

Министерство образования Республики Беларусь  
Учреждение образования  
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерных систем и сетей  
Кафедра программного обеспечения информационных технологий  
Дисциплина: Сетевые технологии и администрирование операционных  
систем (СТиАОС)

**ОТЧЕТ**  
по лабораторной работе №3

Выполнил  
студент: гр. 851006

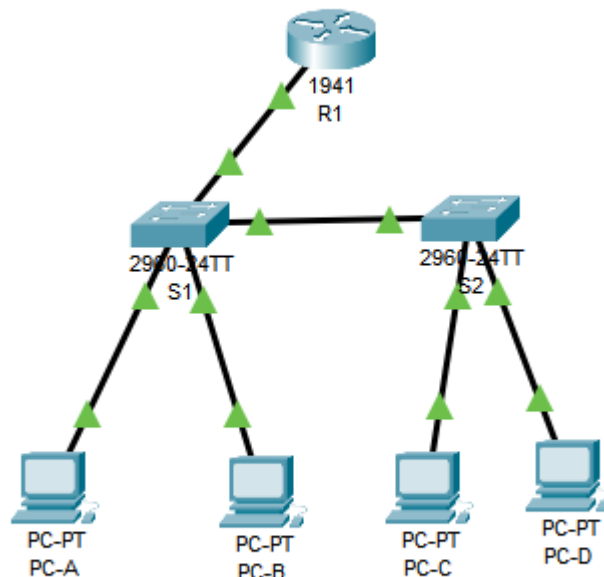
Верещагин Н.В.

Проверил:

Медведев С.А.

Минск 2021

## Топология



### Часть 1: Построение сети и настройка базовых параметров устройства

В первой части лабораторной работы вам предстоит создать топологию сети и настроить базовые параметры для узлов, коммутаторов и маршрутизатора ПК.

**Шаг 1:** Подключите кабели в сети в соответствии с топологией.

**Шаг 2:** Настройте узлы ПК.

**Шаг 3:** Выполните инициализацию и перезагрузку маршрутизатора и коммутаторов.

**Шаг 4:** Настройте базовые параметры каждого коммутатора.

- Настройте имена устройств в соответствии с топологией.
- Настройте IP-адрес, указанный в таблице адресации для сети VLAN 1, на обоих коммутаторах.
- Настройте шлюз по умолчанию на обоих коммутаторах.

**Шаг 5:** Настройте базовые параметры для маршрутизатора.

- Настройте имена устройств в соответствии с топологией.
- Настройте IP-адрес loopback-интерфейса в соответствии с таблицей адресации. На данном этапе не нужно настраивать подынтерфейсы, поскольку их настройка будет выполняться в третьей части лабораторной работы.

## Часть 2: Настройте коммутаторы для работы с сетями VLAN и создания транковых каналов

Во второй части лабораторной работы вы будете настраивать коммутаторы для сетей VLAN и транковых каналов.

### Шаг 1: Настройте сети VLAN на коммутаторе S1.

- а. На коммутаторе S1 настройте сети VLAN и имена, указанные в таблице параметров назначения портов коммутатора.

```
S1(config)# vlan 10
S1(config-vlan)# name Students
S1(config-vlan)# vlan 20
S1(config-vlan)# name Faculty
S1(config-vlan)# exit
```

- б. На коммутаторе S1 настройте интерфейс, подключённый к маршрутизатору R1 в качестве транкового канала. Также настройте интерфейс, подключённый к маршрутизатору R2 в качестве транкового канала.

```
S1(config)# interface fa0/5
S1(config-if)# switchport mode trunk
S1(config-if)# interface fa0/3
S1(config-if)# switchport mode trunk
```

**Перейти в режим администратора и проверить создание транковых каналов.**

```
S1# show interface trunk
```

```
S1# show interface trunk
Port      Mode      Encapsulation  Status        Native vlan
Fa0/3     on        802.1q         trunking      1
Fa0/5     on        802.1q         trunking      1

Port      Vlans allowed on trunk
Fa0/3     1-1005
Fa0/5     1-1005

Port      Vlans allowed and active in management domain
Fa0/3     1,10,20
Fa0/5     1,10,20

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/3     1,10,20
Fa0/5     1,10,20
```

- с. На коммутаторе S1 назначьте порт доступа для компьютеров PC-A сети VLAN 10 и PC-B сети VLAN 20.

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10
S1(config)# interface fa0/2
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 20
```

### Шаг 2: Настройка сетей VLAN на коммутаторе S2.

- а. На коммутаторе S2 настройте сети VLAN и имена, указанные в таблице параметров назначения портов коммутатора аналогично настройке коммутатора S1..

- b. Убедитесь, что номера и имена VLAN на коммутаторе S2 совпадают с данными на коммутаторе S1.

S2# **show vlan brief**

S1:

S1#show vlan brief

VLAN Name	Status	Ports
1 default	active	Fa0/4, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/1, Gig0/2
10 Students	active	Fa0/1
20 Faculty	active	Fa0/2
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

S2:

S2#show vlan brief

VLAN Name	Status	Ports
1 default	active	Fa0/4, Fa0/5, Fa0/6, Fa0/7 Fa0/8, Fa0/9, Fa0/10, Fa0/11 Fa0/12, Fa0/13, Fa0/14, Fa0/15 Fa0/16, Fa0/17, Fa0/18, Fa0/19 Fa0/20, Fa0/21, Fa0/22, Fa0/23 Fa0/24, Gig0/1, Gig0/2
10 Students	active	Fa0/1
20 Faculty	active	Fa0/2
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

Номера и имена VLAN на коммутаторах совпадают

- c. На коммутаторе S2 назначьте порт доступа для компьютера PC-C сети VLAN 10 и PC-D сети VLAN 20
- d. На коммутаторе S2 настройте интерфейс, подключённый к коммутатору S1 в качестве транкового канала.

### Часть 3: Конфигурация маршрутизации между VLAN на основе транкового канала

В третьей части лабораторной работы вам нужно настроить маршрутизатор R1 для маршрутизации данных в несколько сетей VLAN путём создания подынтерфейсов для каждой сети VLAN. Данный метод маршрутизации между VLAN называется конфигурацией ROS (router-on-a-stick).

#### Шаг 1: Настройте подынтерфейс для сети VLAN 1.

- a. Создайте подынтерфейс на интерфейсе G0/1 маршрутизатора R1 для VLAN 1, где 1 — это идентификатор подынтерфейса.

```
R1(config)# interface g0/1.1
```

- b. Настройте подынтерфейс для работы с VLAN 1.

```
R1(config-subif)# encapsulation dot1Q 1
```

- c. Настройте подынтерфейс с IP-адресом из таблицы адресов.

```
R1(config-subif)# ip address 192.168.1.1 255.255.255.0
```

## Шаг 2: Настройте подынтерфейс для сети VLAN 10.

- Создайте подынтерфейс на интерфейсе G0/1 маршрутизатора R1 для VLAN 10, где 10 — это идентификатор подынтерфейса.
- Настройте подынтерфейс для работы с VLAN 10.
- Настройте подынтерфейс с адресом из таблицы адресов.

## Шаг 3: Настройте подынтерфейс для сети VLAN 20.

- Создайте подынтерфейс на интерфейсе G0/1 маршрутизатора R1 для VLAN 20, где 20 — это идентификатор подынтерфейса.
- Настройте подынтерфейс для работы с VLAN 20.
- Настройте подынтерфейс с адресом из таблицы адресов.

## Шаг 4: Включите интерфейс G0/1.

Включите интерфейс G0/1.

```
R1(config)# interface g0/1
```

```
R1(config-if)# no shutdown
```

## Шаг 5: Проверка соединения.

Введите команду, чтобы просмотреть таблицу маршрутизации на R1. Какие сети в ней перечислены?

```
R1#show ip route
Codes: L - local, C - connected, S - static, 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

    192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/1
L       192.168.1.1/32 is directly connected, GigabitEthernet0/1
    192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.10.0/24 is directly connected, GigabitEthernet0/1.10
L       192.168.10.1/32 is directly connected, GigabitEthernet0/1.10
    192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.20.0/24 is directly connected, GigabitEthernet0/1.20
L       192.168.20.1/32 is directly connected, GigabitEthernet0/1.20
    209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.200.224/27 is directly connected, Loopback0
L       209.165.200.225/32 is directly connected, Loopback0
```

Перечислены сети 192.168.1.0, 192.168.10.0, 192.168.20.0, 209.165.200.224

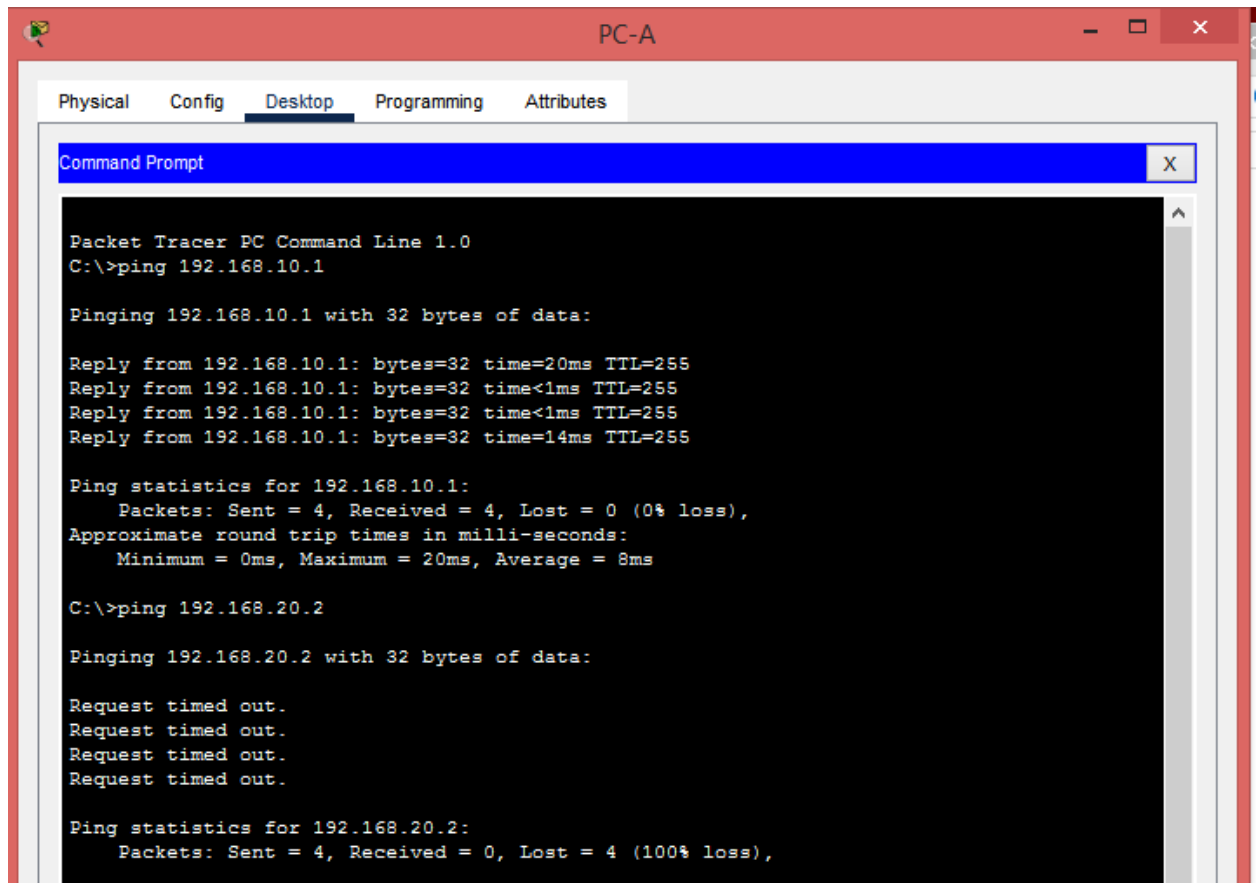
Успешно ли отправляется эхо-запрос с компьютера PC-A на шлюз по умолчанию для VLAN 10? Да

Успешно ли отправляется эхо-запрос от узла PC-A на PC-B? Нет

Успешно ли отправляется эхо-запрос от узла PC-A на PC-C? Да

Успешно ли отправляется эхо-запрос от узла PC-A на PC-D? Нет

Успешно ли отправляется эхо-запрос от PC-A на коммутатор S2? Нет



The screenshot shows a Packet Tracer window titled "PC-A" with tabs for Physical, Config, Desktop, Programming, and Attributes. The "Desktop" tab is active, displaying a "Command Prompt" window. The Command Prompt shows the output of two ping commands. The first command is "C:\>ping 192.168.10.1", which successfully pings the destination with 0% loss. The second command is "C:\>ping 192.168.20.2", which fails with 100% loss, showing "Request timed out." for all four attempts.

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: bytes=32 time=20ms TTL=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
Reply from 192.168.10.1: bytes=32 time=14ms TTL=255

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 20ms, Average = 8ms

C:\>ping 192.168.20.2

Pinging 192.168.20.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.20.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
C:\>ping 192.168.10.3

Pinging 192.168.10.3 with 32 bytes of data:

Reply from 192.168.10.3: bytes=32 time=26ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time=13ms TTL=128
Reply from 192.168.10.3: bytes=32 time=10ms TTL=128

Ping statistics for 192.168.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 26ms, Average = 12ms

C:\>ping 192.168.20.3

Pinging 192.168.20.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.20.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.1.12

Pinging 192.168.1.12 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

## **Вопросы на закрепление**

В чём заключаются преимущества маршрутизации между VLAN с использованием транкового канала или конфигурации ROS?

Позволяет создать в пределах одной физической сети виртуальные сети, в которые будет ограничен доступ, повысив таким образом защиту от несанкционированного доступа и позволив эффективно использовать пропускную способность сети.