршрутизаторах сконфигурируйте заданный протокол маршрутизации (RIP2, OSPF, EIGRP).

6. Проведите отладку сети с использованием команд **show ip route**, **show running-config, show ip interface brief**, **ping**.

7. **Основные параметры, объяснения, комментарии представьте в пояснительной записке**.

Таблица 1

Индивидуальные задания

		Сеть 1	Сеть 2	Сеть 3	Сеть 4
1	RIPv2	**192.168.10.32/27**	172.16.20.16/28	10.1.30.0/27	192.168.10.64/29
2	EIGRP	**192.168.10.64/27**	172.16.20.32/28	10.1.30.0/27	192.168.10.128/29
3	OSPF	**192.168.10.96/27**	172.16.20.48/28	10.1.30.0/27	192.168.10.192/29
4	RIPv2	**172.16.10.0/27**	10.1.20.128/27	192.168.30.8/29	172.16.10.192/28
5	EIGRP	**172.16.10.0/27**	10.1.20.160/27	192.168.30.16/29	172.16.10.64/28
6	OSPF	**172.16.10.0/27**	10.1.20.192/27	192.168.30.24/29	172.16.10.128/28
7	RIPv2	10.1.10.16/28	172.16.20.128/29	**192.168.30.0/27**	10.1.10.64/27
8	EIGRP	10.1.10.32/28	172.16.20.136/29	**192.168.30.0/27**	10.1.10.128/27
9	OSPF	10.1.10.48/28	172.16.20.144/29	**192.168.30.0/27**	10.1.10.192/27
10	RIPv2	192.168.10.8/29	**172.16.20.32/27**	10.1.30.0/27	192.168.10.32/28
11	EIGRP	192.168.10.16/29	**172.16.20.64/27**	10.1.30.0/27	192.168.10.64/28
12	OSPF	192.168.10.24/29	**172.16.20.96/27**	10.1.30.0/27	192.168.10.96/28
13	RIPv2	172.16.10.0/27	10.1.20.8/29	192.168.30.128/28	**172.16.10.64/27**
14	EIGRP	172.16.10.0/27	10.1.20.16/29	192.168.30.144/28	**172.16.10.128/27**
15	OSPF	172.16.10.0/27	10.1.20.24/29	192.168.30.160/28	**172.16.10.192/27**
16	RIPv2	10.1.10.32/29	**192.168.20.128/27**	172.16.30.0/28	192.168.20.0/27
17	EIGRP	10.1.10.64/29	**192.168.20.160/27**	172.16.30.0/28	192.168.20.0/27
18	OSPF	10.1.10.96/29	**192.168.20.192/27**	172.16.30.0/28	192.168.20.0/27
19	RIPv2	192.168.30.8/29	172.16.10.128/28	**10.1.20.128/27**	172.16.10.32/27
20	EIGRP	192.168.30.16/29	172.16.10.144/28	**10.1.20.160/27**	172.16.10.64/27
21	OSPF	192.168.30.24/29	172.16.10.160/28	**10.1.20.192/27**	172.16.10.96/27

22	RIPv2	**172.16.30.128/27**	10.1.10.64/27	192.168.20.24/29	10.1.10.192/28
23	EIGRP	**172.16.30.160/27**	10.1.10.96/27	192.168.20.32/29	10.1.10.176/28
24	OSPF	**172.16.30.192/27**	10.1.10.128/27	192.168.20.40/29	10.1.10.160/28
25	RIPv2	10.1.30.128/29	**192.168.10.160/27**	172.16.20.32/27	192.168.10.64/28
26	EIGRP	10.1.30.136/29	**192.168.10.192/27**	172.16.20.64/27	192.168.10.80/28
27	OSPF	10.1.30.144/29	**192.168.10.224/27**	172.16.20.96/27	192.168.10.96/28
28	RIPv2	192.168.30.48/28	172.16.10.48/29	**10.1.20.0/27**	172.16.10.192/27
29	EIGRP	192.168.30.32/28	172.16.10.40/29	**10.1.20.0/27**	172.16.10.128/27
30	OSPF	192.168.30.16/28	172.16.10.32/29	**10.1.20.0/27**	172.16.10.160/27

Сеть 5 имеет адрес 200.5.5.0/30, Сеть 6 – 200.5.5.4/30, Сеть 7 – 200.5.5.8/30

8. В одной из сетей с префиксом /27 (в рассматриваемом примере – Сеть 3 выделенная в табл. 1 жирным шрифтом) замените маршрутизатор RC на многоуровневый коммутатор MSw (рис. 2). Согласно схеме сети сформируйте три виртуальных локальных сети (Vlan 10, Vlan 20, Vlan 30).

9. Проведите конфигурирование виртуальных локальных сетей Vlan 10, Vlan 20, Vlan 30 на коммутаторах MSw, SwC1, SwC2 сети рис. 2.

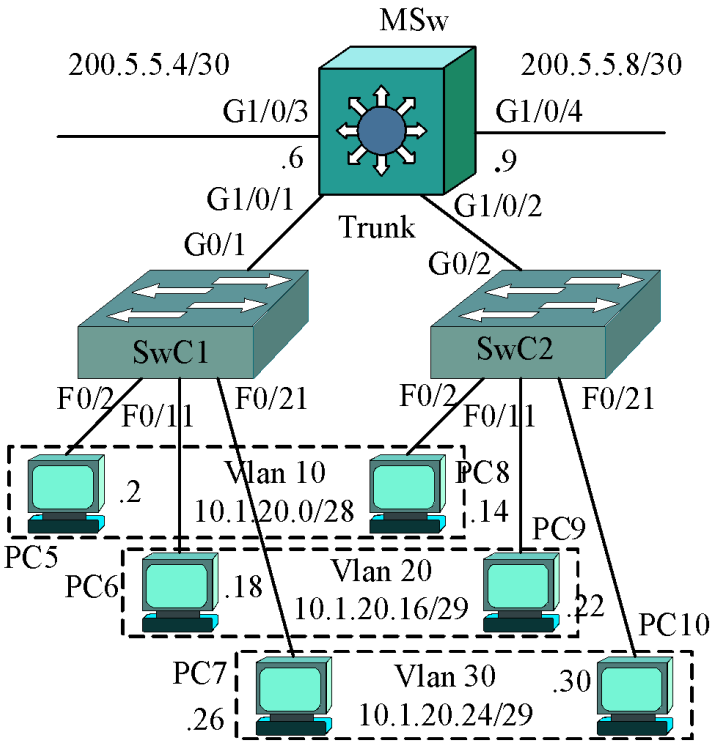

Рис. 2. Формирование виртуальных локальных сети

10. Сформируйте схему сети, объединив схемы рис. 1 и 2. Схема должна быть приведена в пояснительной записке. На схеме укажите адреса интерфейсов и узлов (рис. 3).

11. Сконфигурируйте безопасность на интерфейсах коммутатора, например в локальной сети с префиксом /29 на коммутаторе SwB (рис. 3).:

12. Сконфигурируйте списки доступа к одной из локальных сетей, например к сети с префиксом /29 на маршрутизаторе RB (рис. 3). Запретите удаленный доступ к указанной сети по протоколу SSH одному узлу виртуальной сети Vlan 1. Всем остальным узлам доступ разрешить.

13. Проверьте функционирование обобщенной сети, используя команды **ping, tracert, traceroute, show running-config, show ip route, show access-list, show vlan** и др. Результаты проверки отобразите в пояснительной записке.

Пример выполнения курсовой работы

Задание 30.

30	OSPF	192.168.30.16/28	172.16.10.32/29	**10.1.20.0/27**	172.16.10.160/27

1. Для заданного варианта, соответствующего номеру в списке группы, по заданным адресам и префиксам рассчитайте максимальное количество IP-адресов в каждой из сетей. Сформируйте схему сети (рис. 1).

2. Рассчитайте адреса первого и последнего компьютера в каждой сети, а также шлюза по умолчанию. Определите широковещательный адрес сети. Адреса должны быть отражены в пояснительной записке.

Например, в сети 1: адрес шлюза – 192.168.30.17;
адрес первого компьютера – 192.168.30.18;
адрес последнего компьютера – 192.168.30.30;
широковещательный адрес – 192.168.30.31.

Аналогично адресуйте другие сети.

3. Сконфигурируйте основные параметры **всех маршрутизаторов**, задав имя и сконфигурировав интерфейсы. Например, маршрутизатор RA:

```
Router(config)#hostname RA
RA(config)#interface gigabitEthernet0/0
RA(config-if)#ip address 192.168.30.17 255.255.255.240
RA(config-if)#no shutdown
RA(config-if)#interface gigabitEthernet0/1
RA(config-if)#ip address 200.5.5.1 255.255.255.252
A(config-if)# no shutdown
```

Аналогично сконфигурируйте остальные маршрутизаторы RB, RC, RD.

4. Сконфигурируйте протокол маршрутизации

4.1. В первом варианте устанавливают RIPv2. Например, на RA:

```
RA(config)#router rip
RA(config-router)#version 2
RA(config-router)#network 192.168.30.0
RA(config-router)#network 200.5.5.0
RA(config-router)#no auto-summary
```

Задается протокол RIP, версия 2, адреса присоединенных сетей полного класса (без задания маски), отменяется автосуммирование адресов.

Аналогично конфигурируют другие маршрутизаторы: RB, RC, RD.

4.2. Вариант протокола EIGRP:

```
RA(config)#router eigrp 20
RA(config-router)#network 192.168.30.16  0.0.0.15
RA(config-router)#network 200.5.5.0  0.0.0.3
```

Задается протокол EIGRP, номер автономной системы (например 20), адреса присоединенных подсетей и их инверсные маски. В старых версиях протокола EIGRP отменялось автосуммирование адресов, в новых – автосуммирование отменено по умолчанию.

4.3. Вариант протокола OSPF:

```
RA(config)#router ospf 1
RA(config-router)#network 192.168.30.16 0.0.0.15 area 0
RA(config-router)#network 200.5.5.0 0.0.0.3 area 0
```

Задается протокол OSPF, номер процесса (например 1), адреса присоединенных подсетей и их инверсные маски, задается номер области. В курсовой работе используется единственная область **area 0**. Автосуммирование адресов протокол не выполняет.

5. На одном из маршрутизаторов (в сети, где префикс /28), например на RA, установите пароли на консоль, на виртуальные линии, на вход в привилегированный режим. Используются нижеприведенные команды .

```
RA(config)#line console 0
RA(config-line)#password cis-1
RA(config-line)#login
RA(config-line)#line vty 0 4
RA(config-line)#password cis-2
RA(config-line)#login
```

```
RA(config-line)#exit
RA(config)#enable secret cisco
```

6. Проверьте функционирование паролей. В пояснительной записке приведите распечатки и комментарии.

7. Текущую конфигурацию маршрутизатора проверьте по команде **show running-config**. В пояснительной записке следует отразить только существенные результаты, например:

```
RA#show running-config
...
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
...
interface GigabitEthernet0/0
ip address 192.168.30.17 255.255.255.240
!
interface GigabitEthernet0/1
ip address 200.5.5.1 255.255.255.252
...
router ospf 1
log-adjacency-changes
network 192.168.30.16 0.0.0.15 area 0
network 200.5.5.0 0.0.0.3 area 0
...
line con 0
password cis-1
login
...
line vty 0 4
password cis-2
login
...
RA#
```

Результат по всем маршрутизаторам в **компактной форме** отобразите в пояснительной записке. Прокомментируйте полученные результаты.

8. Проанализируйте таблицы маршрутизации всех маршрутизаторов (RA, RB, RC, RD), например:

```
RA>show ip route
...
   10.0.0.0/27 subnetted, 1 is subnets
O    10.1.20.0/27 [110/3] via 200.5.5.2, 00:22:21,
GigabitEthernet0/1
```

```
   172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
O    172.16.10.32/29 [110/2] via 200.5.5.2, 00:22:21,
GigabitEthernet0/1
O    172.16.10.160/27 [110/4] via 200.5.5.2, 00:22:21,
GigabitEthernet0/1
   192.168.30.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.30.16/28 is directly connected, GigabitEthernet0/0
L    192.168.30.17/32 is directly connected, GigabitEthernet0/0
   200.5.5.0/24 is variably subnetted, 4 subnets, 2 masks
C    200.5.5.0/30 is directly connected, GigabitEthernet0/1
L    200.5.5.1/32 is directly connected, GigabitEthernet0/1
O    200.5.5.4/30 [110/2] via 200.5.5.2, 00:22:21,
GigabitEthernet0/1
O    200.5.5.8/30 [110/3] via 200.5.5.2, 00:22:21,
GigabitEthernet0/1
```

9. В пояснительной записке объясните, как построены маршруты к удаленным сетям, **чему равна метрика и как она рассчитывается,** что такое родительские и дочерние маршруты. Рассчитайте метрики и сравните с заданными значениями в таблице маршрутизации.

10. Проверьте и прокомментируйте состояние интерфейсов, например:

```
RA>show ip interface brief
Interface              IP-Address  OK? Method Status
Protocol
GigabitEthernet0/0  192.168.30.17 YES manual up
up
GigabitEthernet0/1  200.5.5.1      YES manual up
up
GigabitEthernet0/2  unassigned     YES unset  administratively
down down
Vlan1               unassigned     YES unset  administratively
down down
RA>
```

11. Проведите конфигурирование конечных узлов, задав соответствующий IP-адрес, сетевую маску, шлюз по умолчанию.

12. Проверьте работоспособность сети с использованием команд **ping**, выполняемых из маршрутизатора и с конечных узлов. В пояснительной записке отобразите результаты (**в компактной форме**!), например:

```
PC1:\>ping 172.16.10.162
```

```
Pinging 172.16.10.162 with 32 bytes of data:

Request timed out.
Reply from 172.16.10.162: bytes=32 time<1ms TTL=124
Reply from 172.16.10.162: bytes=32 time<1ms TTL=124
Reply from 172.16.10.162: bytes=32 time<1ms TTL=124
```

13. Внесите изменения в схему сети, согласно рис. 3. Пронумеруйте все PC. В качестве многоуровневого коммутатора (Multilayer Switch – **MSw**) используйте Cisco Catalyst 3650. В режиме Physical включите MSw, установив модуль AC Power Supply. Задайте имя (MSw).

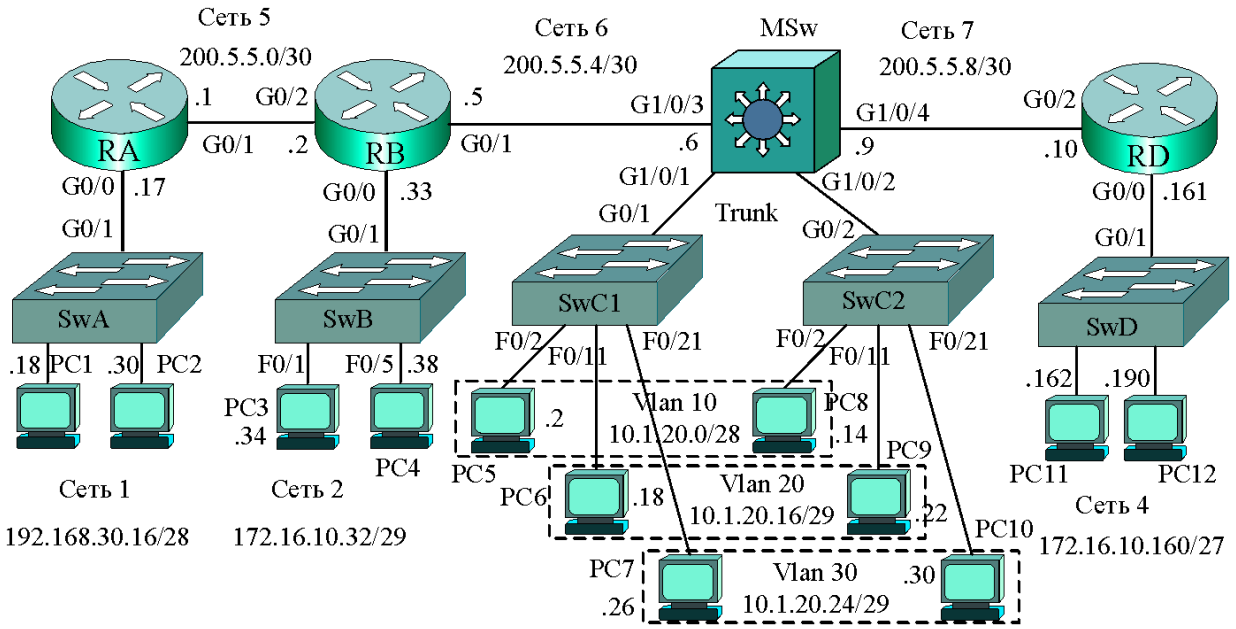

Рис. 3 Схема сети

14. На коммутаторах MSw, SwC1, SwC2 сформируйте три виртуальных локальных сети (vlan 10, vlan 20, vlan 30), например:

```
MSw(config)#vlan 10
MSw(config-vlan)#vlan 20
MSw(config-vlan)#vlan 30
```

15. Для vlan 10 зарезервируйте 16 адресов (10.1.20.0/28), для сети vlan 20 – 8 адресов (10.1.20.16/29), для vlan 30 – 8 адресов (10.1.20.24/29).

16. На порты F0/2 коммутаторов SwC1 и SwC2 назначьте vlan 10. На порты F0/11 коммутаторов SwC1 и SwC2 назначьте vlan 20. На порты F0/21 коммутаторов SwC1 и SwC2 назначьте vlan 30. Например:

```
SwC1(config)#interface fastEthernet0/2
SwC1(config-if)#switchport mode access
SwC1(config-if)#switchport access vlan 10
...
```

Объясните функции приведенных команд.

17. На интерфейсе G1/0/1 коммутатора MSw включите инкапсуляцию dot1q и затем установите транковый режим:

```
MSw(config)#interface g1/0/1
MSw(config-if)#switchport trunk encapsulation dot1q
MSw(config-if)#switchport mode trunk
```

Аналогично сконфигурируйте G1/0/2.

18. Проверьте конфигурацию коммутаторов MSw, SwC1, SwC2 по команде **show vlan brief**, например:

```
MSw#show vlan brief

VLAN Name       Status    Ports
---- ------     ------   -------------------------------
1    default     active   Gig1/0/3, Gig1/0/4, Gig1/0/5, Gig1/0/6
                          Gig1/0/7, Gig1/0/8, Gig1/0/9, Gig1/0/10
                          Gig1/0/11, Gig1/0/12, Gig1/0/13,
                          Gig1/0/14
                          Gig1/0/15, Gig1/0/16, Gig1/0/17,
                          Gig1/0/18
                          Gig1/0/19, Gig1/0/20, Gig1/0/21,
                          Gig1/0/22
                          Gig1/0/23, Gig1/0/24, Gig1/1/1, Gig1/1/2
                          Gig1/1/3, Gig1/1/4
10   VLAN0010   active
20   VLAN0020   active
30   VLAN0030   active
1002      fddi-default active
...
MSw#
```

Объясните, почему в распечатке списка портов (Ports) отсутствуют G1/0/1, G1/0/2. Какие порты отсутствуют в распечатках команды в SwC1, SwC2?

19. Проверьте конфигурацию интерфейсов G1/0/1, G1/0/2 коммутатора MSw, по команде **show interface <**инт**> switchport**, например:

```
MSw>show interface g1/0/1 switchport
Name: Gig1/0/1
Switchport: Enabled
Administrative Mode: trunk
```

```
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
...
```

Из распечатки следует, что административный режим **Trunk**, рабочий (**Operational**) режим тоже **Trunk**, инкапсуляция **dot1q**.

20. Аналогичную команду используйте для проверки портов SwC1, SwC2.

```
C1>show interface g0/1 switchport
Name: Gig0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
```

Особое внимание следует обратить и прокомментировать строки:

```
Administrative Mode: dynamic auto
Operational Mode: trunk
```

21. Объясните, почему рабочие режимы (Operational Mode) порта G0/1 коммутатора SwC1 и порта G0/2 коммутатора SwC2 **транковые**. **Ведь этот режим на них не конфигурировали**!

22. Проверьте связь компьютера PC5 (10.1.20.2) с узлами PC8 (10.1.20.14), PC9 (10.1.20.22) и PC10 (10.1.20.30). Объясните результат.

Маршрутизация между виртуальными локальными сетями

23. Для управления коммутатором и формирования шлюзов Vlan создают виртуальные интерфейсы **SVI**. В рассматриваемом примере сети (рис. 3) на MSw необходимо сконфигурировать три SVI (по числу Vlan). При этом коммутатор MSw будет выполнять маршрутизацию между Vlan 10, 20, 30.

24. Сконфигурируйте виртуальные интерфейсы на MSw:

```
MSw(config)#interface vlan 10
MSw(config-if)#ip address 10.1.20.1 255.255.255.240

MSw(config)#interface vlan 20
MSw(config-if)#ip address 10.1.20.17 255.255.255.248

MSw(config)#interface vlan 30
MSw(config-if)#ip address 10.1.20.25 255.255.255.248
```

25. Проверьте текущую конфигурацию:

```
MSw#show running-config

...
ip routing
...
interface GigabitEthernet1/0/1
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface GigabitEthernet1/0/2
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface GigabitEthernet1/0/3
!
interface GigabitEthernet1/0/4
...
interface Vlan1
no ip address
shutdown

interface Vlan10
mac-address 00d0.5888.7301
ip address 10.1.20.1 255.255.255.240
!
interface Vlan20
mac-address 00d0.5888.7302
ip address 10.1.20.17 255.255.255.248
!
interface Vlan30
mac-address 00d0.5888.7303
ip address 10.1.20.25 255.255.255.248
!
ip classless
...

MSw#
```

26. Убедитесь, что в таблице маршрутизации MSw появились записи маршрутов к присоединенным сетям.

```
MSw#show ip route
...
10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C 10.1.20.0/28 is directly connected, Vlan10
C 10.1.20.16/29 is directly connected, Vlan20
C 10.1.20.24/29 is directly connected, Vlan30

MSw#
```

27. Проверьте связь между узлами всех Vlan, например:

```
PC5:\>ping 10.1.20.30

Pinging 10.1.20.30 with 32 bytes of data:

Request timed out.
Reply from 10.1.20.30: bytes=32 time<1ms TTL=127
Reply from 10.1.20.30: bytes=32 time<1ms TTL=127
Reply from 10.1.20.30: bytes=32 time<1ms TTL=127
```

28. Убедитесь, что связи с узлами из удаленных сетей 1, 2, 4 нет.

29. Создайте **маршрутизируемые порты** многоуровневого коммутатора:

```
MSw(config)#interface g1/0/3
MSw(config-if)#no switchport
MSw(config-if)#ip address 200.5.5.6 255.255.255.252

MSw(config)#interface g1/0/4
MSw(config-if)#no switchport
MSw(config-if)#ip address 200.5.5.9 255.255.255.252
```

Почему отменили режим **switchport**?

30. Сконфигурируйте протокол маршрутизации на MSw.

```
MSw(config)#router ospf 1
MSw(config-router)#network 200.5.5.4 0.0.0.3 area 0
MSw(config-router)#network 200.5.5.8 0.0.0.3 area 0
MSw(config-router)#network 10.1.20.0 0.0.0.15 area 0
MSw(config-router)#network 10.1.20.16 0.0.0.7 area 0
MSw(config-router)#network 10.1.20.24 0.0.0.7 area 0
MSw(config-router)#
```

```
01:36:39: %OSPF-5-ADJCHG: Process 1, Nbr 200.5.5.5 on
GigabitEthernet1/0/3 from LOADING to FULL, Loading Done

01:36:39: %OSPF-5-ADJCHG: Process 1, Nbr 200.5.5.10 on
GigabitEthernet1/0/4 from LOADING to FULL, Loading Done
```

О чем говорят появившиеся записи после таблицы маршрутизации?

31. **Проверьте** функционирования сети, используя команды **ping, tracert, traceroute, show running-config, show ip route, show vlan** и др. Прокомментируйте результат выполнения команд.

32. Соответствующее описание (таблицы маршрутизации – **show ip route**, распечатки команд **show running-config**, результаты «пингования») привести в пояснительной записке в компактной форме и прокомментировать.

Конфигурирование безопасности

33. В сети произведите изменения согласно схемы (рис. 4).

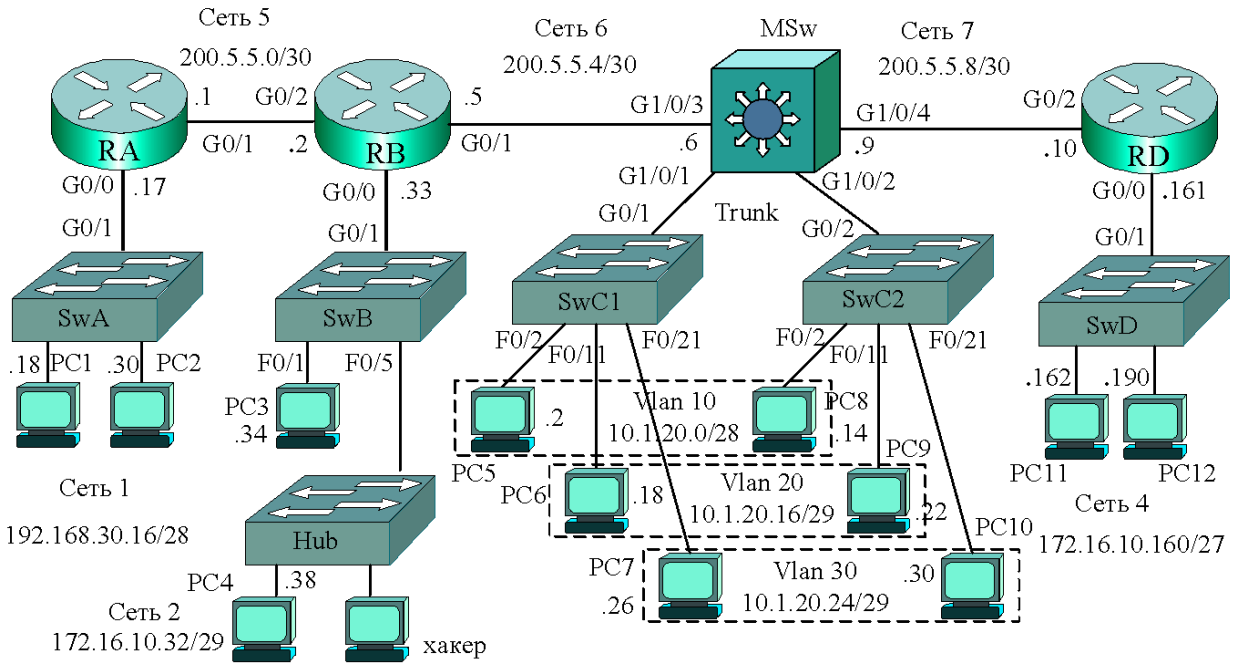

Рис. 4. Видоизмененная схема сети

В локальной сети с префиксом/29 (в данном варианте сеть 172.16.10.32, присоединенная к маршрутизатору RB) выполните конфигурирование безопасности коммутатора SwB на портах F0/1, F0/5, к которым присоединены компьютер PC3 и концентратор Hub. Легальный пользователь PC4 с адресом 172.16.10.38 подключен к коммутатору через концентратор Hub. К свободному порту концентратора подключился нелегальный пользователь (хакер).

34. Выполните команду **`ping`** с компьютера PC3 (172.16.10.34) на узел в той же локальной сети, например:

```
PC3:\>ping 172.16.10.38

Pinging 172.16.10.38 with 32 bytes of data:

Reply from 172.16.10.38: bytes=32 time=1ms TTL=128
Reply from 172.16.10.38: bytes=32 time<1ms TTL=128
Reply from 172.16.10.38: bytes=32 time=1ms TTL=128
Reply from 172.16.10.38: bytes=32 time=1ms TTL=128
```

Связь внутри локальной сети 2 установлена

35. Проанализируйте таблицу MAC-адресов коммутатора SwB:

```
SwB>show mac-address-table
     Mac Address Table
-----------------------------------
Vlan Mac Address     Type     Ports
---- --------------  -------  -----
1    0001.422c.2735  DYNAMIC  Fa0/5
1    000c.cf0a.2020  DYNAMIC  Fa0/1
1    00d0.ff44.0601  DYNAMIC  Gig0/1
```

Прокомментируйте таблицу.

36. Сформируйте безопасность на интерфейсах F0/1 и F0/5 коммутатора:

```
SwB(config)#interface f0/1
SwB(config-if)#switchport mode access
SwB(config-if)#switchport port-security
SwB(config)#interface f0/5
SwB(config-if)#switchport mode access
SwB(config-if)#switchport port-security
```

37. Произведите «прозвонку» с узла 172.16.10.38 на узел 172.16.10.34 и вновь проверьте таблицу MAC-адресов:

```
SwB#show mac-address-table
Mac Address Table
-----------------------------------
Vlan Mac Address     Type    Ports
---- --------------  ------  -----
1    0001.422c.2735  STATIC  Fa0/5
1    000c.cf0a.2020  STATIC  Fa0/1
1    00d0.ff44.0601  DYNAMIC Gig0/1
SwB#
```

38. Установите на компьютере хакера IP-адрес, например 172.16.10.37. Произведите «прозвонку» любого узла сети, например 172.16.10.34.

Объясните и напишите в пояснительной записке, что произошло, почему и как изменить ситуацию.

39. Верните коммутатор SwB в исходное состояние. Неиспользуемые порты выключите.

40. На маршрутизаторе RB сформируйте конфигурацию, обеспечивающую удаленный доступ к RB по протоколу SSH.

```
RB(config)#ip domain-name class
RB(config)#crypto key generate rsa
The name for the keys will be: RB.class
Choose the size of the key modulus in the range of 360
to 2048 for your
General Purpose Keys. Choosing a key modulus greater
than 512 may take a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be
non-exportable...[OK]

RB(config)#username vas secret cisco
*??? 1 0:4:3.608:  %SSH-5-ENABLED: SSH 1.99 has been
enabled
RB(config)#line vty 0 4
RB(config-line)#transport input ssh
RB(config-line)#login local
RB(config-line)#exit
RB(config)#ip ssh version 2
```

41. Проверьте возможность удаленного доступа. Результаты приведите в пояснительной записке, например, удаленный доступ с компьютера 192.168.30.18 из первой сети:

```
C:\>ssh -l vas 172.16.10.33

Password:                                    (cisco)

RB>
```

42. На маршрутизаторе RB сформируйте **список доступа** к локальной сети (172.16.10.32/29), блокирующий доступ по **SSH** к данной сети последнему узлу (PC9) из второй виртуальной локальной сети (vlan 20). Разрешить

доступ к сети 172.16.10.32/29 всем остальным узлам со всеми типами трафика. Список оформить, как именованный, например:

```
RB#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
RB(config)#ip access-list extended ACL
RB(config-ext-nacl)#deny tcp host 10.1.20.22 172.16.10.32 0.0.0.7 eq 22
RB(config-ext-nacl)#permit ip any any
RB(config-ext-nacl)#int g0/1
RB(config-if)#ip access-group ACL in
```

43. Проведите проверку работоспособности списка доступа. Например, проверка доступа с последнего узла (PC9) из второй виртуальной локальной сети (vlan 20) дает следующий результат (объясните его):

```
PC9:\>ssh -l vas 172.16.10.33

% Connection timed out; remote host not responding

C:\>
```

В то же время, обмен пакетами ICMP по команде ping проходит успешно:

```
PC9:\>ping 172.16.10.33

Pinging 172.16.10.33 with 32 bytes of data:

Reply from 172.16.10.33: bytes=32 time=3ms TTL=254
Reply from 172.16.10.33: bytes=32 time<1ms TTL=254
Reply from 172.16.10.33: bytes=32 time<1ms TTL=254
Reply from 172.16.10.33: bytes=32 time<1ms TTL=254
```

Доступ в маршрутизатор RB возможен с другого узла, например:

```
PC5:\>ssh -l vas 172.16.10.33

Password:                                    (cisco)


RB>
```

Однако, доступ в привилегированный режим для анализа текущей конфигурации не возможен:

```
RB>en
% No password set.

RB>
```

Объясните, почему и как исправить ситуацию.

Прокомментируйте результаты выполнения команд ssh, telnet и **ping!**

Список литературы

1. www/netacad.com. Электронный учебник по курсу CCNA. Часть 2. Принципы маршрутизации и коммутации CCNA.
2. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. СПб: Питер, 2011. – 944 с.
3. Васин Н.Н. Технологии пакетной коммутации: Учебник. – М.: ИНТУИТ, 2017. – 408 с.
4. Васин Н.Н. Технологии пакетной коммутации: Учебник. – СПб.: Лань, 2019. – 284 с.