

# **Лабораторная работа № 1**

**Знакомство с Cisco Packet Tracer**

Хватов Максим Григорьевич

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>4</b>
<b>2</b>	<b>Задание</b>	<b>5</b>
<b>3</b>	<b>Выполнение лабораторной работы</b>	<b>6</b>
<b>4</b>	<b>Выводы</b>	<b>14</b>
<b>5</b>	<b>Ответы на контрольные вопросы</b>	<b>15</b>

## Список иллюстраций

3.1	Модель простой сети с концентратором . . . . .	6
3.2	Добавление Simple PDU . . . . .	7
3.3	Информация о PDU: уровень OSI . . . . .	7
3.4	Модель простой сети с коммутатором . . . . .	9
3.5	Информация о PDU при отправке пакета через коммутатор . . . .	10
3.6	Конфигурация маршрутизатора . . . . .	13

# 1 Цель работы

Установить инструмент моделирования конфигурации сети Cisco Packet Tracer, ознакомиться с его интерфейсом.

## 2 Задание

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

### 3 Выполнение лабораторной работы

Создадим новый проект lab\_PT-01.pkt.

В рабочем пространстве разместим концентратор (Hub-PT) и четыре оконечных устройства PC. Соединим оконечные устройства с концентратором прямым кабелем. Щёлкнув последовательно на каждое оконечном устройстве, зададим статические IP-адреса 192.168.1.11, 192.168.1.12, 192.168.1.13, 192.168.1.14 с маской подсети 255.255.255.0

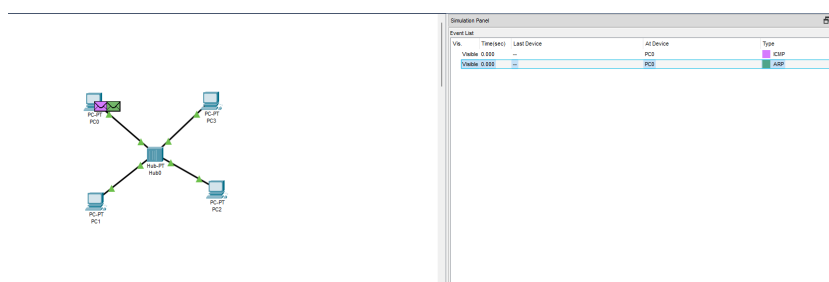


Рис. 3.1: Модель простой сети с концентратором

В основном окне проекта перейдем из режима реального времени (Realtime) в режим моделирования (Simulation). Выберем на панели инструментов мышкой «Add Simple PDU (P)» и щёлкнем сначала на PC0, затем на PC2. В рабочей области должны появились два конверта, обозначающих пакеты, в списке событий на панели моделирования должны будут появиться два события, относящихся к пакетам ARP и ICMP соответственно. На панели моделирования нажмем кнопку «Play» и проследим за движением пакетов ARP и ICMP от устройства PC0 до устройства PC2 и обратно.

Можно увидеть, что пакет сначала отправляется на хаб, далее рассылается по

всем устройствам, но принимает его только тот ПК, которому был предназначен пакет.

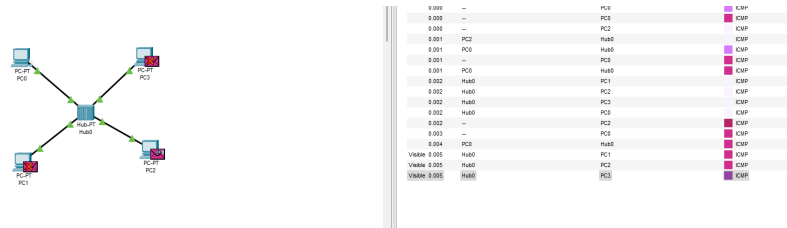


Рис. 3.2: Добавление Simple PDU

Щёлкнув на строке события, откроем окно информации о PDU и изучим, что происходит на уровне модели OSI при перемещении пакета. Используя кнопку «Проверь себя» (Challenge Me) на вкладке OSI Model, ответим на вопросы.

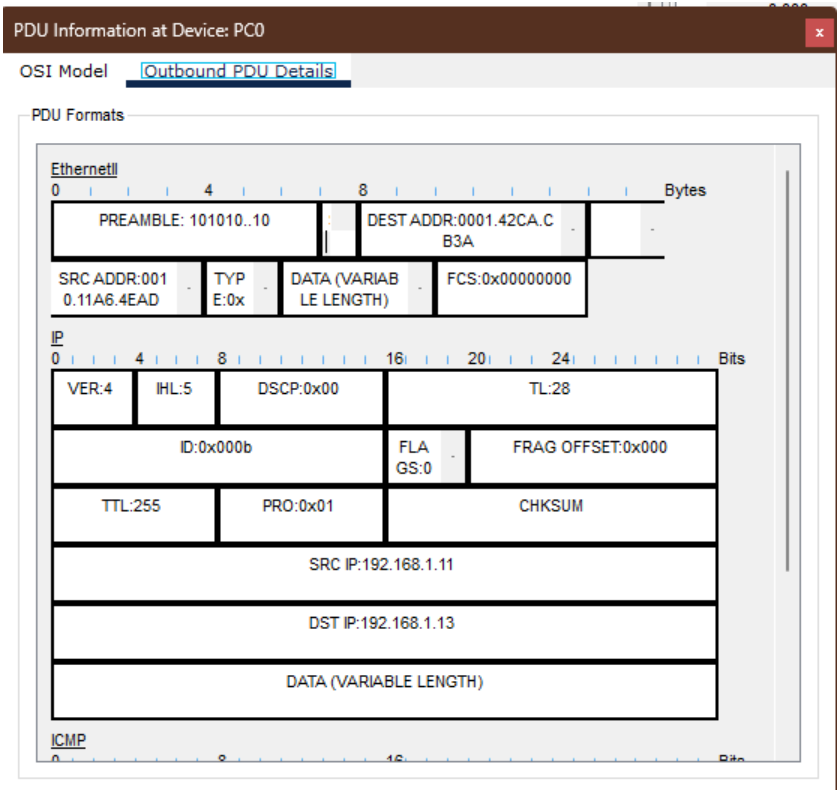


Рис. 3.3: Информация о PDU: уровень OSI

Откроем вкладку с информацией о PDU. Исследуем структуру пакета ICMP. Изначально в PDU есть только заголовок IP, в котором есть соответственно инфор-

мация об IP-адресах источника и назначения. Также там есть заголовок ICMP. В нем содержится данные о типе ICMP-пакета, его коде, контрольной сумме, его идентификаторе и порядковом номере. Эти заголовки остаются постоянными при передаче.

Далее появляется кадр Ethernet. Тут есть поле преамбула для синхронизации. Поле SFD. Destination Address — Ethernet-адрес получателя, 6 байт. Source Address — Ethernet-адрес отправителя, 6 байт. Type — тип, для обозначения типа протокола уровня. FCS — frame check sequence, 4 байта, поле контрольной последовательности фрейма.

Очистим список событий, удалив сценарий моделирования. Выберем на панели инструментов мышкой «Add Simple PDU (P)» и щёлкнем сначала на PC0, затем на PC2. Снова выберем на панели инструментов мышкой «Add Simple PDU (P)» и щёлкнем сначала на PC2, затем на PC0. На панели моделирования нажмем кнопку «Play» и проследим за возникновением коллизии. В списке событий посмотрим информацию о PDU.

Увидим, что пакеты сначала передаются на хаб, где и возникает коллизия, так как он не может передать два сообщения одновременно. У первого сообщения информация о PDU не отображается, а у второго ее в принципе не должно быть. Далее второй пакет вообще исчезает, а второй отправляется на все устройства, но пустое, возникает ошибка.

Перейдем в режим реального времени (Realtime). В рабочем пространстве разместим коммутатор (например Cisco 2950-24) и 4 оконечных устройства PC. Соединим оконечные устройства с коммутатором прямым кабелем. Щёлкнув последовательно на каждом оконечном устройстве, зададим статические IP-адреса 192.168.1.21, 192.168.1.22, 192.168.1.23, 192.168.1.24 с маской подсети 255.255.255.0.





Рис. 3.4: Модель простой сети с коммутатором

В основном окне проекта перейдем из режима реального времени (Realtime) в режим моделирования (Simulation). Выберем на панели инструментов мышкой «Add Simple PDU (P)» и щёлкнем сначала на PC4, затем на PC6. В рабочей области появились два конверта, обозначающих пакеты, в списке событий на панели моделирования появились два события, относящихся к пакетам ARP и ICMP соответственно. На панели моделирования нажмем кнопку «Play» и проследим за движением пакетов ARP и ICMP от устройства PC4 до устройства PC6 и обратно.

Сначала, как и в случае с хабом, пакеты ARP рассылаются по всем оконечным устройствам, но принимает его только ПК, которому предназначалось сообщение. Обратное же ARP не рассылается по всем устройствам, пакет идет только к ПК6 (он уже знает свой путь).

Исследуем структуру пакета ICMP. Изначально в PDU есть только заголовок IP, в котором есть соответственно информация об IP-адресах источника и назначения. Также там есть заголовок ICMP. В нем содержится данные о типе ICMP-пакета, его коде, контрольной сумме, его идентификаторе и порядковом номере. Эти заголовки остаются постоянными при передаче.

Далее появляется кадр Ethernet. Тут есть поле преамбула — 7 байт для синхронизации. Поле SFD. Destination Address — Ethernet-адрес получателя, 6 байт. Source Address — Ethernet-адрес отправителя, 6 байт. Type — тип, для обозначения типа протокола уровня. FCS — frame check sequence, 4 байта, поле контрольной последовательности фрейма.

Пакет отправляется на коммутатор, в заголовке указаны mac-адреса, в которых

указано, что пакет идет от ПК4 к ПК6.

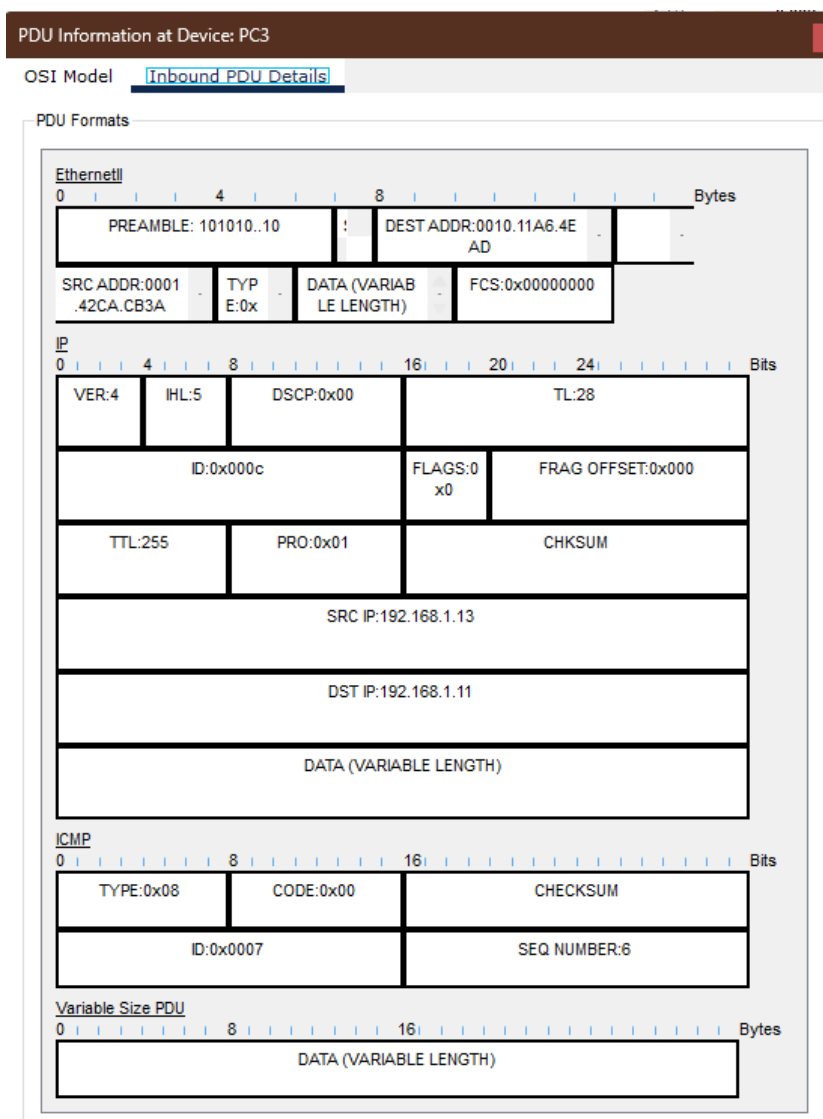


Рис. 3.5: Информация о PDU при отправке пакета через коммутатор

Очистим список событий, удалив сценарий моделирования. Выберем на панели инструментов мышкой «Add Simple PDU (P)» и щёлкнем сначала на PC4, затем на PC6. Снова выберем на панели инструментов мышкой «Add Simple PDU (P)» и щёлкнем сначала на PC6, затем на PC4. На панели моделирования нажмем кнопку «Play» и проследим за движением пакетов.

Коллизия не возникает, потому что пакет не отправляется всем устройствам, а

расходится по нужным назначениям коммутатором.

Перейдем в режим реального времени (Realtime). В рабочем пространстве соединим кроссовым кабелем концентратор и коммутатор. Перейдем в режим моделирования (Simulation). Очистим список событий, удалив сценарий моделирования. Выберем на панели инструментов мышкой «Add Simple PDU (P)» и щёлкнем сначала на PC0, затем на PC4. Снова выберем на панели инструментов мышкой «Add Simple PDU (P)» и щёлкнем сначала на PC4, затем на PC0. На панели моделирования нажмем кнопку «Play» и проследим за движением пакетов.

Пакет, который отправлен из сети с хабом, как и в прошлый раз исчезает. А пакет, отправленный из сети с коммутатором достигает своего назначения. Так получается, потому что коммутатор может работать в режиме полного дуплекса (двунаправленная передача данных. Способность устройства или линии связи передавать данные одновременно в обоих направлениях по одному каналу, потенциально удваивая пропускную способность).

Очистим список событий, удалив сценарий моделирования. На панели моделирования нажмем «Play» и в списке событий получим пакеты STP. Исследуем структуру STP.

Заголовок STP (Spanning Tree Protocol) включает в себя поля: Идентификатор протокола (Protocol Identifier) — 2-х байтовое поле, которое всегда равно нулю. Версия STP протокола (Protocol Version Identifier) — поле размером в 1 байт, значение которого, всегда равно «0». Тип BPDU (BPDU type) — 1 байт, которые принимает значение «0», если это конфигурационный BPDU (CBPDU), или «1», если это TCN BPDU. CBPDU (Configuration Bridge Protocol Data Unit) — кадр, используемый для вычисления связующего дерева. То есть, когда значение = 0. Флаги (Flags) — в этом поле используются только 1 байт. Эти флаги используются при изменении топологии (бит «1») и при подтверждении топологии (бит «8»). Идентификатор корневого моста (Root Identifier) — в этом поле содержится информация о корневом коммутаторе, а именно его приоритет и MAC-адрес. Расстояние до корневого моста (Root Path Cost) — здесь содержится суммарная

стоимость до корневого коммутатора. Идентификатор моста (Bridge Identifier) — сюда коммутатор-отправитель записывает свои данные (приоритет + MAC-адрес). Идентификатор порта (Port Identifier) — сюда коммутатор-отправитель записывает идентификатор порта (то есть тот, с которого этот BPDU выйдет). Время жизни сообщения (Message Age) — здесь содержится временной интервал (в секундах). Он нужен для того, чтобы распознать устаревшие кадры и отбросить. Максимальное время жизни сообщения (Max Age) — это поле отвечает, как раз, за максимальное время жизни. Превысив его, коммутатор отбрасывает кадр. Время приветствия (Hello Time) — Временной интервал, через который коммутатор посылает BPDU кадры. По-умолчанию — это 2 секунды. Задержка смены состояний (Forward Delay) — временной интервал, указывающий сколько секунд порт коммутатора будет находиться в состоянии прослушивания и обучения.

Перейдем в режим реального времени (Realtime). В рабочем пространстве добавим маршрутизатор (например, Cisco 2811). Соединим прямым кабелем коммутатор и маршрутизатор. Щёлкнем на маршрутизаторе и на вкладке его конфигурации пропишем статический IP-адрес 192.168.1.254 с маской 255.255.255.0, активируем порт, поставив галочку «On» напротив «Port Status».

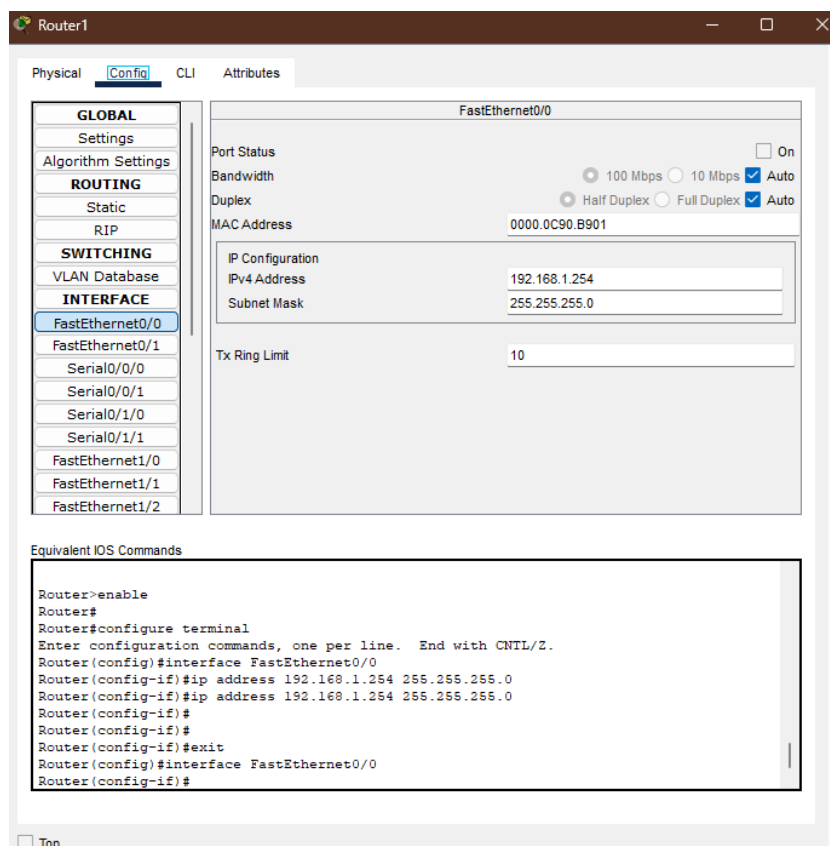


Рис. 3.6: Конфигурация маршрутизатора

Исследуем структуру пакета CDP. Поле Version - поле версии содержит используемую версию протокола CDP. В этом поле всегда содержится значение 0x01.

Поле Time-to-Live (время жизни) указывает время в секундах, в течение которого получатель пакета CDP должен сохранять информацию, содержащуюся в пакете.

Поле Checksum контрольной суммы содержит стандартную для протокола IP контрольную сумму.

Поле Type - поле типа указывает на тип тройки type/length/value.

Length - поле длины содержит общую длину в байтах полей type/length/value.

Value - поле значения содержит нечто, зависящее от параметра Type.

## 4 Выводы

В процессе выполнения данной лабораторной работы я установил инструмент моделирования конфигурации сети Cisco Packet Tracer, ознакомился с его интерфейсом.

## 5 Ответы на контрольные вопросы

1. Концентратор — это устройство, которое объединяет несколько устройств в локальной сети, пересылая данные на все порты без фильтрации. Используется в небольших сетях, но неэффективен из-за высокой нагрузки и коллизий.

Коммутатор — это более усовершенствованная версия концентратора, который направляет данные только к конкретному устройству, используя MAC-адреса. Эффективен для средних и больших сетей, позволяет уменьшить количество коллизий и повысить производительность.

Маршрутизатор — это устройство, которое направляет данные между различными сетями, определяя наилучший путь для передачи. Используется для подключения сетей к Интернету и между собой, подходит для масштабируемых решений.

Шлюз (gateway) — это устройство, обеспечивающее связь между сетями с различными протоколами. Его используют в сложных сетевых архитектурах, где требуется интеграция разных технологий.

2. IP-адрес — это уникальный числовой идентификатор устройства в сети, который необходим для его адресации и обмена данными. Существует два типа IP-адресов: IPv4 (например, 192.168.1.1) и IPv6.

Сетевая маска — это 32-битное число, которое делит IP-адрес на две части: сеть и узел. Она помогает определить, какие адреса принадлежат одной сети, и указывает, какие биты в адресе являются идентификатором сети.

Broadcast-адрес — это специальный адрес, используемый для отправки сообщения всем устройствам в сети. Он позволяет передавать данные всем узлам одновременно, например, адрес 192.168.1.255 в сети 192.168.1.0 с маской 255.255.255.0.

3. Для проверки доступности узла сети можно использовать следующие методы:

Ping — команда, которая отправляет ICMP-запросы на указанный IP-адрес или доменное имя. Если узел доступен, он отвечает, показывая время отклика. Команда выполняется в терминале или командной строке, например, `ping 192.168.1.1`.

Traceroute — утилита, позволяющая проследить маршрут пакетов до узла. Она показывает, какие промежуточные устройства (роутеры) пакет проходит. В Linux команда выглядит как `traceroute 192.168.1.1`, а в Windows — `tracert 192.168.1.1`.

Telnet — используется для проверки доступности определенных портов на узле. Например, команда `telnet 192.168.1.1 80` проверяет, доступен ли веб-сервер по порту 80.

Nslookup — позволяет проверить доступность доменного имени и его IP-адреса. Команда `nslookup example.com` вернет IP-адрес.