Лабораторная работа № 5

Тема: Настройка маршрутизации между VLAN (Inter-VLAN Routing) в Cisco Packet Tracer с использованием режима Simulation

1. Цель работы

Изучить принципы маршрутизации между виртуальными локальными сетями (Inter-VLAN Routing). Получить практические навыки настройки маршрутизатора для обмена данными между различными VLAN.

Научиться:

- создавать несколько VLAN на коммутаторе;
- назначать IP-адреса конечным устройствам;
- настраивать транковое соединение между коммутатором и маршрутизатором;
- настраивать маршрутизацию с помощью технологии Router-on-a-Stick;
- проверять связь между устройствами из разных VLAN;
- исследовать процесс передачи пакетов с помощью режима Simulation;
- анализировать заголовки Ethernet и IP-пакетов.

2. Теоретические сведения

2.1. Что такое Inter-VLAN Routing?

VLAN позволяет разделить одну физическую локальную сеть на несколько логических сетей.
Например, в организации могут быть созданы три виртуальные сети:

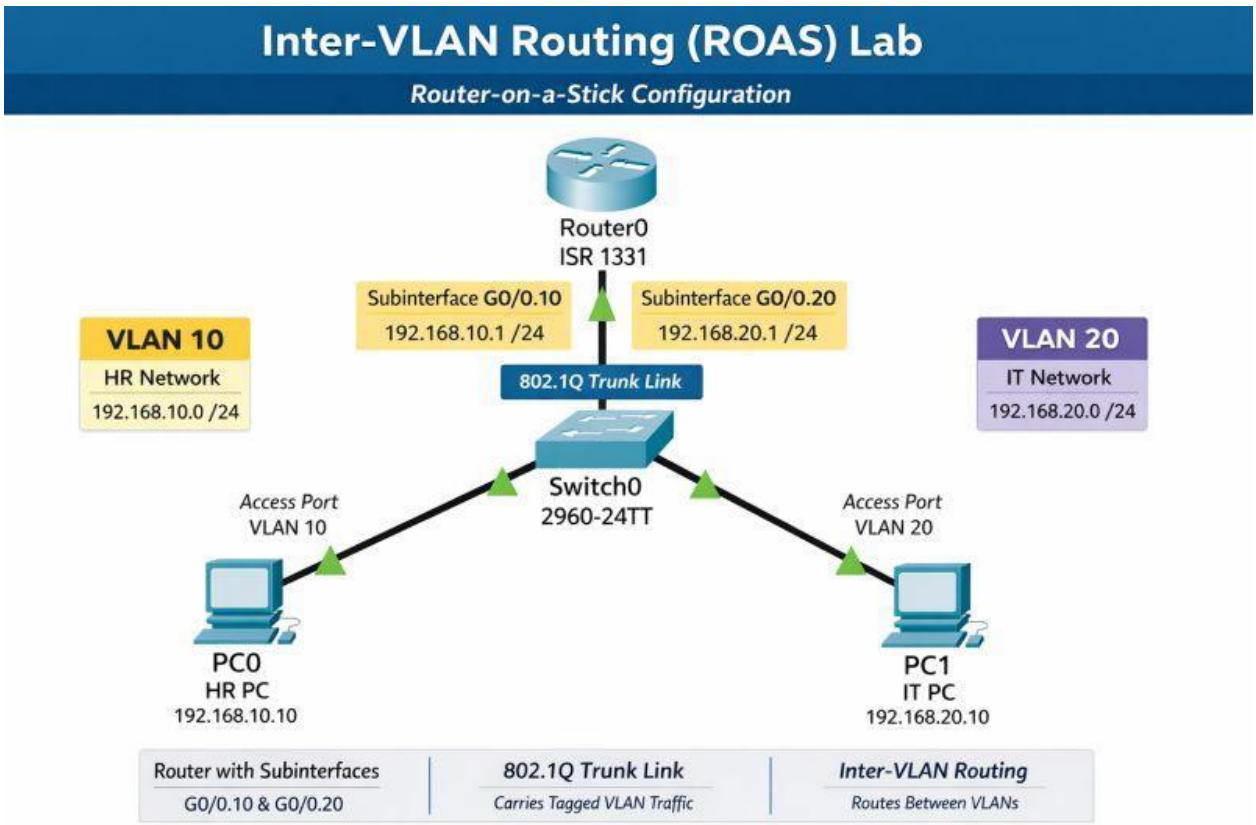
- **VLAN 10** – отдел администрации;
- **VLAN 20** – отдел преподавателей;
- **VLAN 30** – отдел студентов.

Каждая VLAN образует отдельную широковещательную область. Поэтому устройства из разных VLAN не могут обмениваться данными напрямую через обычный коммутатор второго уровня.
Для организации обмена данными между VLAN используется маршрутизатор или коммутатор третьего уровня.
Inter-VLAN Routing – это процесс передачи IP-пакетов между устройствами, которые находятся в разных виртуальных локальных сетях.

2.2. Принцип работы Router-on-a-Stick

В данной лабораторной работе используется технология **Router-on-a-Stick**.
Её принцип заключается в следующем:

1. Маршрутизатор подключается к коммутатору через один физический интерфейс.
2. На маршрутизаторе создаются логические подынтерфейсы.
3. Каждому подынтерфейсу назначается отдельный IP-адрес.
4. Для каждого подынтерфейса указывается соответствующий VLAN с помощью IEEE 802.1Q.
5. Физический порт коммутатора, который соединён с маршрутизатором, настраивается в режиме Trunk.



Например:

Подынтерфейс маршрутизатора	VLAN	IP-адрес
G0/0.10	10	192.168.10.1
G0/0.20	20	192.168.20.1
G0/0.30	30	192.168.30.1

IP-адрес каждого подынтерфейса выступает в качестве основного шлюза для соответствующей VLAN.

2.3. Как происходит передача данных между VLAN?

Рассмотрим пример:

Компьютер PC0 из VLAN 10 отправляет пакет компьютеру PC1 из VLAN 20.

1. PC0 определяет, что адрес получателя находится в другой подсети.
2. PC0 передаёт пакет на MAC-адрес своего основного шлюза.
3. Коммутатор получает Ethernet-кадр и определяет принадлежность PC0 к VLAN 10.
4. Кадр передаётся через транковое соединение к маршрутизатору с тегом VLAN 10.
5. Маршрутизатор принимает кадр через подынтерфейс G0/0.10.
6. Маршрутизатор анализирует IP-адрес назначения и определяет, что сеть получателя относится к VLAN 20.
7. Пакет передаётся через подынтерфейс G0/0.20.
8. Маршрутизатор формирует новый Ethernet-кадр с тегом VLAN 20.
9. Коммутатор передаёт кадр компьютеру PC1.

Важно: IP-адреса отправителя и получателя сохраняются, но MAC-адреса в Ethernet-заголовке изменяются при маршрутизации.

3. Оборудование и программное обеспечение

Для выполнения лабораторной работы потребуются:

- Cisco Packet Tracer;
- маршрутизатор Cisco 1941;
- коммутатор Cisco 2960;
- три компьютера PC0, PC1, PC2;
- кабели Copper Straight-Through.

4. Построение топологии сети

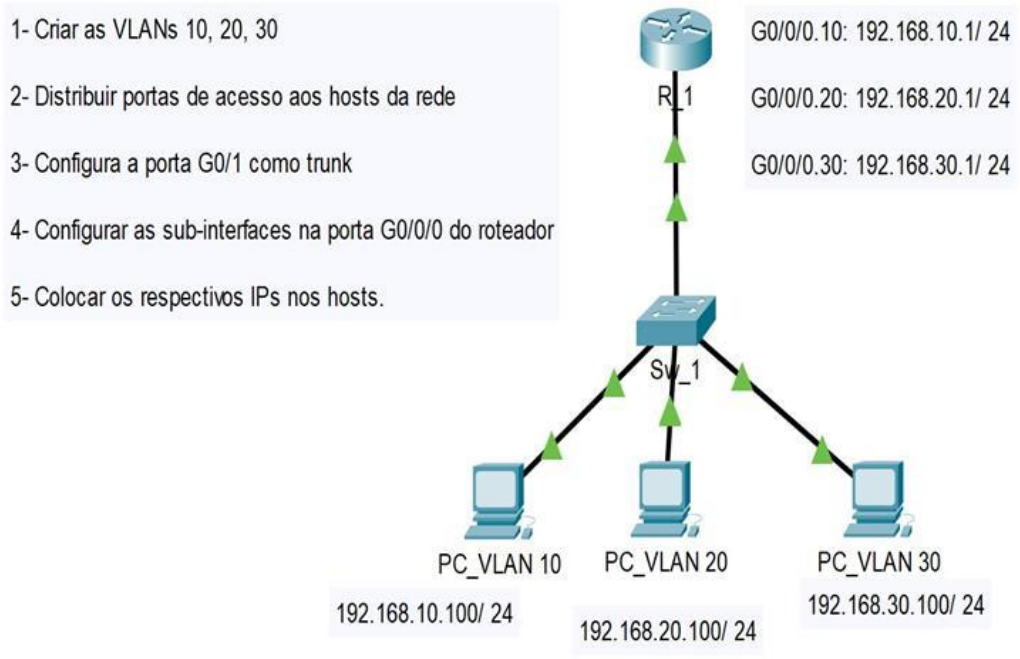
4.1. Создание сети

Разместить на рабочем поле Cisco Packet Tracer:

- один маршрутизатор Router0;
- один коммутатор Switch0;
- три компьютера PC0, PC1, PC2.

Подключить устройства следующим образом:

Устройство 1	Порт	Устройство 2	Порт
PC0	FastEthernet0	Switch0	Fa0/1
PC1	FastEthernet0	Switch0	Fa0/2
PC2	FastEthernet0	Switch0	Fa0/3
Switch0	Gi0/1	Router0	Gi0/0



4.2. План IP-адресации

Для каждой VLAN необходимо выделить отдельную IP-подсеть.

Устройство	VLAN	IP-адрес	Маска	Шлюз
PC0	10	192.168.10.2	255.255.255.0	192.168.10.1
PC1	20	192.168.20.2	255.255.255.0	192.168.20.1
PC2	30	192.168.30.2	255.255.255.0	192.168.30.1

Адреса маршрутизатора:

Подынтерфейс	VLAN	IP-адрес
G0/0.10	10	192.168.10.1
G0/0.20	20	192.168.20.1
G0/0.30	30	192.168.30.1

4.3. Настройка IP-адресов компьютеров

Для каждого компьютера открыть:

`Desktop → IP Configuration`

На PC0 указать:

- IP Address: `192.168.10.2`
- Subnet Mask: `255.255.255.0`
- Default Gateway: `192.168.10.1`

На PC1 указать:

- IP Address: `192.168.20.2`
- Subnet Mask: `255.255.255.0`
- Default Gateway: `192.168.20.1`

На PC2 указать:

- IP Address: `192.168.30.2`
- Subnet Mask: `255.255.255.0`
- Default Gateway: `192.168.30.1`

5. Настройка коммутатора Switch0

5.1. Создание виртуальных локальных сетей

Открыть CLI коммутатора и выполнить команды:

```
enable
configure terminal

vlan 10
name ADMINISTRATION
exit

vlan 20
name TEACHERS
exit

vlan 30
name STUDENTS
exit
```

Таким образом, на коммутаторе созданы три VLAN.

5.2. Назначение портов VLAN

Порт Fa0/1 назначить VLAN 10:

```
interface fa0/1
switchport mode access
switchport access vlan 10
exit
```

Порт Fa0/2 назначить VLAN 20:

```
interface fa0/2
switchport mode access
switchport access vlan 20
exit
```

Порт Fa0/3 назначить VLAN 30:

```
interface fa0/3
switchport mode access
switchport access vlan 30
exit
```

5.3. Настройка транкового соединения

Порт Gi0/1 используется для подключения маршрутизатора.

Выполнить:

```
interface gigabitEthernet 0/1
switchport mode trunk
switchport trunk allowed vlan 10,20,30
exit
```

Сохранить конфигурацию:

```
end
write memory
```

Проверить созданные VLAN:

```
show vlan brief
```

Проверить транковое соединение:

```
show interfaces trunk
```

Ожидаемый результат: порт Gi0/1 должен работать в режиме Trunk, а список разрешённых VLAN должен содержать номера 10, 20 и 30.

6. Настройка маршрутизатора Router0

Это основной этап лабораторной работы.

6.1. Включение физического интерфейса

Открыть CLI маршрутизатора.
Выполнить:

```
enable
configure terminal

interface gigabitEthernet 0/0
no shutdown
exit
```

Команда `no shutdown` активирует физический интерфейс маршрутизатора.

На физический интерфейс IP-адрес не назначается. IP-адреса будут назначены логическим подынтерфейсам.

6.2. Создание подынтерфейса для VLAN 10

```
interface gigabitEthernet 0/0.10
encapsulation dot1Q 10
ip address 192.168.10.1 255.255.255.0
exit
```

Объяснение команд:

- `interface gigabitEthernet 0/0.10` – создание подынтерфейса;
- `encapsulation dot1Q 10` – указание стандарта IEEE 802.1Q и номера VLAN 10;
- `ip address` – назначение IP-адреса шлюза.

6.3. Создание подынтерфейса для VLAN 20

```
interface gigabitEthernet 0/0.20
encapsulation dot1Q 20
ip address 192.168.20.1 255.255.255.0
exit
```

6.4. Создание подынтерфейса для VLAN 30

```
interface gigabitEthernet 0/0.30
encapsulation dot1Q 30
ip address 192.168.30.1 255.255.255.0
exit
```

Завершить настройку:

```
end
write memory
```

6.5. Проверка настройки маршрутизатора

Выполнить команду:

```
show ip interface brief
```

В таблице должны отображаться следующие интерфейсы:

Интерфейс	IP-адрес	Состояние
G0/0	unassigned	up/up
G0/0.10	192.168.10.1	up/up
G0/0.20	192.168.20.1	up/up
G0/0.30	192.168.30.1	up/up

Физический интерфейс и подынтерфейсы должны находиться в активном состоянии.

Дополнительно выполнить:

```
show ip route
```

В таблице маршрутизации должны появиться три непосредственно подключённые сети:

- 192.168.10.0/24;
- 192.168.20.0/24;
- 192.168.30.0/24.

Маршрутизатор автоматически добавляет эти сети в таблицу маршрутизации после назначения IP-адресов подынтерфейсам и активации интерфейса.

7. Проверка маршрутизации между VLAN

7.1. Проверка доступности шлюза

На PC0 открыть:

```
Desktop → Command Prompt
```

Выполнить:

```
ping 192.168.10.1
```

На PC1:

```
ping 192.168.20.1
```

На PC2:

```
ping 192.168.30.1
```

Все компьютеры должны получить ответы от своих шлюзов.

7.2. Проверка передачи данных между разными VLAN

Теперь необходимо проверить обмен данными между компьютерами, которые находятся в разных VLAN.

На PC0 выполнить:

```
ping 192.168.20.2
```

Здесь PC0 из VLAN 10 отправляет запрос PC1 из VLAN 20.

На PC0 также выполнить:

```
ping 192.168.30.2
```

Здесь проверяется связь между VLAN 10 и VLAN 30.

На PC1 выполнить:

```
ping 192.168.30.2
```

Проверяется связь между VLAN 20 и VLAN 30.

Ожидаемый результат: все три проверки должны завершиться успешно.

Если первый запрос завершается неудачно, повторить команду `ping`. Это может быть связано с первоначальным обменом ARP-запросами для определения MAC-адресов.

8. Исследование передачи пакетов в режиме Simulation

Основная практическая часть

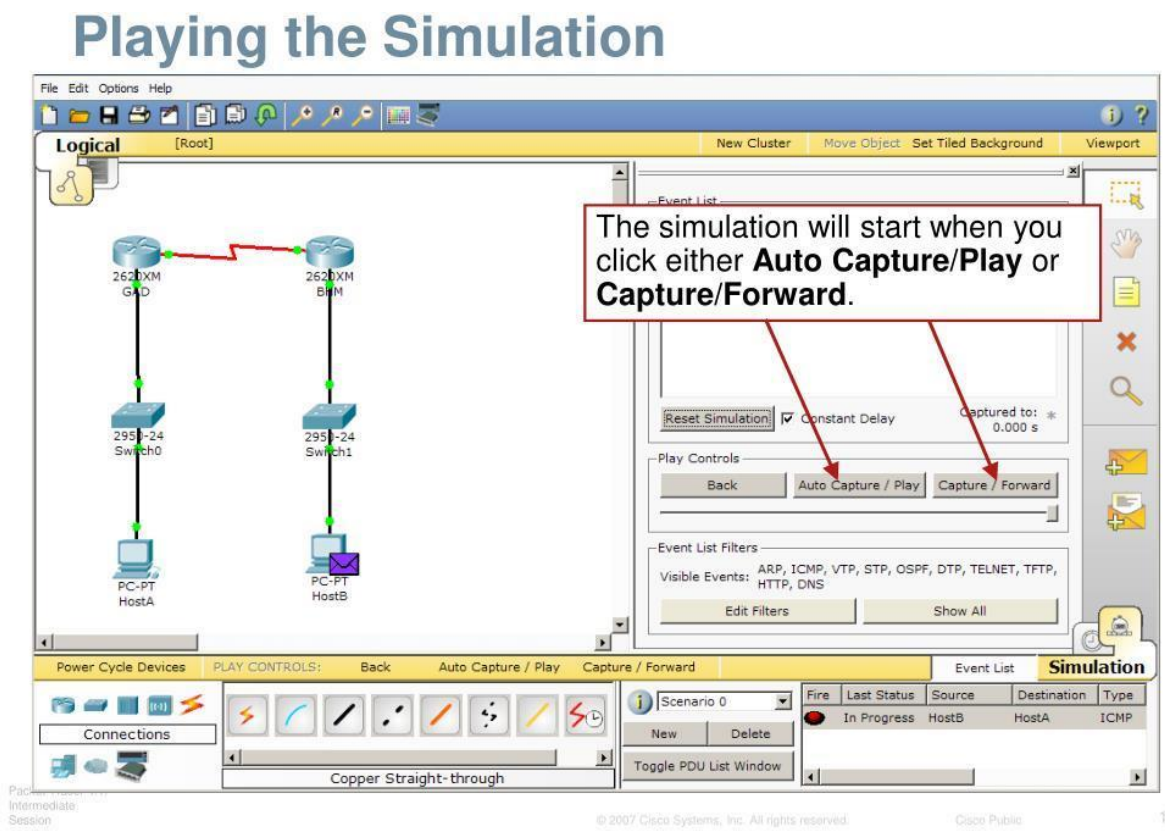
В этом разделе необходимо не просто проверить связь между компьютерами, а проследить весь путь IP-пакета от отправителя до получателя.

8.1. Переход в режим Simulation

В нижней правой части окна Cisco Packet Tracer находятся два режима:

- Realtime;
- Simulation.

Выбрать режим Simulation.



После перехода в режим Simulation появится панель управления передачей пакетов.

Основные элементы:

Элемент	Назначение
Auto Capture / Play	Автоматическое воспроизведение событий
Capture / Forward	Переход к следующему событию
Reset Simulation	Сброс событий
Event List	Список событий передачи пакетов
Edit Filters	Настройка отображаемых типов пакетов

8.2. Настройка фильтров Simulation

Нажать кнопку `Edit Filters`.
В списке протоколов оставить:

- ARP;
- ICMP.

Если доступны дополнительные фильтры Ethernet или 802.1Q, их также можно включить.

Нажать кнопку закрытия окна фильтров.

Почему нужны ARP и ICMP?

- ARP используется для определения MAC-адреса следующего узла.
- ICMP используется для передачи запросов и ответов команды `ping`.

Именно эти два протокола позволят проследить процесс передачи данных между разными VLAN.

8.3. Создание тестового пакета

Для исследования используем PC0 и PC1.

Исходные данные:

Параметр	Значение
Отправитель	PC0
VLAN отправителя	10
IP отправителя	192.168.10.2
Получатель	PC1
VLAN получателя	20
IP получателя	192.168.20.2
Шлюз PC0	192.168.10.1

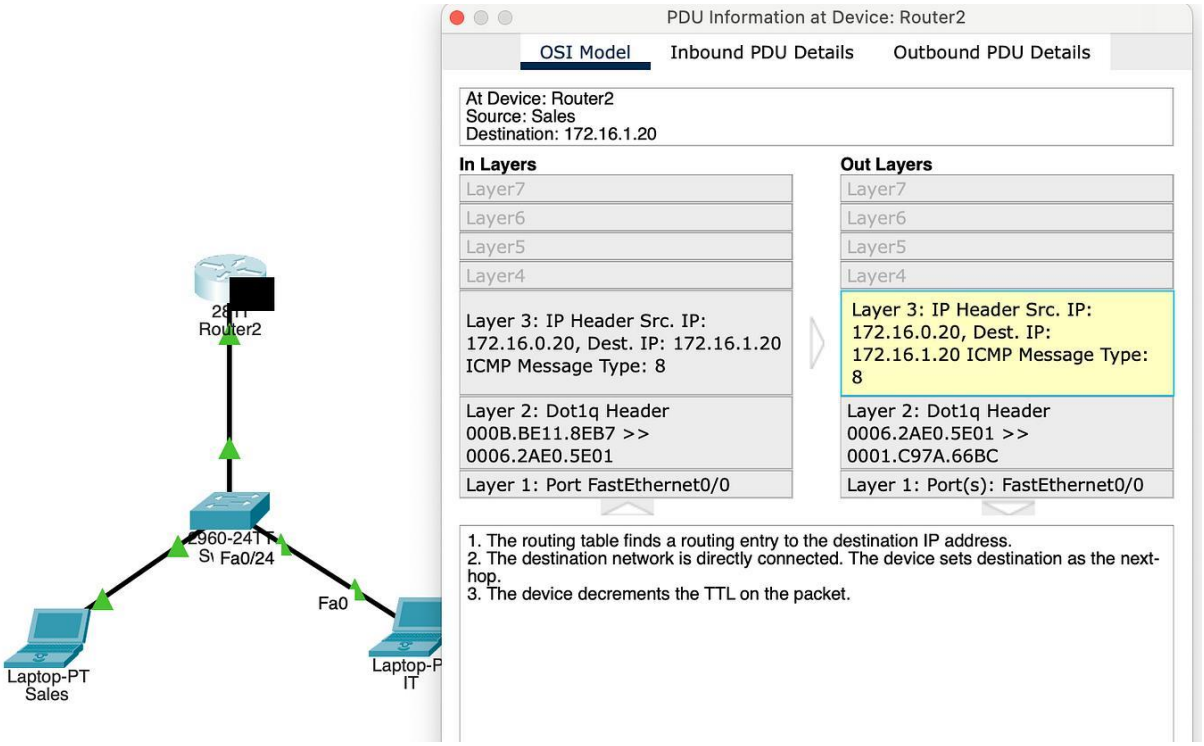
В режиме Simulation выполнить:

1. Нажать PC0.
2. Открыть вкладку Desktop.
3. Выбрать Command Prompt.
4. Выполнить команду:

```
ping 192.168.20.2
```

5. Вернуться к окну Simulation.
6. Нажать Capture / Forward.

На рабочем поле появятся анимированные конверты, которые показывают передачу сетевых сообщений.



8.4. Анализ первого этапа: ARP-запрос

PC0 должен передать пакет за пределы своей локальной сети.

Для этого он использует основной шлюз `192.168.10.1`.

Но для отправки Ethernet-кадра ему необходим MAC-адрес маршрутизатора.

Поэтому PC0 отправляет ARP-запрос.

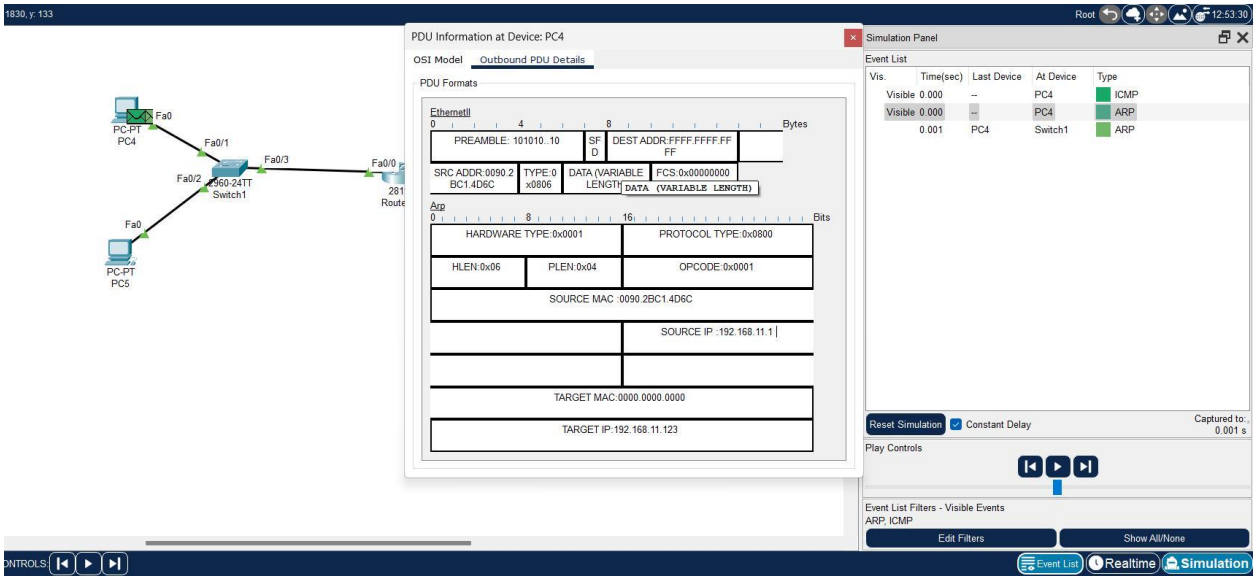
В режиме Simulation:

1. Нажать Capture / Forward.
2. Проследить передачу ARP-пакета от PC0 к Switch0.
3. Нажать на конверт с ARP.
4. Открыть окно PDU Information.
5. Перейти во вкладку Inbound PDU Details или Outbound PDU Details.

Изучить следующие поля:

- Sender IP Address;
- Sender MAC Address;
- Target IP Address;
- Target MAC Address.

PC0 отправляет широковещательный ARP-запрос, чтобы узнать MAC-адрес шлюза `192.168.10.1`.



8.5. Анализ второго этапа: передача кадра к маршрутизатору

После получения ARP-ответа PC0 знает MAC-адрес шлюза.

Теперь компьютер формирует ICMP Echo Request.

В режиме Simulation нажимать Capture / Forward до появления ICMP-пакета.

Проследить путь:

`PC0 → Switch0 → Router0`

На этом этапе необходимо установить:

1. Через какой порт коммутатора передаётся кадр?
2. К какой VLAN относится исходный кадр?
3. Почему кадр передаётся на маршрутизатор?
4. Какую роль выполняет транковое соединение?

При передаче через транковый порт кадр получает тег IEEE 802.1Q с номером VLAN 10.

8.6. Анализ третьего этапа: обработка пакета маршрутизатором

После поступления кадра маршрутизатор определяет VLAN по тегу 802.1Q.

Кадр поступает на подынтерфейс:

```
G0/0.10
```

Маршрутизатор анализирует IP-адрес назначения:

```
192.168.20.2
```

Далее по таблице маршрутизации определяется сеть:

```
192.168.20.0/24
```

Для передачи пакета используется подынтерфейс:

```
G0/0.20
```

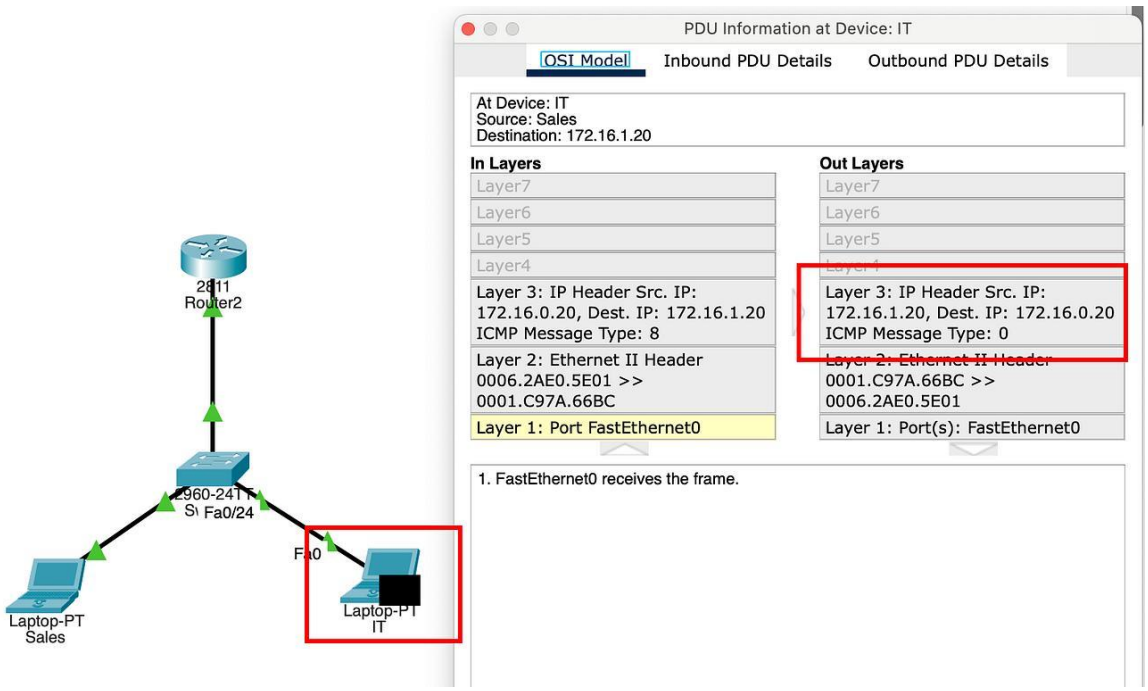
На этом этапе необходимо открыть PDU Information и изучить заголовки пакета.

Обратить внимание:

Поле	До маршрутизации	После маршрутизации
Source IP	192.168.10.2	192.168.10.2
Destination IP	192.168.20.2	192.168.20.2
Source MAC	MAC PC0	MAC Router0
Destination MAC	MAC шлюза	MAC PC1
VLAN	10	20

MAC-адреса изменяются, поскольку маршрутизатор формирует новый Ethernet-кадр для другой сети.

IP-адреса отправителя и получателя при обычной маршрутизации сохраняются. Также уменьшается TTL IP-пакета.



8.7. Анализ четвёртого этапа: передача пакета в VLAN 20

После обработки IP-пакета маршрутизатор передаёт его через подынтерфейс G0/0.20.

Далее пакет поступает к коммутатору.

Путь передачи:

```
Router0 → Switch0 → PC1
```

Коммутатор определяет VLAN 20 и передаёт кадр через порт Fa0/2.

PC1 получает ICMP Echo Request.

В режиме Simulation необходимо:

1. Нажимать Capture / Forward.
2. Проследить движение конверта от Router0 к Switch0.
3. Проследить передачу от Switch0 к PC1.
4. Открыть PDU Information.
5. Проверить IP-адрес источника и получателя.

8.8. Анализ пятого этапа: возврат ICMP-ответа

После получения запроса PC1 формирует ICMP Echo Reply.

Ответ должен пройти обратный путь:

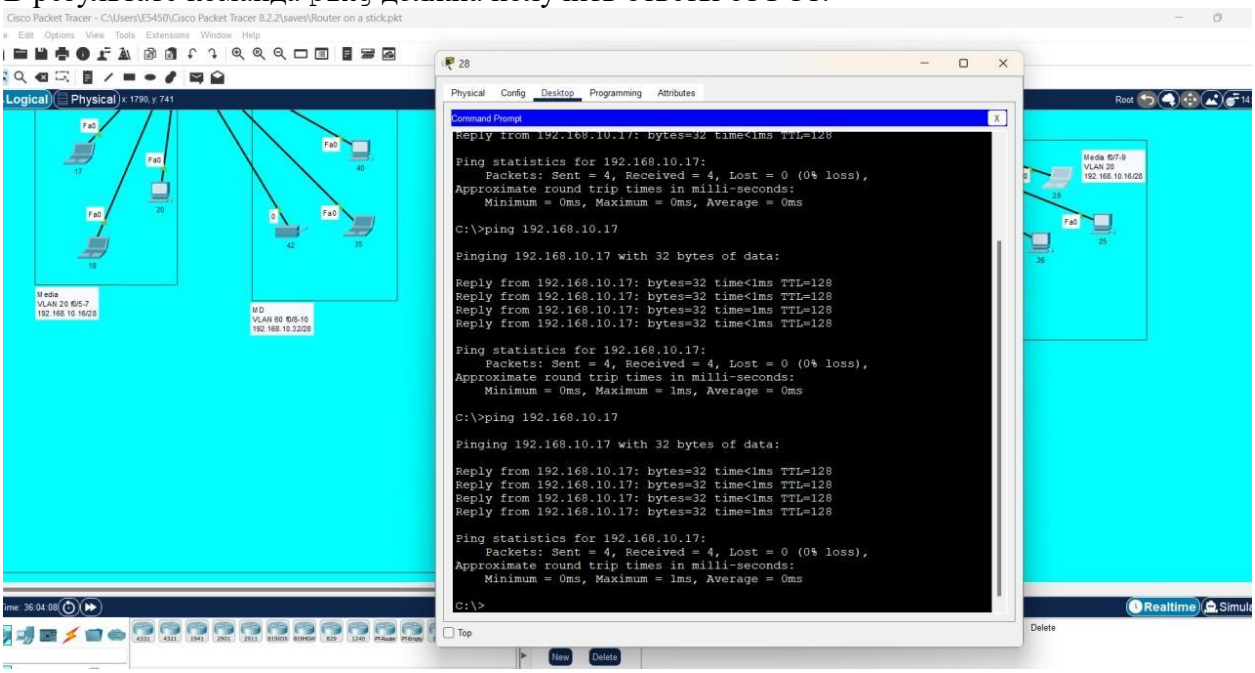
```
PC1 → Switch0 → Router0 → Switch0 → PC0
```

При этом:

- PC1 передаёт ответ через шлюз `192.168.20.1`;
- маршрутизатор принимает пакет через G0/0.20;

- определяет сеть `192.168.10.0/24`;
- передаёт пакет через G0/0.10;
- PC0 получает ICMP Echo Reply.

В результате команда `ping` должна получить ответы от PC1.



8.9. Итоговая схема прохождения пакета

Передача ICMP-пакета между VLAN 10 и VLAN 20

PC0
192.168.10.2 · VLAN 10

↓

Access · Fa0/1 · VLAN 10

Switch0
Коммутатор Cisco 2960

↓

Trunk · IEEE 802.1Q · VLAN 10, 20, 30

Router0

G0/0.10	G0/0.20
192.168.10.1	192.168.20.1
VLAN 10	**VLAN 20**

Маршрутизация IP-пакета и создание нового Ethernet-кадра

↓

Trunk · VLAN 20

Switch0
Передача кадра через Fa0/2

↓

PC1
192.168.20.2 · VLAN 20

9. Дополнительные экспериментальные задания

Задание 1. Отключение маршрутизации между VLAN

На маршрутизаторе выполнить:

```
configure terminal
interface gigabitEthernet 0/0.20
shutdown
end
```

Повторить проверку:

```
ping 192.168.20.2
```

Ответить: почему обмен данными между VLAN 10 и VLAN 20 перестал работать?

После проверки восстановить интерфейс:

```
configure terminal
interface gigabitEthernet 0/0.20
no shutdown
end
```

Задание 2. Изменение IP-адреса шлюза

На PC0 изменить Default Gateway на:

```
192.168.10.254
```

Повторить команду:

```
ping 192.168.20.2
```

Объяснить, почему передача данных не работает.

После проверки восстановить правильный адрес шлюза.

Задание 3. Исследование маршрутизации VLAN 10 и VLAN 30

Выполнить на PC0:

```
ping 192.168.30.2
```

В режиме Simulation проследить путь пакета.

Заполнить таблицу:

Этап	Устройство	Действие
1	PC0	Формирование ICMP-запроса
2	Switch0	Передача кадра VLAN 10
3	Router0	Приём через G0/0.10
4	Router0	Маршрутизация в VLAN 30
5	Switch0	Передача кадра VLAN 30
6	PC2	Получение ICMP-запроса
7	Router0	Передача ответного пакета

10. Анализ результатов Simulation

После выполнения экспериментов заполнить таблицу.

№	Исследуемый параметр	Результат
1	IP-адрес отправителя	192.168.10.2
2	IP-адрес получателя	192.168.20.2
3	VLAN отправителя	10
4	VLAN получателя	20
5	Подынтерфейс приёма	G0/0.10
6	Подынтерфейс передачи	G0/0.20
7	Протокол маршрутизации	IP
8	Протокол проверки связи	ICMP
9	Протокол определения MAC-адреса	ARP
10	Результат передачи	Успешно

11. Контрольные вопросы

1. Что такое Inter-VLAN Routing?
2. Почему устройства из разных VLAN не могут обмениваться данными без маршрутизатора?
3. Что представляет собой технология Router-on-a-Stick?
4. Для чего создаются подынтерфейсы маршрутизатора?
5. Какую функцию выполняет команда `encapsulation dot1Q`?
6. Почему физический интерфейс маршрутизатора не имеет отдельного IP-адреса в данной конфигурации?
7. Для чего используется транковое соединение между коммутатором и маршрутизатором?
8. Какую роль выполняет Default Gateway?
9. Что происходит с MAC-адресами при маршрутизации IP-пакета?
10. Почему IP-адреса отправителя и получателя сохраняются?
11. Для чего используется протокол ARP?
12. Какую информацию можно получить в режиме Simulation?
13. Чем отличаются режимы Realtime и Simulation?
14. Что произойдёт, если отключить один из подынтерфейсов маршрутизатора?
15. Можно ли организовать Inter-VLAN Routing без отдельного маршрутизатора?

12. Содержание отчёта

В отчёте должны быть представлены:

1. Титульный лист (Пример приведен в конце лабораторной работы № 4)
2. Название и цель лабораторной работы.
3. Теоретические сведения о маршрутизации между VLAN.
4. Схема построенной сети.
5. Таблица IP-адресации.
6. Команды настройки VLAN на коммутаторе.
7. Команды настройки транкового соединения.
8. Команды настройки подынтерфейсов маршрутизатора.
9. Результаты выполнения `show vlan brief`.

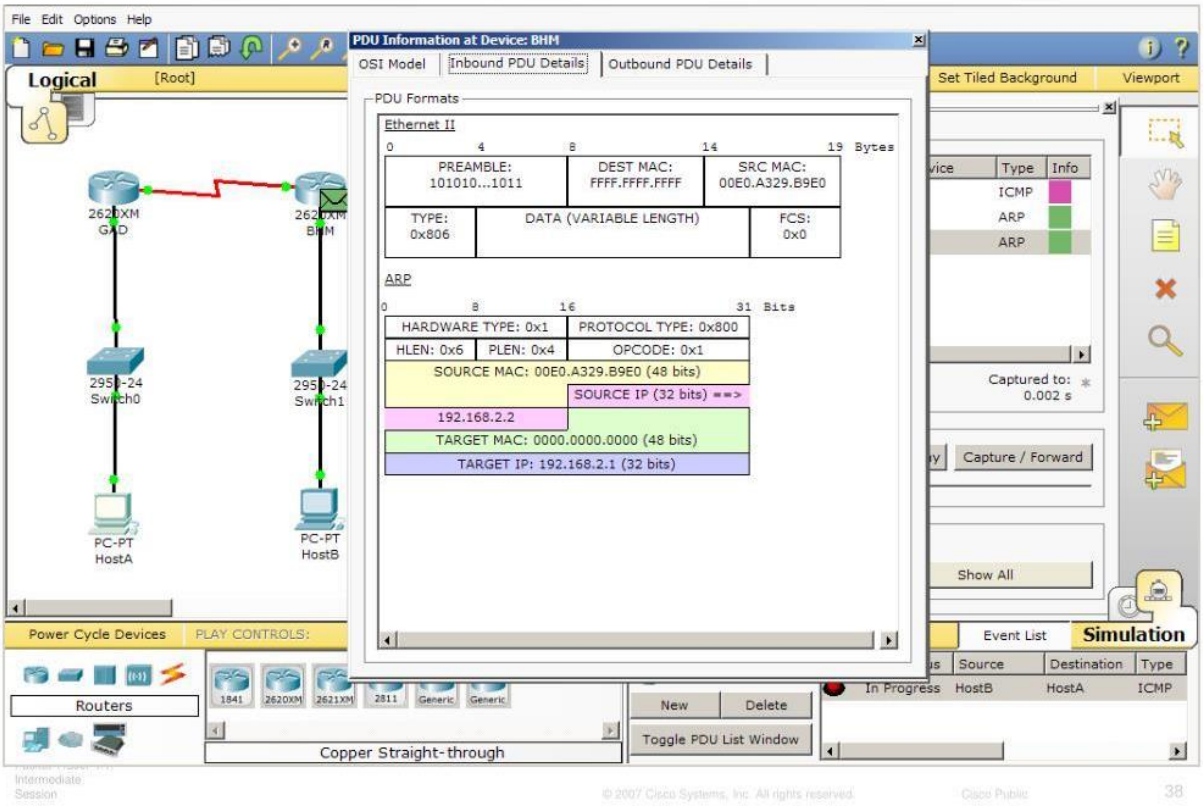
10. Результаты выполнения `show interfaces trunk`.
11. Результаты выполнения `show ip interface brief` и `show ip route`.
12. Скриншоты успешной проверки `ping`.
13. Не менее четырёх скриншотов режима Simulation с анализом прохождения пакета.
14. Заполненная таблица анализа передачи пакетов.
15. Ответы на контрольные вопросы.
16. Вывод по лабораторной работе.

13. Требования к скриншотам Simulation

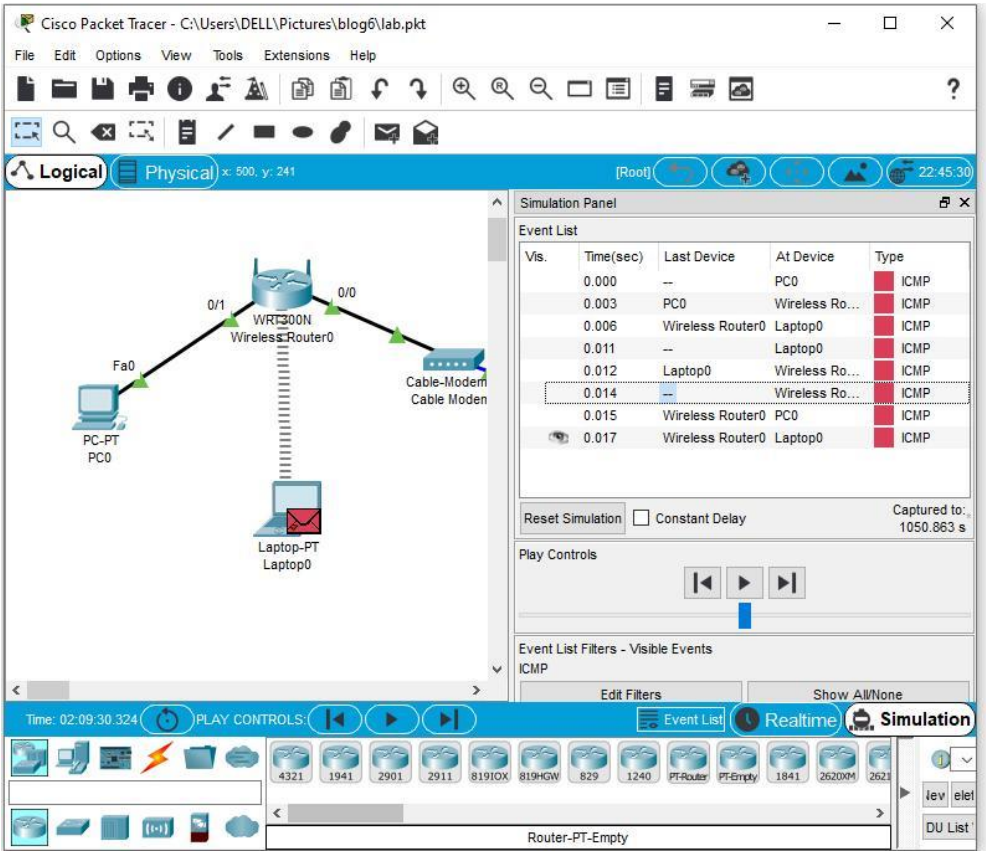
Для подтверждения выполнения лабораторной работы студент должен представить следующие снимки экрана:

Скриншот 1. ARP-запрос

Отображение ARP-запроса от PC0 к основному шлюзу.

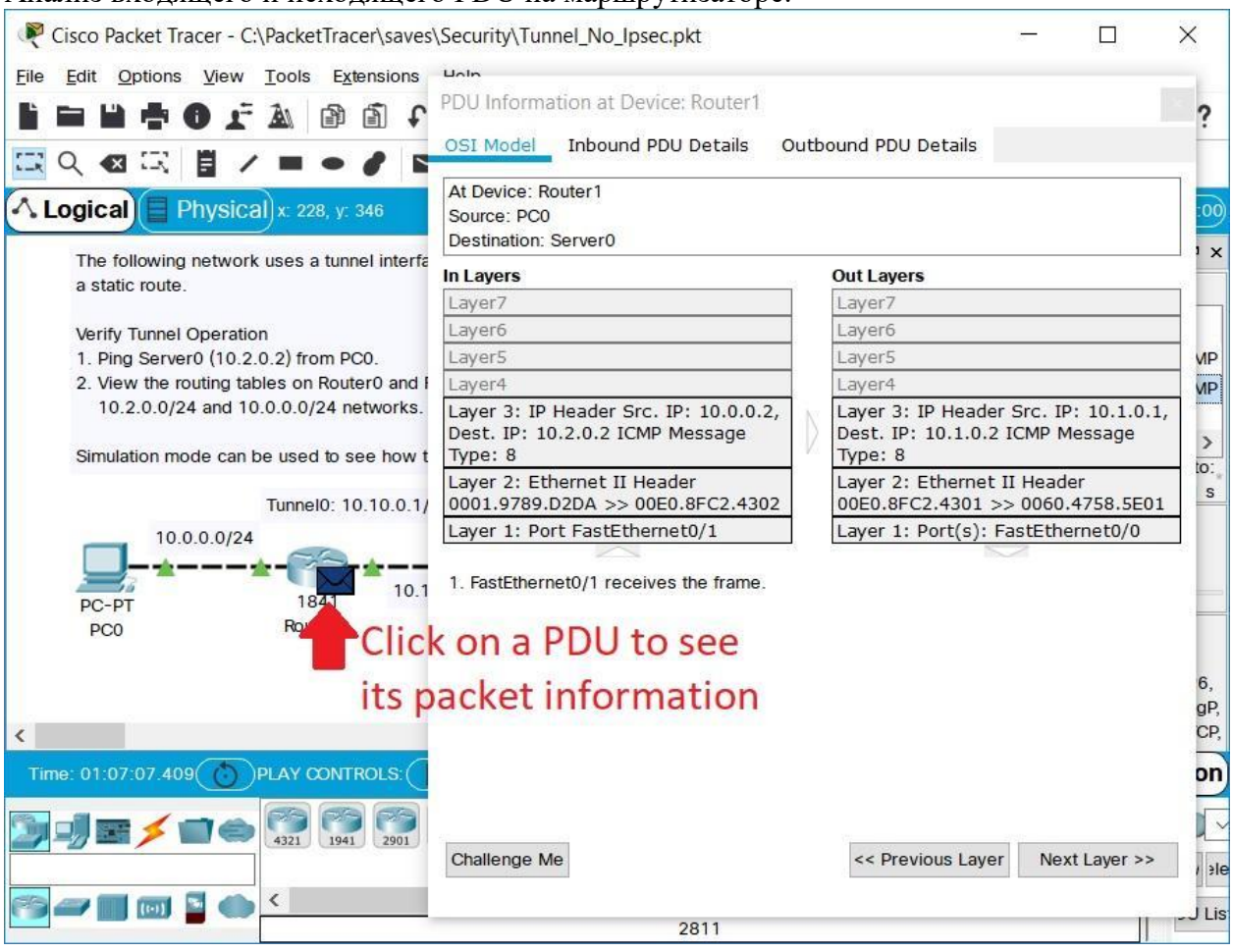


Скриншот 2. Передача пакета маршрутизатору
Отображение ICMP-пакета при передаче через транковое соединение.

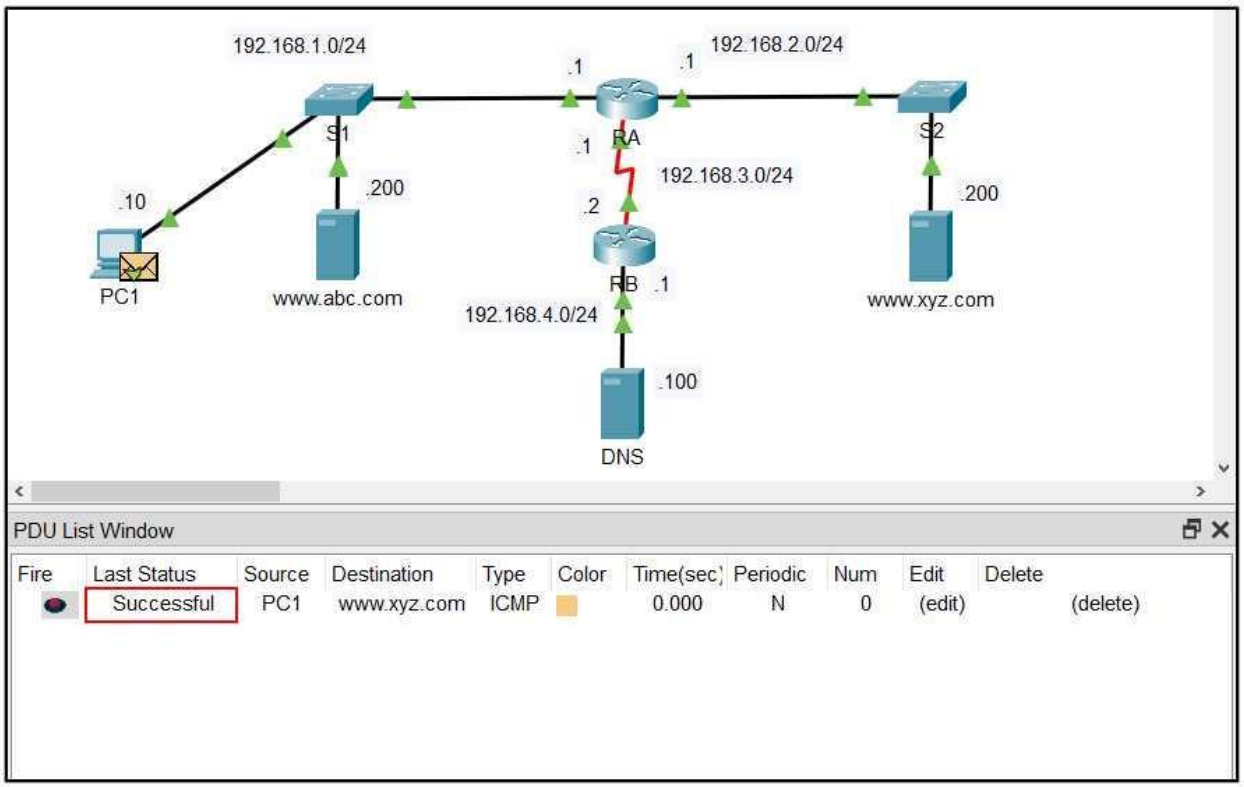


Скриншот 3. Маршрутизация пакета

Анализ входящего и исходящего PDU на маршрутизаторе.



Скриншот 4. Получение ответа
Отображение успешной доставки ICMP Echo Reply компьютеру PC0.



14. Вывод

В ходе лабораторной работы была создана локальная сеть с тремя виртуальными локальными сетями VLAN 10, VLAN 20 и VLAN 30. На коммутаторе были настроены VLAN и транковое соединение с маршрутизатором. На маршрутизаторе были созданы подынтерфейсы с использованием стандарта IEEE 802.1Q.

С помощью технологии Router-on-a-Stick была организована маршрутизация между различными VLAN. Работоспособность сети была проверена командой `ping`.

В режиме Simulation был исследован процесс передачи IP-пакетов между разными VLAN. Были изучены ARP-запросы, ICMP-сообщения, изменение MAC-адресов и работа подынтерфейсов маршрутизатора.