Лабораторная работа № 1

Знакомство с Cisco Packet Tracer

Абд эль хай Мохамад

Содержание

# 1 Цель работы

Здесь приводится формулировка цели лабораторной работы. Формулировки цели для каждой лабораторной работы приведены в методических указаниях.

Цель данного шаблона — максимально упростить подготовку отчётов по лабораторным работам. Модифицируя данный шаблон, студенты смогут без труда подготовить отчёт по лабораторным работам, а также познакомиться с основными возможностями разметки Markdown.

# 2 Задание

1. Установить на домашнем устройстве Cisco Packet Tracer.
2. Постройте простейшую сеть в Cisco Packet Tracer, проведите простейшую настройку оборудования.

# 3 Выполнение лабораторной работы

## 3.1 Построение простейшей сети

В рабочем пространстве разместил концентратор (Hub-PT) и четыре оконечных устройства PC. Соединил оконечные устройства с концентратором прямым кабелем.

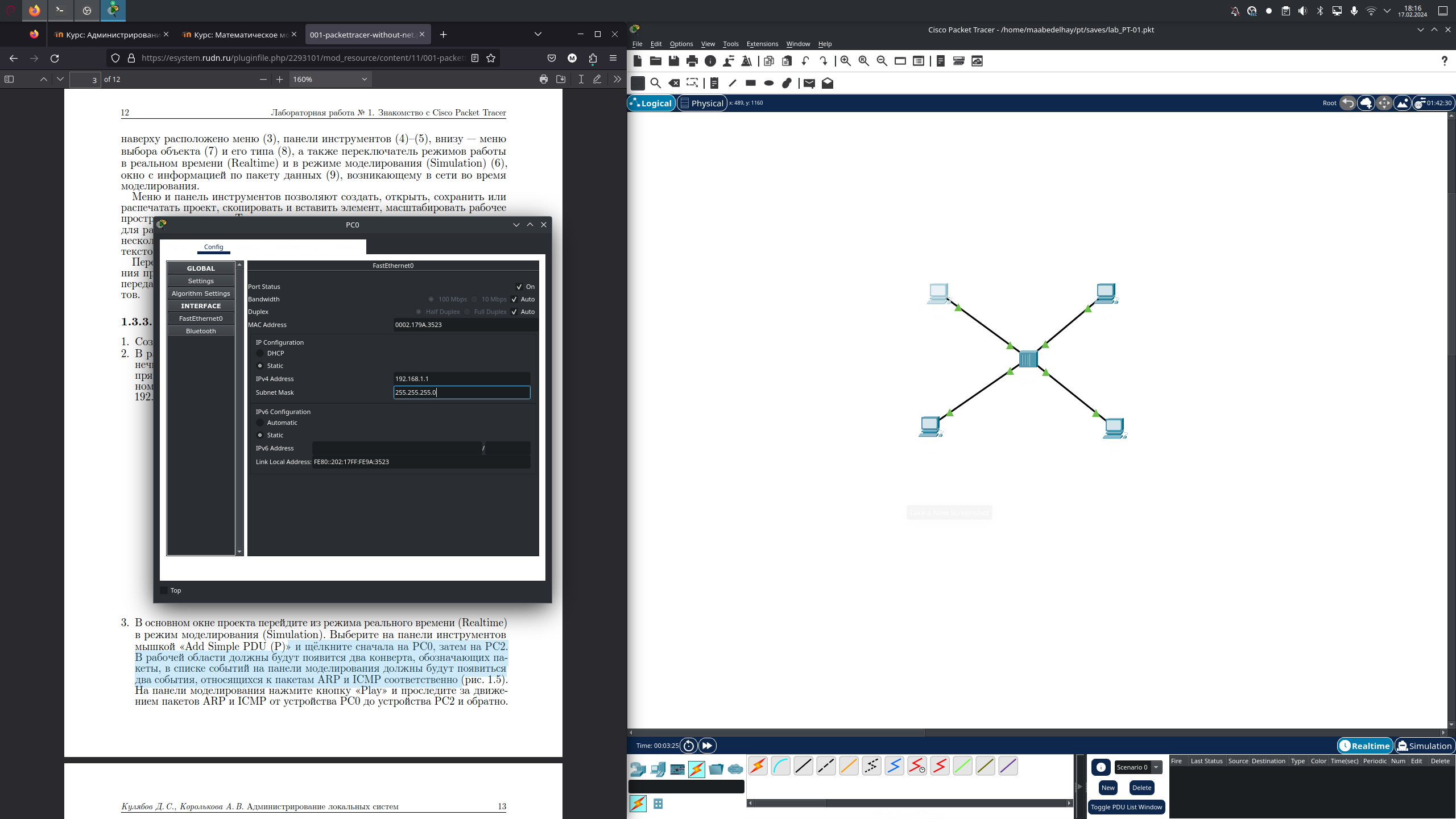


Рис. 1: Модель простой сети с концентратором

Щёлкнув последовательно на каждом оконечном устройстве, статические IP-адреса 192.168.1.11, 192.168.1.12, 192.168.1.13, 192.168.1.14 с маской подсети 255.255.255.

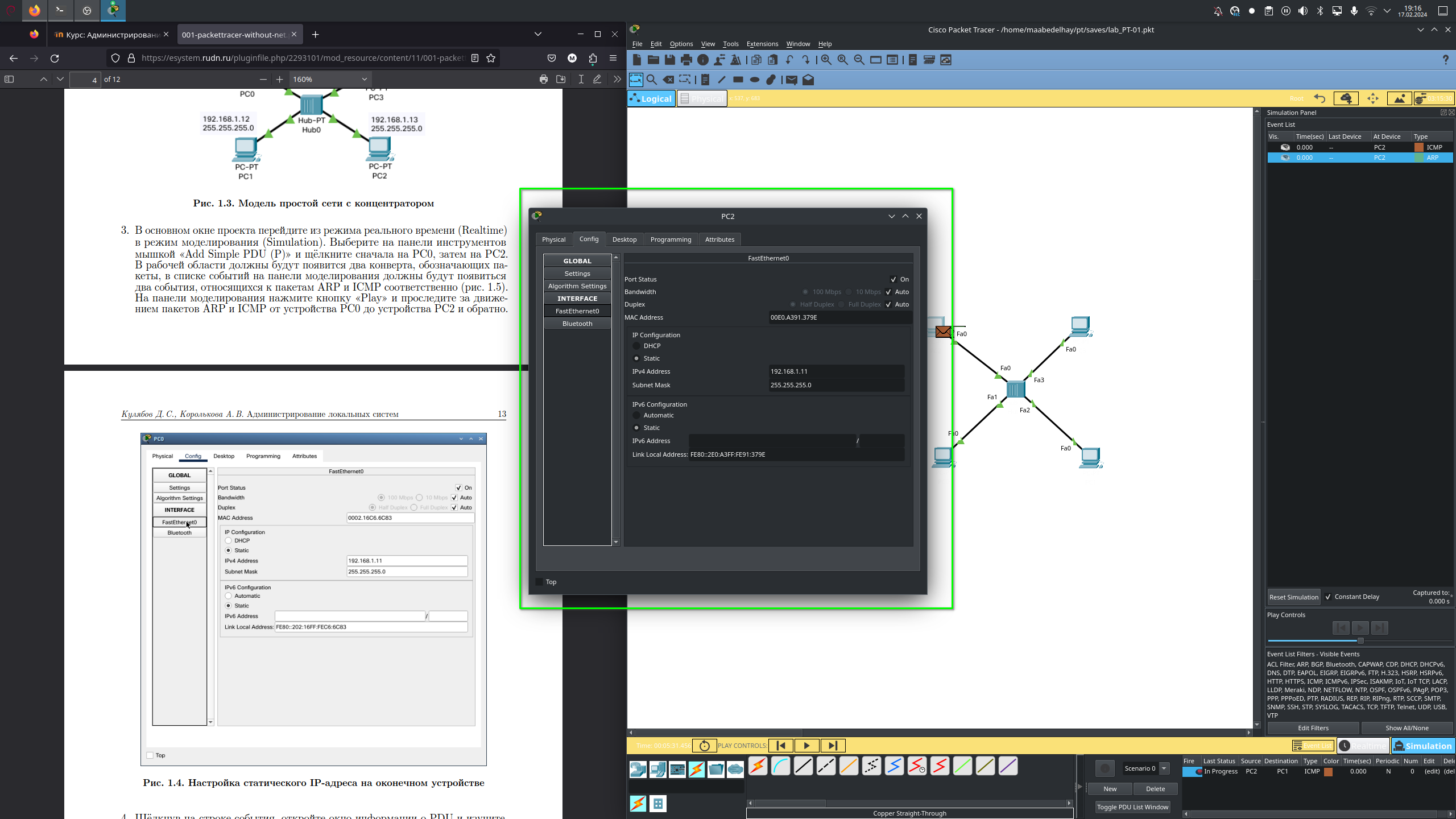


Рис. 2: Настройка статического IP-адреса

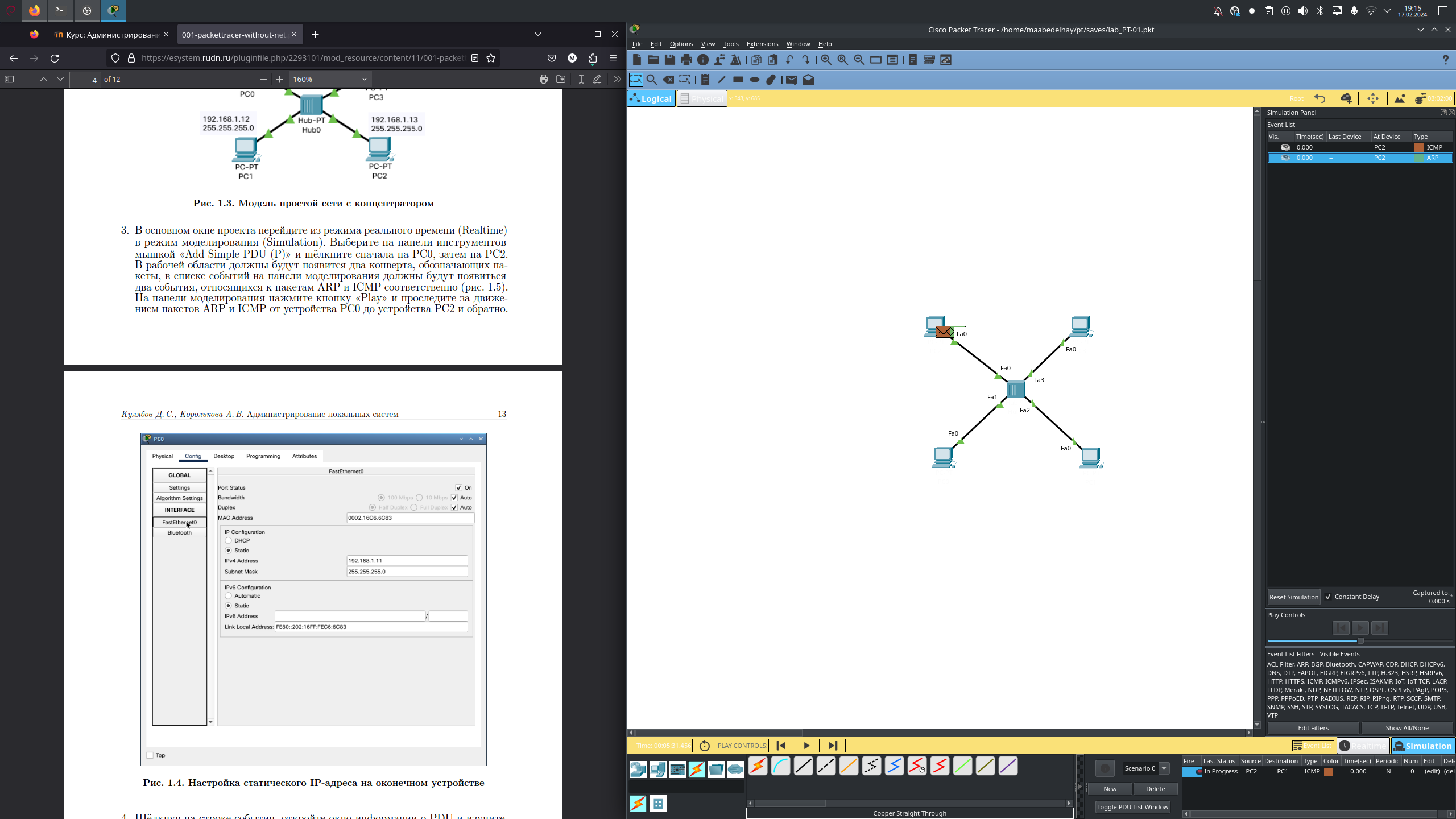


Рис. 3: События в режиме моделирования

в режим моделирования. Я выбрал «Добавить простой PDU (P)» на панели инструментов и щелкнул сначала на ПК0, затем на ПК2.

В рабочей области появились два конверта с указанием пакетов, а в списке событий на панели моделирования появилось На панели моделирования нажмите кнопку «Воспроизвести» и наблюдайте за перемещением пакетов ARP и ICMP от устройства PC0 к устройству PC2 и обратно.

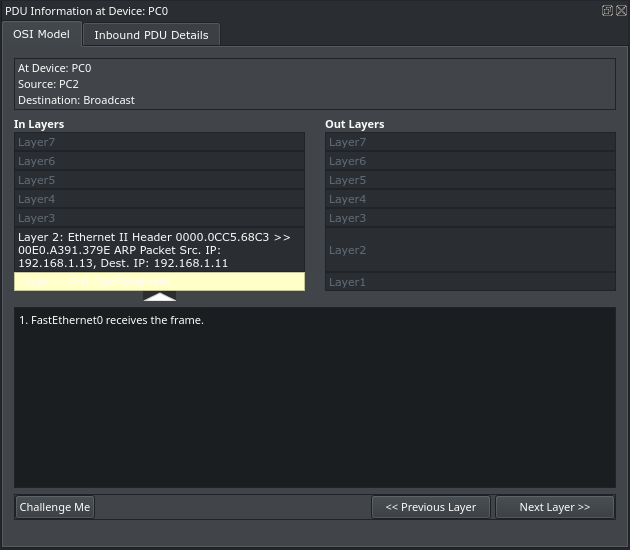


Рис. 4: Информация о PDU

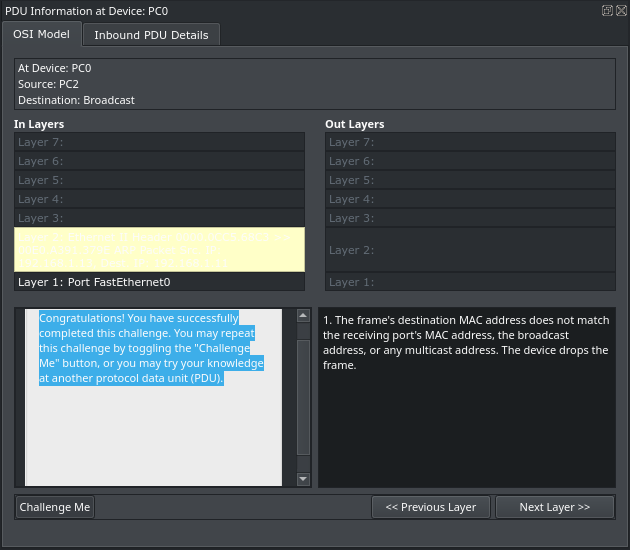


Рис. 5: Challenge Me

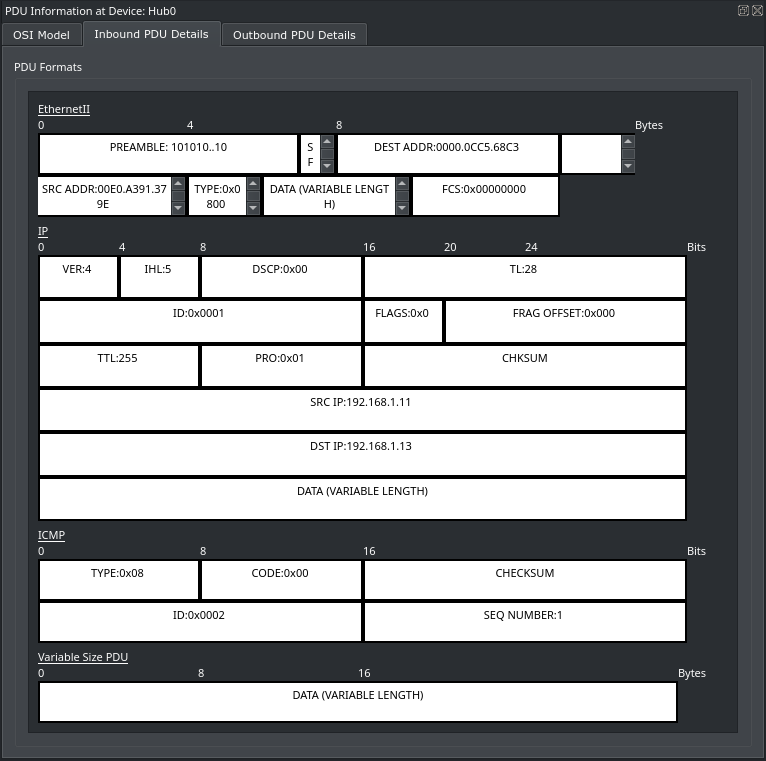


Рис. 6: Структуру пакета ICMP

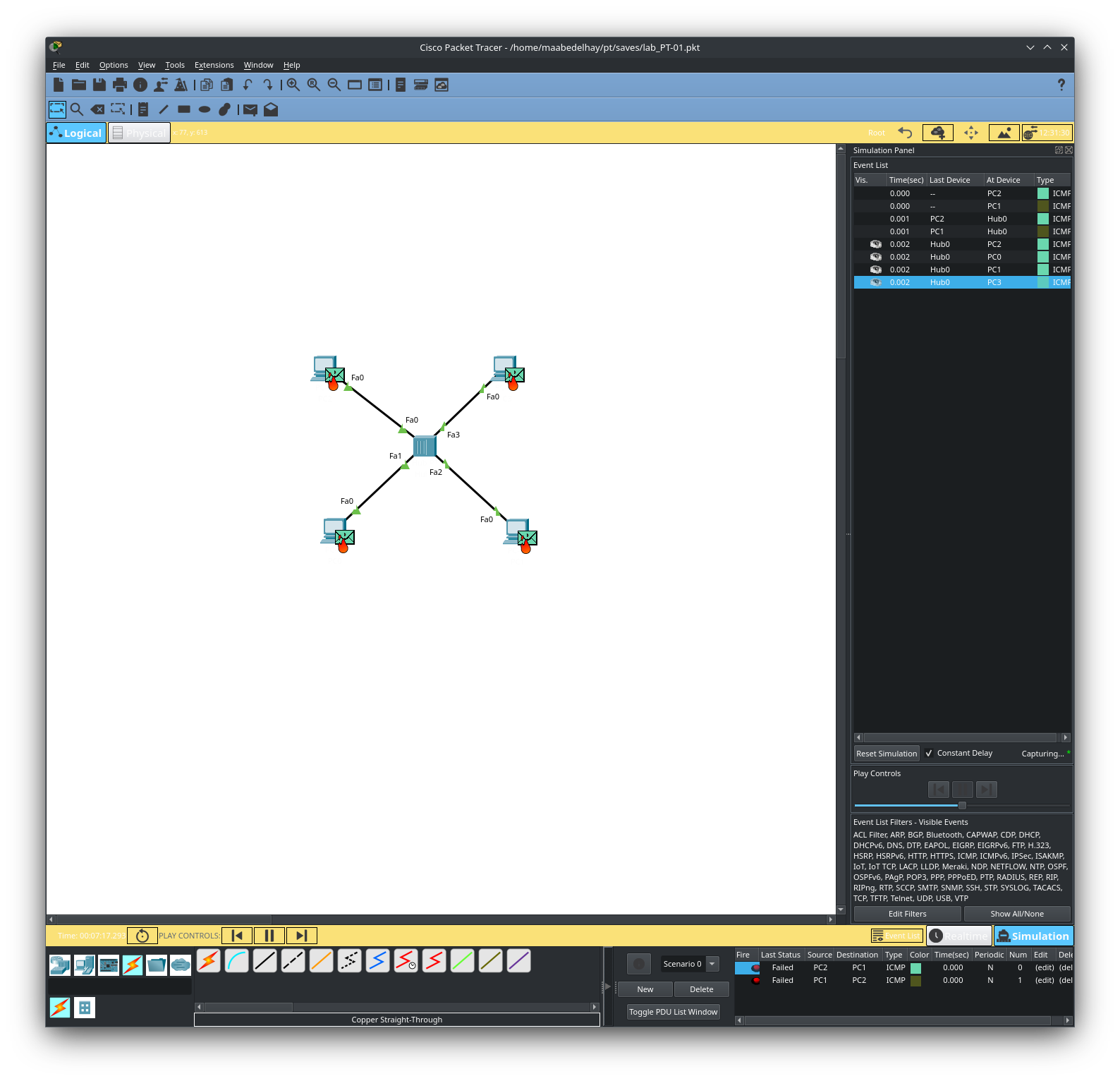


Рис. 7: Коллизии

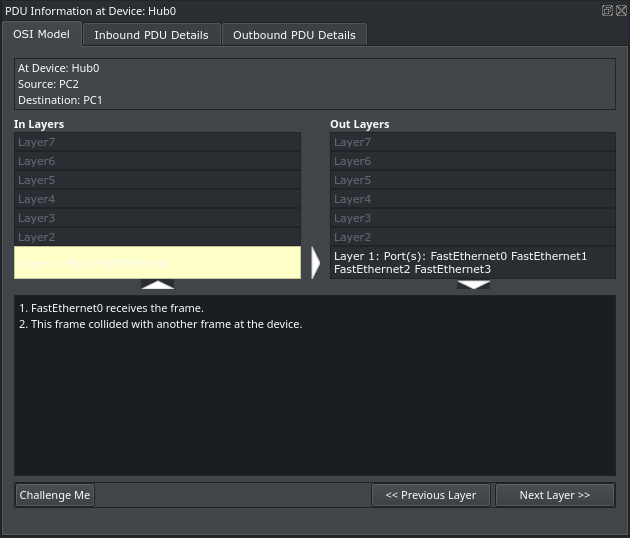


Рис. 8: Название рисунка

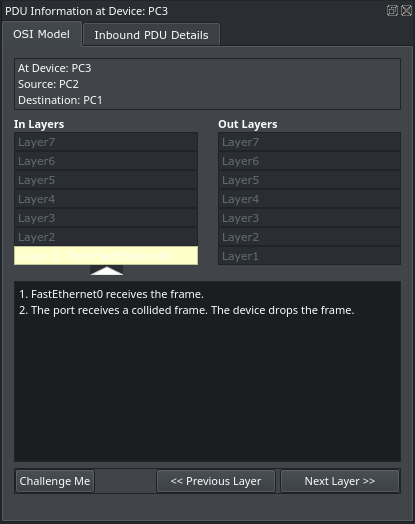


Рис. 9: Название рисунка

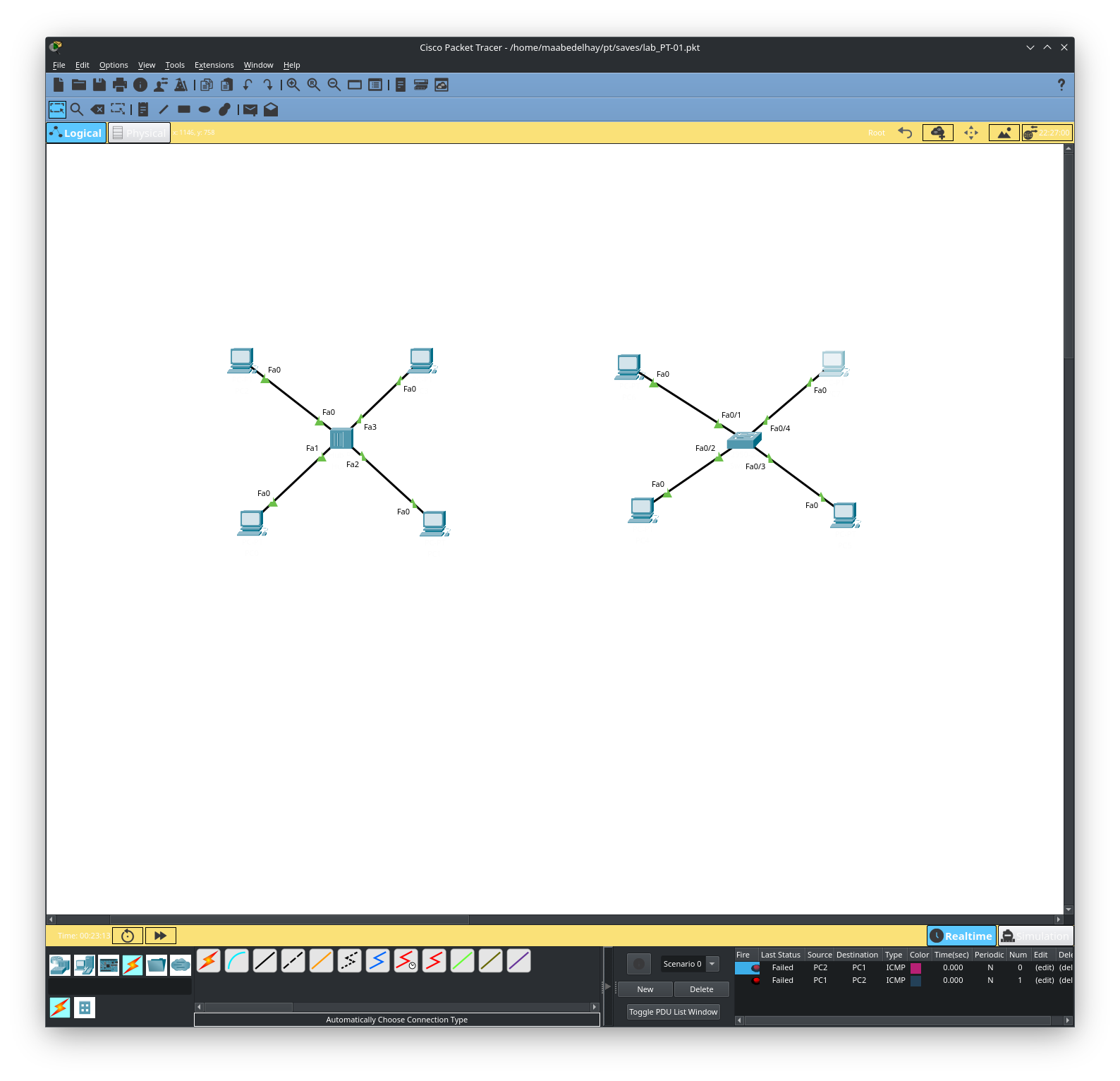


Рис. 10: Название рисунка

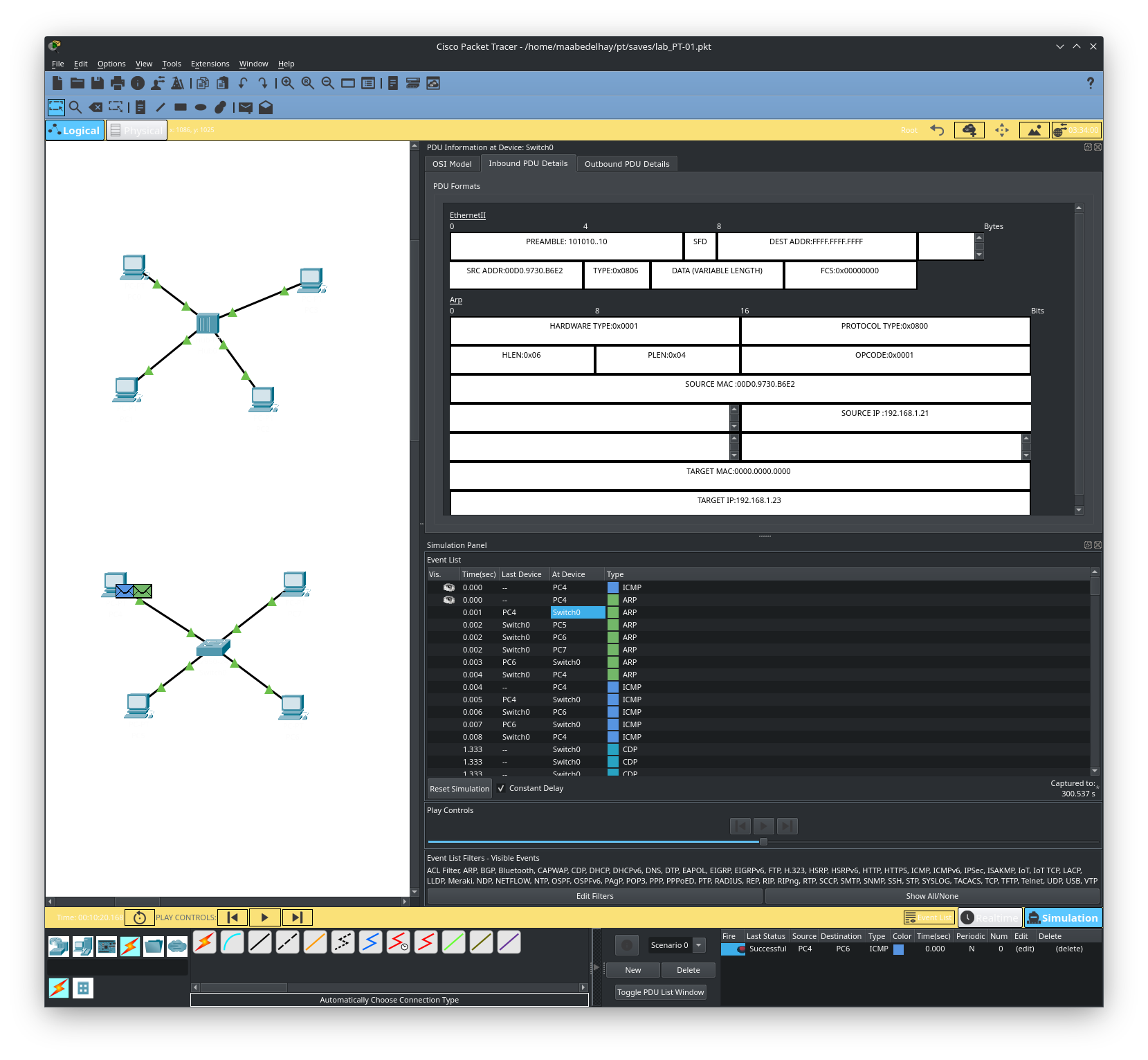


Рис. 11: Название рисунка

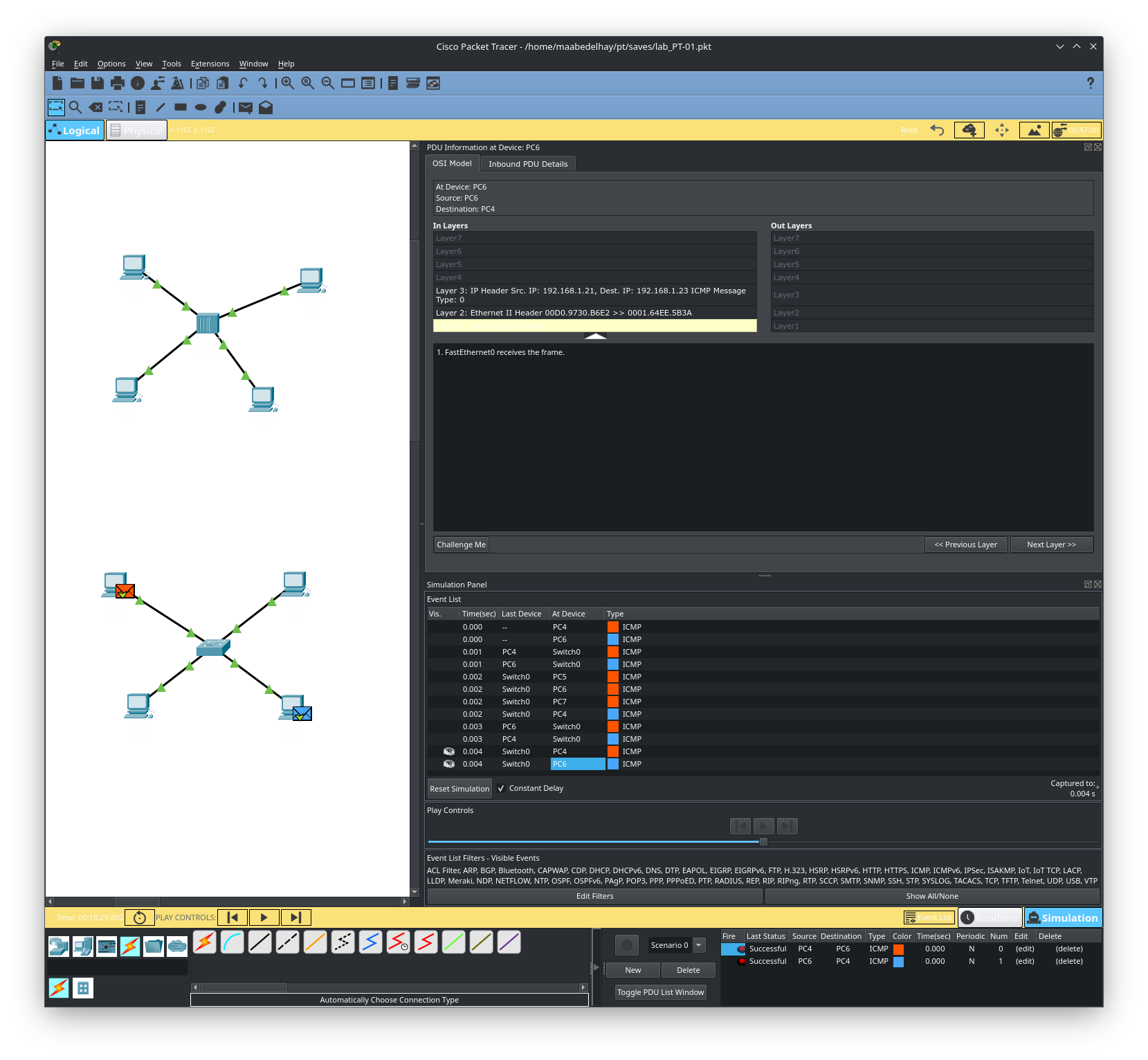


Рис. 12: Название рисунка

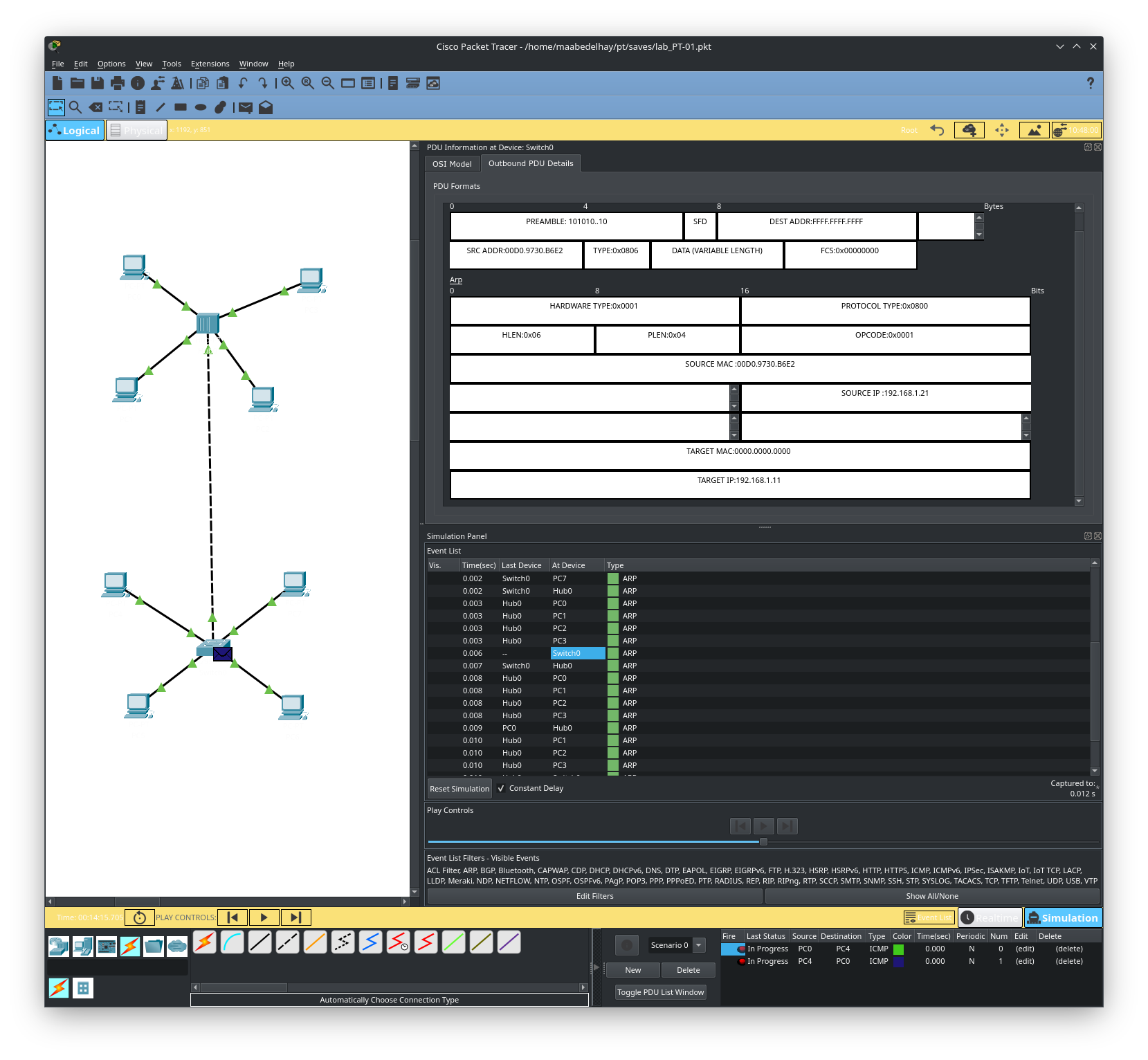


Рис. 13: Название рисунка

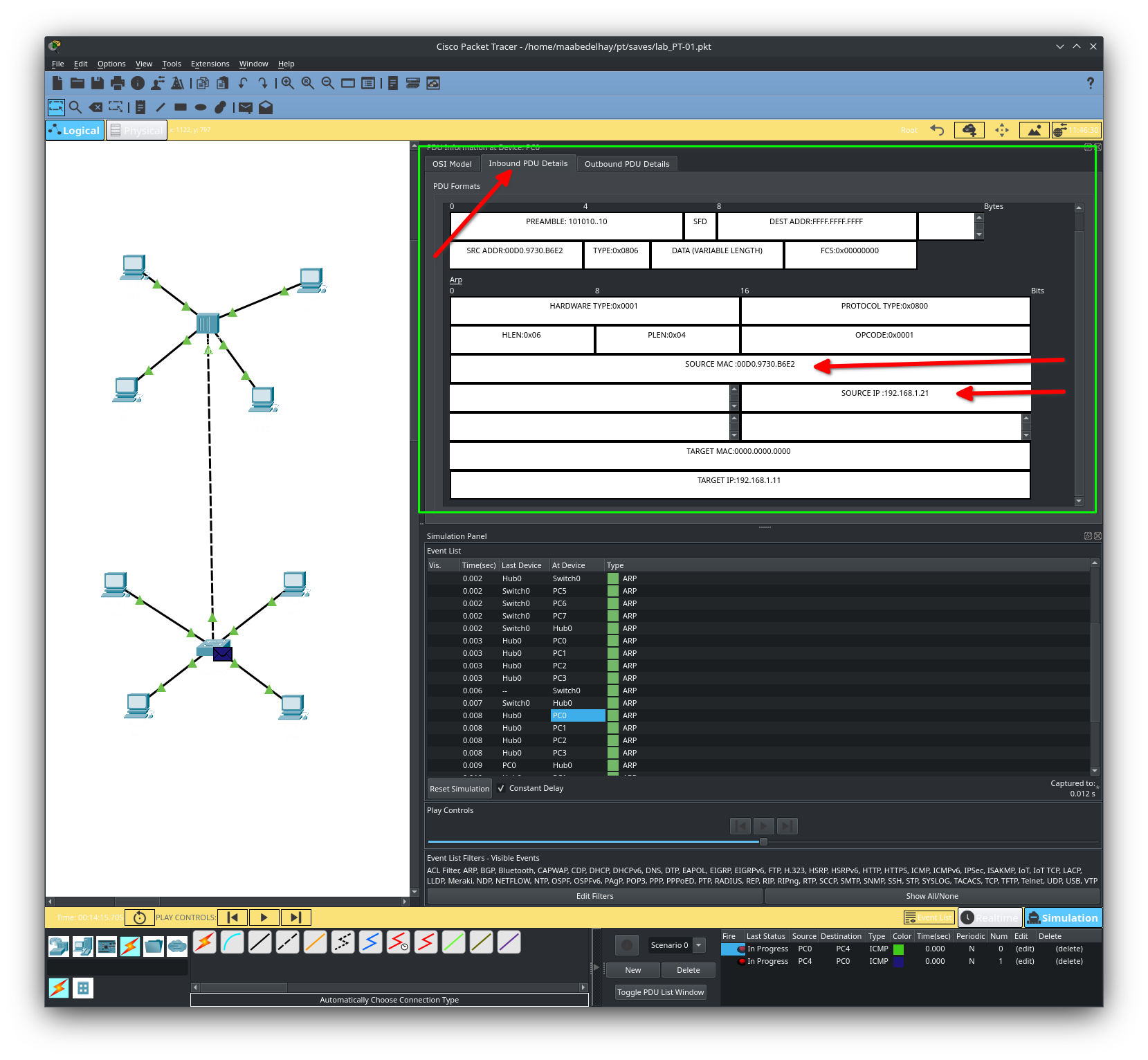


Рис. 14: Название рисунка

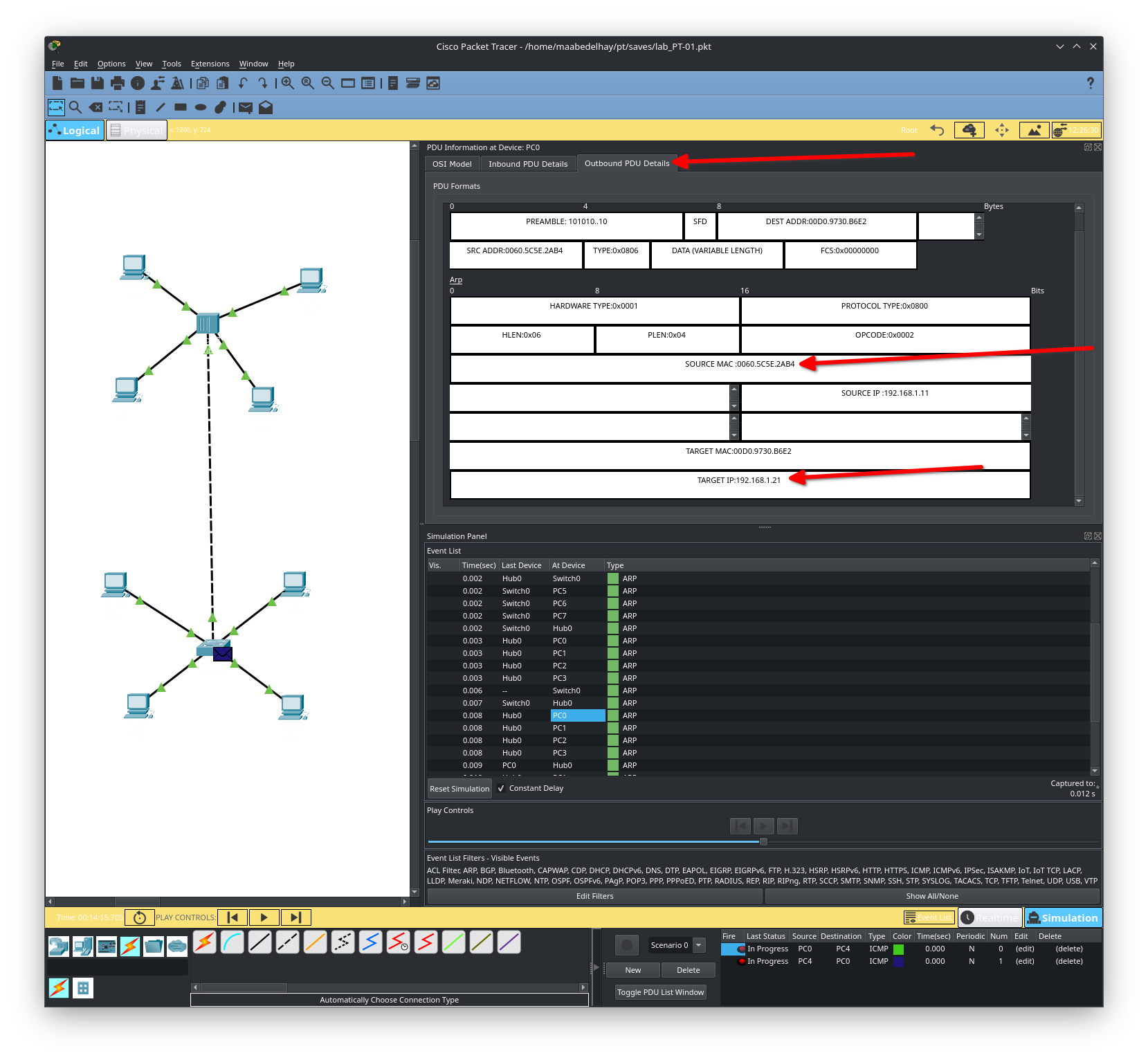


Рис. 15: Название рисунка

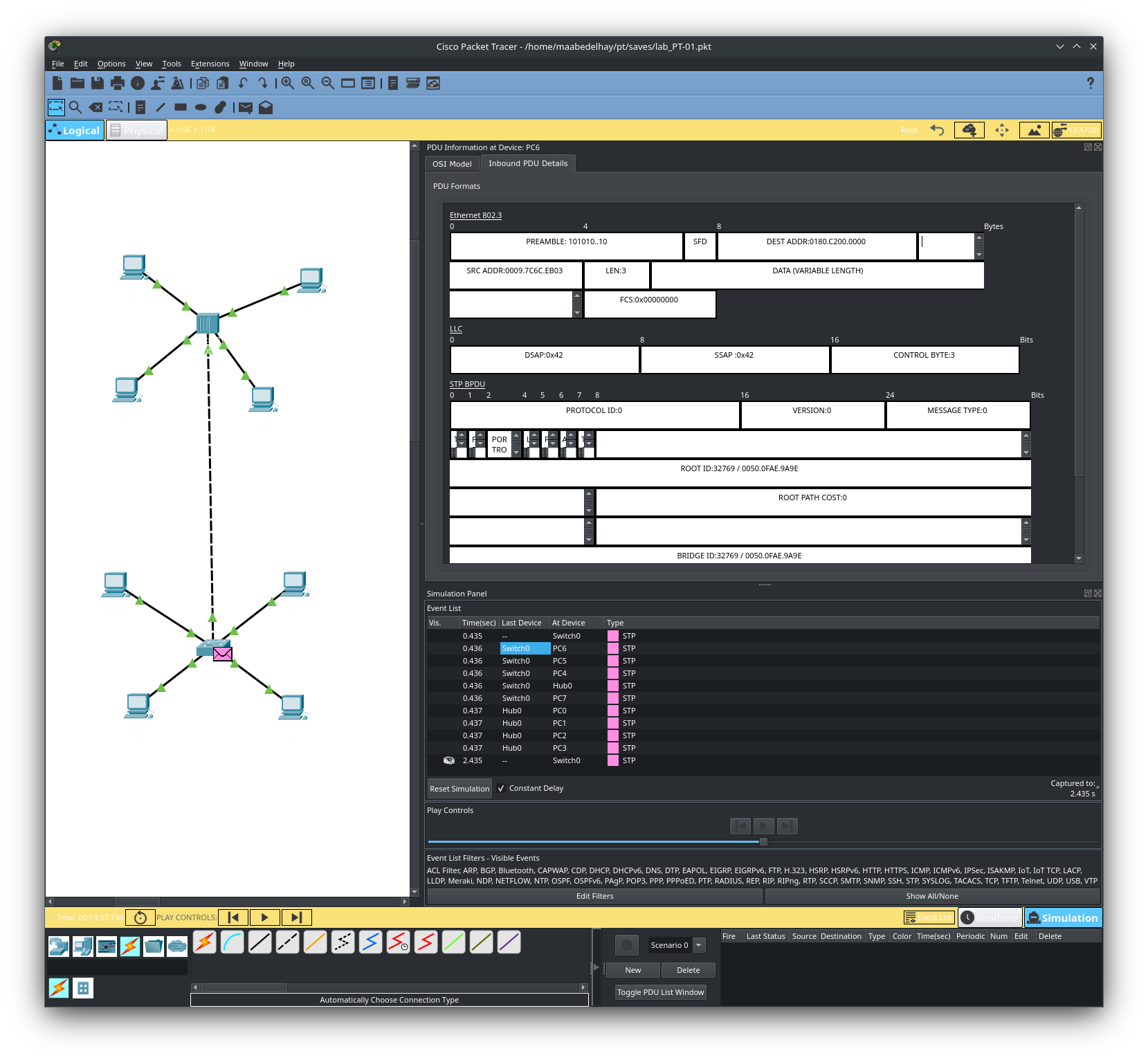


Рис. 16: Название рисунка

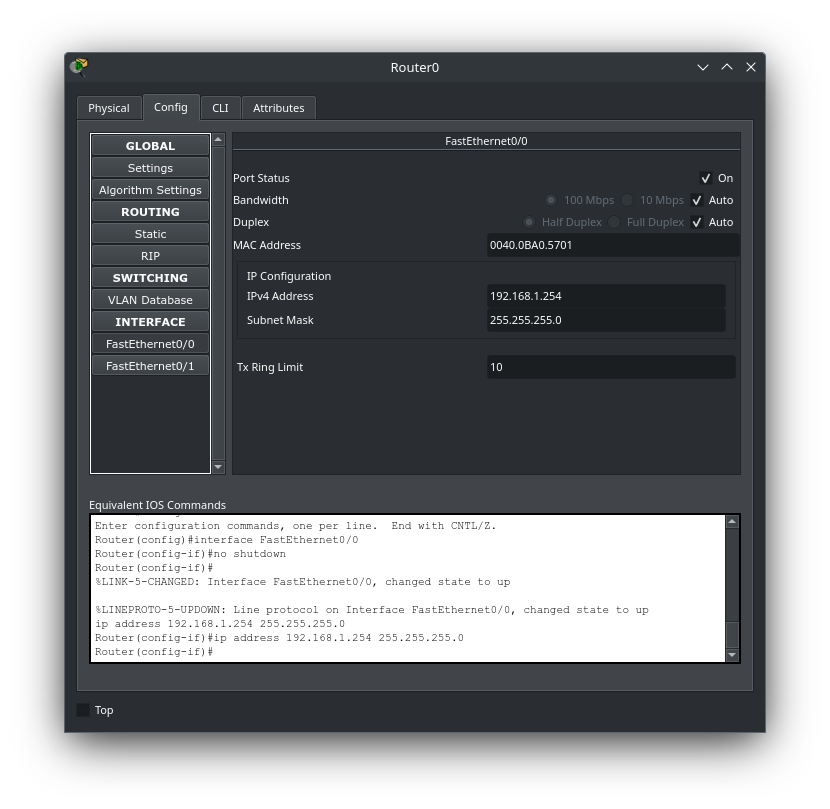


Рис. 17: Название рисунка

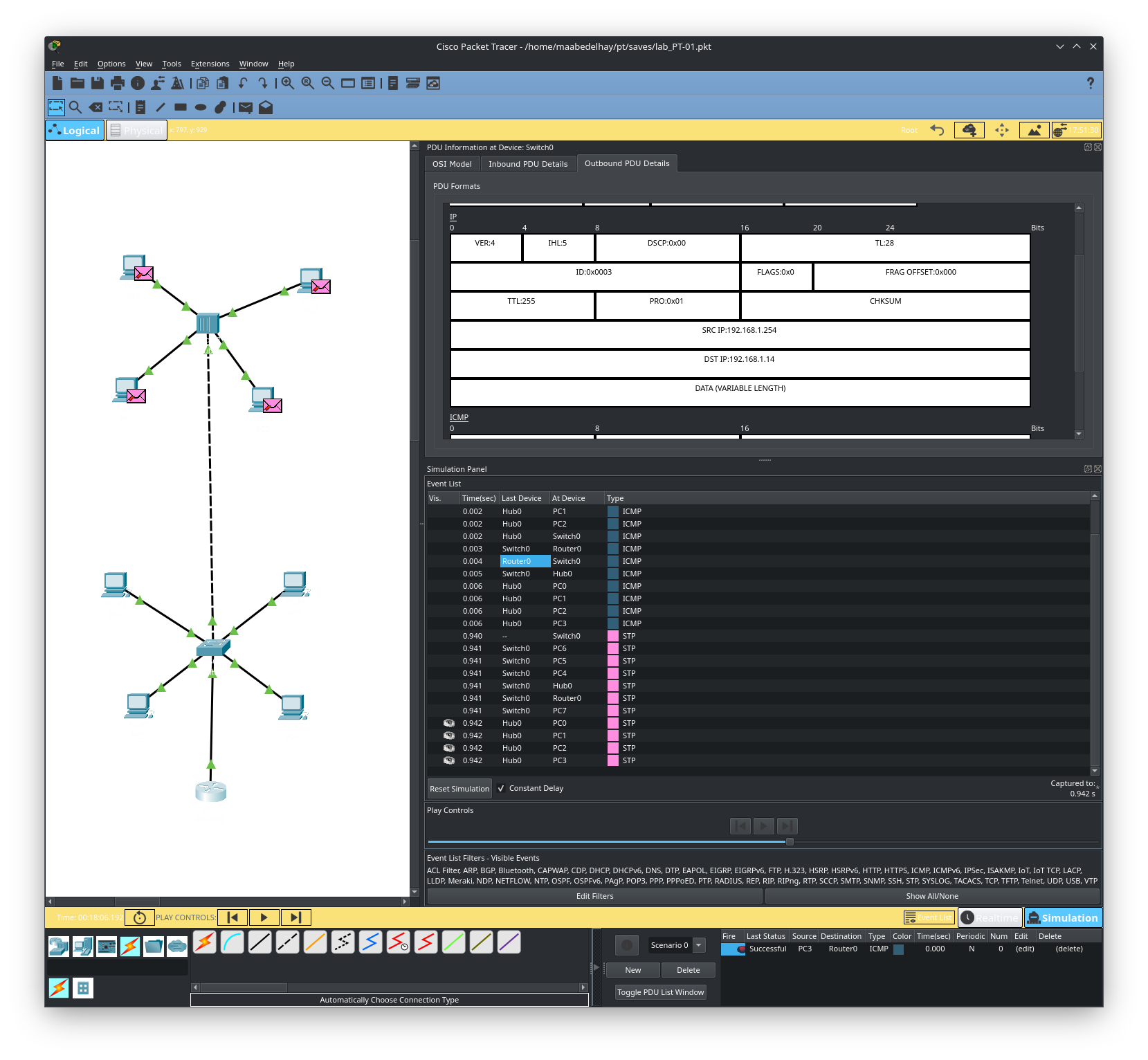


Рис. 18: Название рисунка

# 4 Выводы

Здесь кратко описываются итоги проделанной работы.

# 5 Контрольные вопросы

***Дайте определение следующим понятиям: концентратор, коммутатор, маршрутизатор, шлюз (gateway). В каких случаях следует использовать тот или иной тип сетевого оборудования?***

Определение сетевого оборудования:

Концентратор - это устройство, которое объединяет несколько сегментов сети в единую локальную сеть. Он передает данные от одного устройства к другому в пределах сети, но не имеет возможности принимать решения о маршрутизации или управлении трафиком. Коммутатор

Коммутатор - это устройство, которое принимает данные от устройства и передает их только тому устройству, для которого данные предназначены. Он обеспечивает более эффективное управление трафиком в сети, поскольку данные передаются только тем устройствам, которым они действительно нужны. Маршрутизатор

Маршрутизатор - это устройство, которое принимает данные из различных сетей и принимает решения о том, куда направить эти данные, используя информацию из сетевых протоколов. Он позволяет соединять несколько сетей и обеспечивает передачу данных между ними. Шлюз (Gateway)

Шлюз (или gateway) - это устройство, которое соединяет разные сети, преобразуя протоколы передачи данных. Он работает как точка входа или выхода для сети, позволяя устройствам в разных сетях обмениваться данными. Использование сетевого оборудования

Концентратор: Используется в небольших сегментированных сетях, где требуется простое объединение устройств в единую сеть без управления трафиком.  
  
Коммутатор: Рекомендуется для более крупных сетей, где требуется более эффективное управление трафиком и предотвращение конфликтов при передаче данных между устройствами.  
  
Маршрутизатор: Используется для соединения различных сетей, таких как локальные сети (LAN) с интернетом или другими удаленными сетями, обеспечивая маршрутизацию данных между ними.  
  
Шлюз (Gateway): Применяется для связи разнородных сетей, например, для соединения локальной сети с интернетом или для обеспечения соединения между протоколами передачи данных.

***Дайте определение следующим понятиям: ip-адрес, сетевая маска, broadcast адрес.***

IP-адрес (Internet Protocol address) - это уникальный числовой идентификатор, присваиваемый каждому устройству в сети, чтобы оно могло быть идентифицировано и обмениваться данными с другими устройствами в сети. IP-адрес состоит из четырех числовых сегментов, разделенных точками, например, 192.168.1.1. Сетевая маска

Сетевая маска (subnet mask) - это числовой параметр, определяющий, какая часть IP-адреса относится к сети, а какая - к устройству в этой сети. Она используется для разделения IP-адреса на две части: сетевую и хостовую, и определяет, какие биты адреса относятся к сети. Broadcast адрес

Broadcast адрес - это специальный адрес в сети, который используется для передачи данных всем устройствам в этой сети. При отправке данных на broadcast адрес, все устройства в сети получают эти данные. Использование сетевых терминов

IP-адрес: Каждое устройство в сети должно иметь уникальный IP-адрес, чтобы быть идентифицированным в сети и обмениваться данными с другими устройствами.  
  
Сетевая маска: Сетевая маска определяет, какая часть IP-адреса относится к сети, а какая - к устройству в этой сети. Она используется для разделения IP-адресов на подсети и определения границы между ними.  
  
Broadcast адрес: При необходимости отправить данные всем устройствам в сети, используется broadcast адрес. Это позволяет обеспечить широковещательную передачу данных в пределах сети.

***Как можно проверить доступность узла сети?***

Для проверки доступности узла сети можно воспользоваться несколькими способами: Использование командной строки (Windows или macOS)

Ping: Используйте команду "ping" с IP-адресом или доменным именем устройства, чтобы проверить доступность узла в сети. Например:  
  
  
  
ping 192.168.1.1  
  
В ответ вы получите информацию о времени отклика и потерянных пакетах.

Использование сетевых утилит (Linux)

Ping: Аналогично Windows и macOS, команда "ping" также доступна в большинстве дистрибутивов Linux для проверки доступности узла в сети.

Использование специализированных программ и сервисов

Утилиты мониторинга сети: Существуют специализированные программы и сервисы, такие как Nagios, Zabbix, PRTG, которые обеспечивают более детальный мониторинг доступности узлов сети, включая уведомления при недоступности.

Использование сетевых сканеров

Nmap: Этот инструмент может использоваться для сканирования сети и определения доступности узлов, а также для определения открытых портов и другой информации о сетевых устройствах.

Программы мониторинга сети

Wireshark: Это инструмент анализа сетевых пакетов, который может использоваться для отслеживания сетевого трафика и проверки доступности узлов в реальном времени.

Выбор метода зависит от ваших потребностей и уровня детализации, необходимой для проверки доступности узлов в сети.