

Лабораторная работа № 1

Тема: Изучение пакета Packet Tracer

Цель работы: познакомиться с основными возможностями пакета Packet Tracer и приобрести некоторые навыки работы с этой программой.

Краткое руководство по использованию программы Packet Tracer

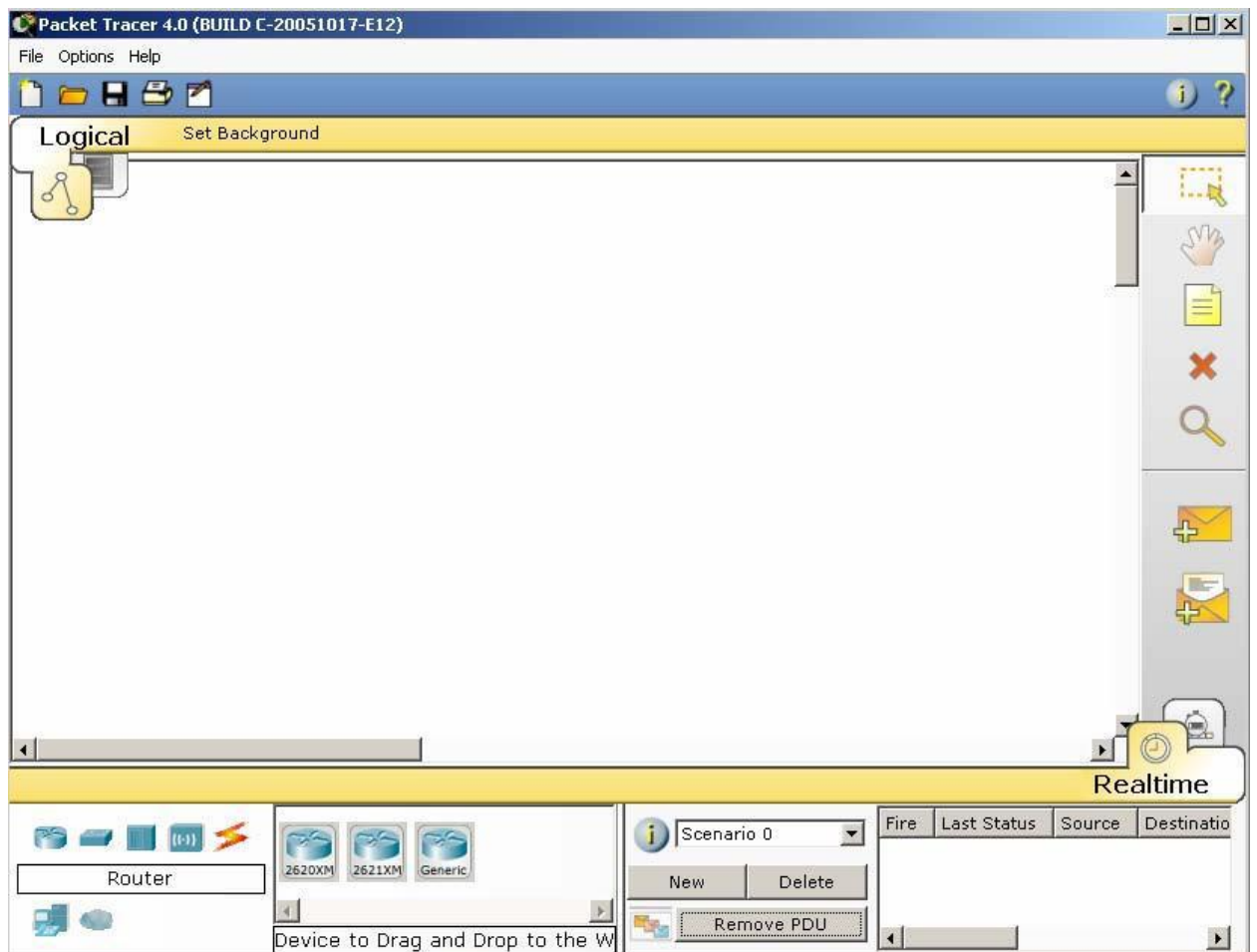
Учимся использовать Packet Tracer

Packet Tracer (PT) – симулятор протоколов разработанный Cisco Systems. Это мощный динамический инструмент, который отображает различные протоколы, используемые в организации сети, либо в режиме реального времени (Real Time), либо в режиме моделирования (Simulation mode). Включает в себя: протоколы второго уровня, такие как Ethernet и PPP, протоколы третьего уровня, такие как IP, ICMP и ARP и протоколы четвертого уровня, такие как TCP и UDP. Работа протоколов маршрутизации также может быть трассирована (отслежена).

Цель: Заключается в том, чтобы ознакомиться с интерфейсом Packet Tracer, разобраться как использовать существующие топологии и создавать свои собственные.

Действие 1: Ознакомление с интерфейсом PT используя Hub топологию

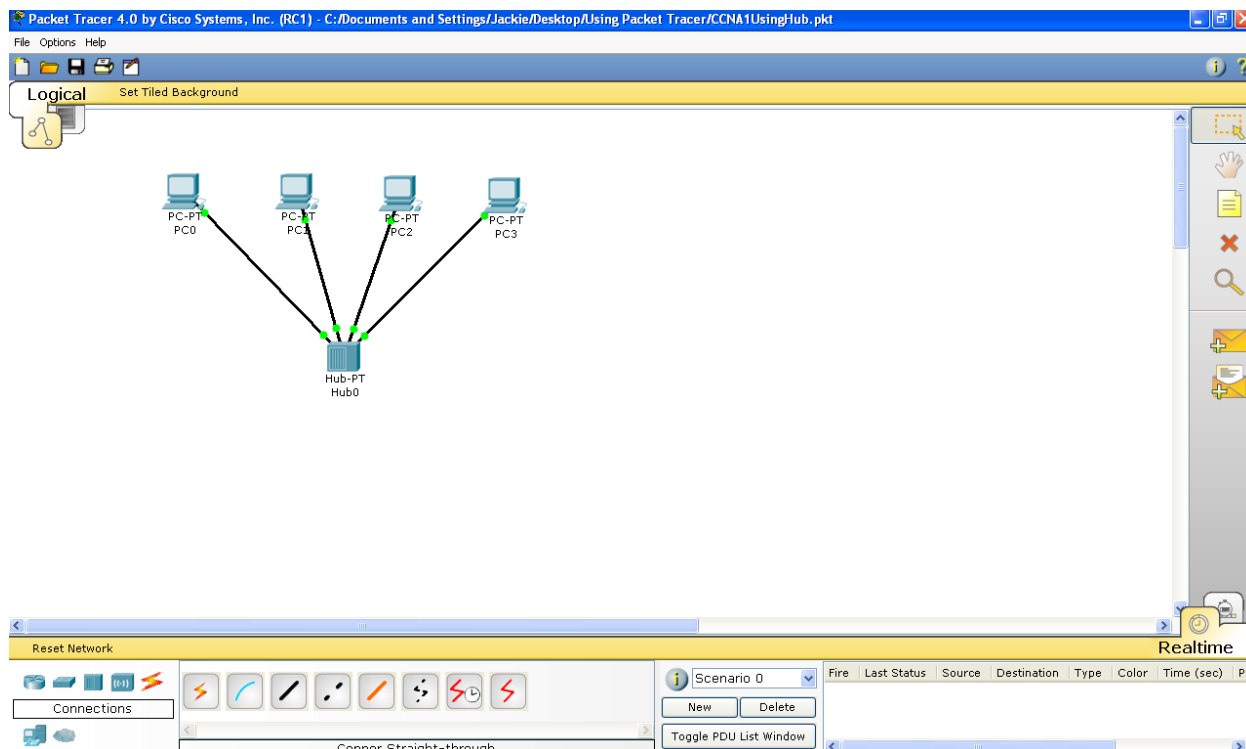
Шаг 1: Запуск Packet Tracer и вход в режим моделирования (Simulation Mode)



Шаг 2: Открыть существующую топологию

Выполните следующие шаги чтобы открыть файл lab1_hub.pkt

1. Кликните кнопку Open на панели инструментов
2. Откройте файл lab1_hub.pkt

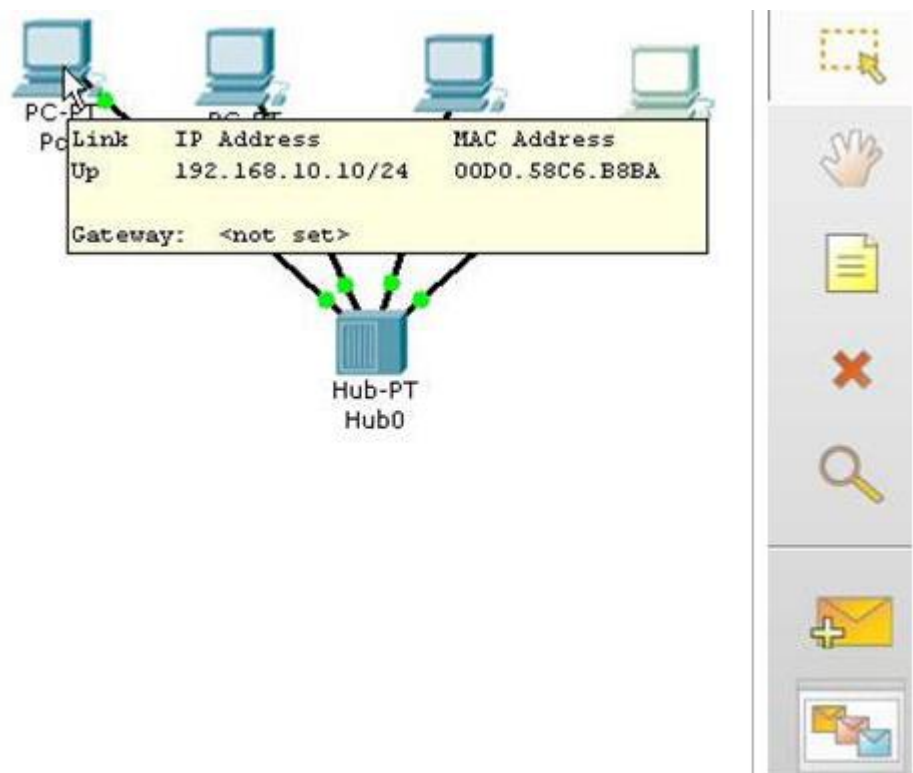


По умолчанию топология открывается в режиме реального времени (RealTime mode). Мы подробнее рассмотрим различие между режимами реального времени и моделирования в следующих шагах.

Режим моделирования (Simulation) позволяет увидеть последовательность событий, связанную с соединениями между двумя и более устройствами. Режим реального времени (RealTime) выполняет операцию со всей последовательностью событий происходящих в «реальном времени»

При возникновении различных вопросов можно воспользоваться меню Help. Online помощь и обучающие программы также доступны, так что можете использовать эти услуги в своих интересах.

Чтобы посмотреть IP-адрес, маску подсети, шлюз по умолчанию и MAC-адрес хоста (хозяина), наведите курсор мышки на нужный Вам компьютер. Удостоверьтесь в том, что справа выбрана опция Select Tool.



Шаг 3: Проблема пингования PC1 с PC0

Пингование (pings) и ICMP протокол будут рассмотрены более подробно при следующих шагах. Программа для пингования генерирует IP-пакет со скрытым сообщением ICMP эхо запроса. Этот инструмент используется для тестирования основных связей второго и третьего уровня между двумя устройствами. Когда пользователь запускает команду ping, большинство операционных систем посылают несколько (4 или 5) ICMP эхо сообщений. Когда устройство назначения получает ping эхо запрос, оно генерирует эхо ответ.

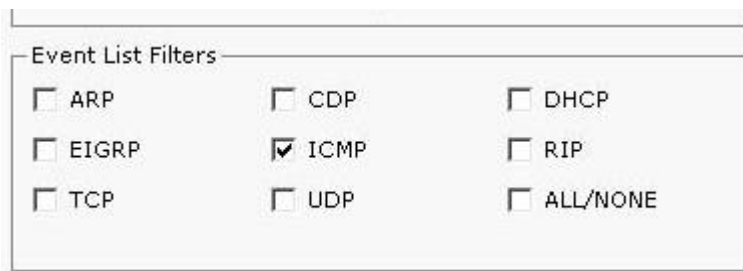
Команда, которую следует вводить с PC0 имеет вид: ping 192.168.10.37

Packet Tracer позволяет Вам либо ввести команду в командной строке (Command Prompt), либо использовать инструмент Add Simple PDU. Ниже будут продемонстрированы оба этих метода.

Чтобы включить режим моделирования, кликните закладку **Simulation Mode** в правом нижнем углу интерфейса.



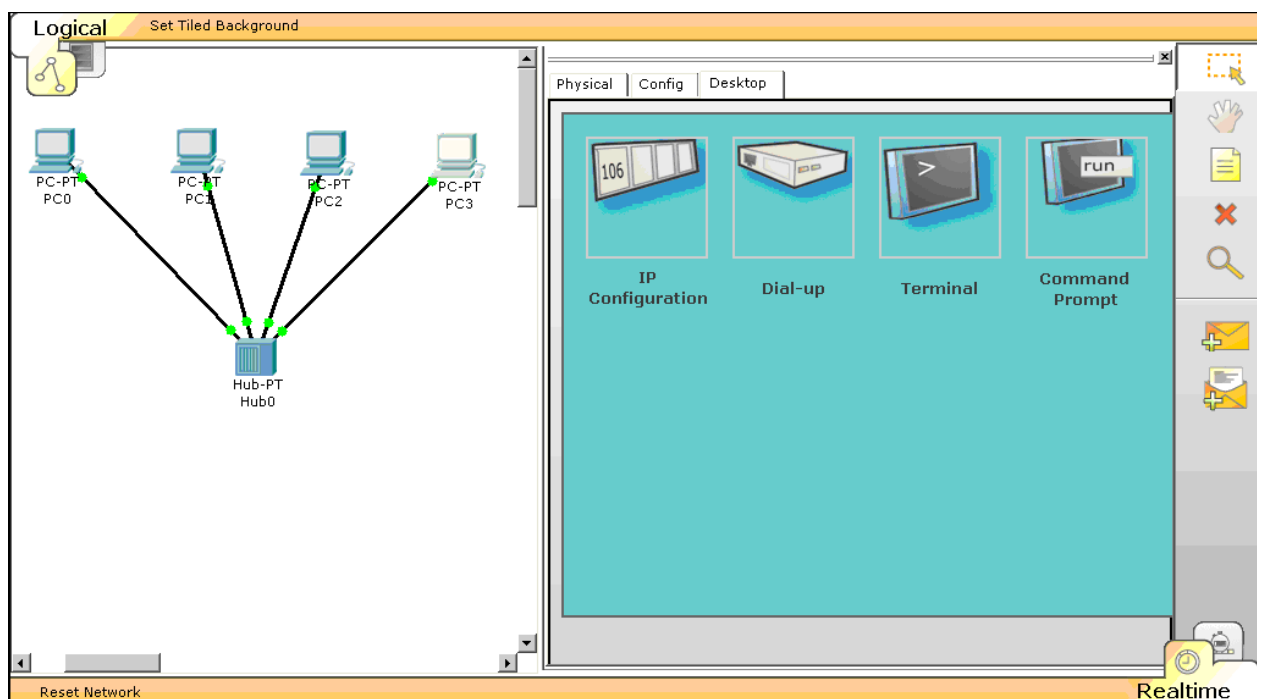
Вместо того, чтобы просматривать “pings” в списке событий (**Event List**), кликните **ALL/NONE**, для снятия всех галочек, затем кликните **ICMP** и выберете только этот протокол.



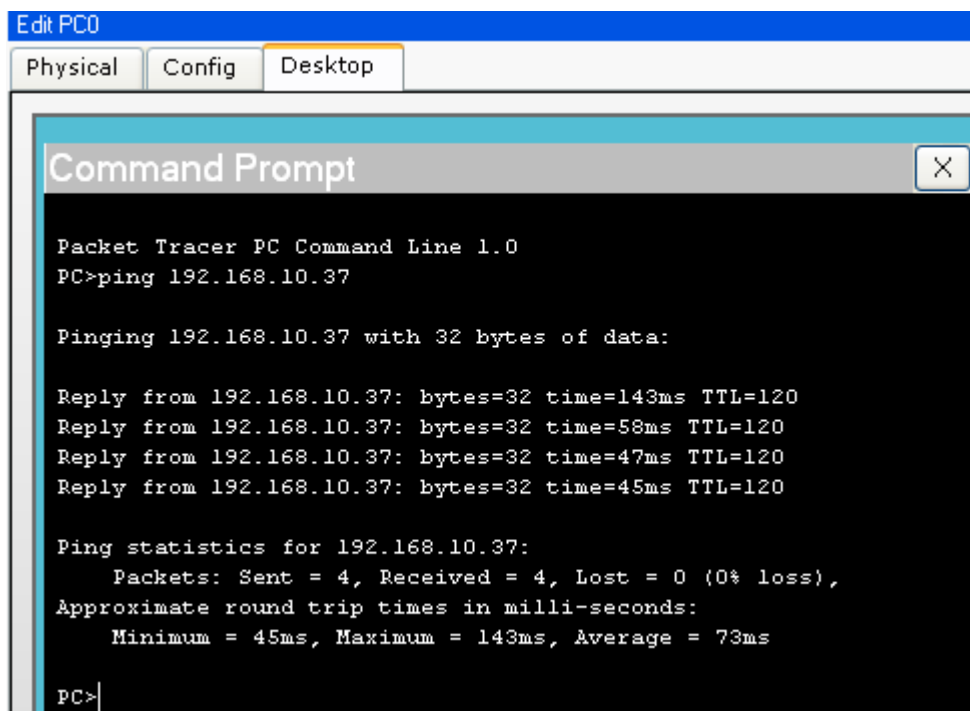
Ping: Использование командной строки в режиме реального времени.

Вернитесь в режим реального времени (кликните закладку **Realtime** в правом нижнем углу экрана)

Один раз кликните **PC0** левой кнопкой мышки, затем кликните на закладку **Desktop**. В появившемся окне выберете **Command Prompt**.



Установите курсор после **PC>** и введите следующую ping-команду:
ping 192.168.10.37 Нажмите Enter.



```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.10.37

Pinging 192.168.10.37 with 32 bytes of data:

Reply from 192.168.10.37: bytes=32 time=143ms TTL=120
Reply from 192.168.10.37: bytes=32 time=58ms TTL=120
Reply from 192.168.10.37: bytes=32 time=47ms TTL=120
Reply from 192.168.10.37: bytes=32 time=45ms TTL=120

Ping statistics for 192.168.10.37:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 45ms, Maximum = 143ms, Average = 73ms

PC>
```

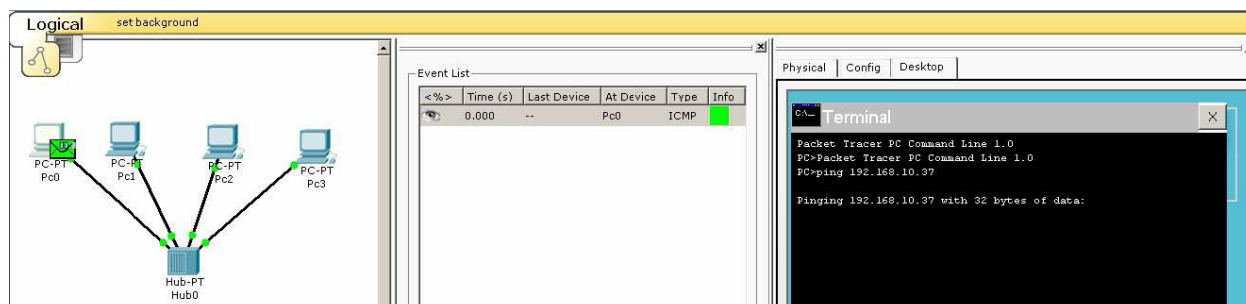
Ping: Использование режима моделирования

Кликните на закладку **Simulation** в правом нижнем углу экрана Packet Tracer (расположена позади **Realtime**)

Если Вы не видите топологии, закройте окно **Event List**.

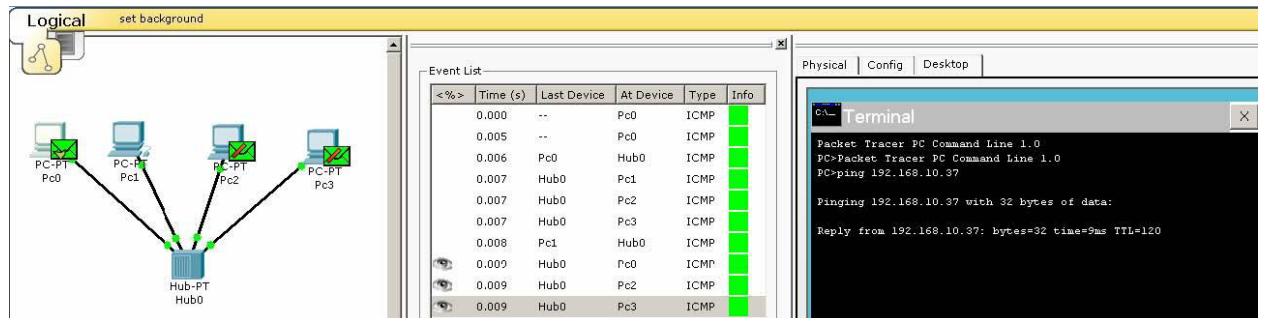
Введите заново команду ping в окне **Terminal** (используйте стрелку вверх на Вашей клавиатуре для повтора последней команды).

Вы заметите, что пакет ICMP готовится покинуть PC0 (левый экран). Это также отображается в **Event List** (средний экран).



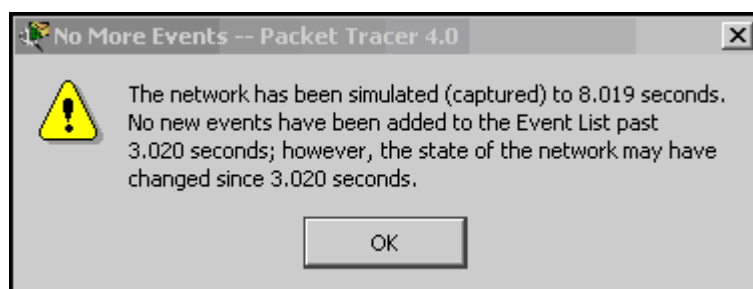
Кликните кнопку **Capture / Forward** в **Play Controls** (желтая панель под окнами) чтобы посмотреть пошаговый процесс выполнения команды ping.

Когда просмотрите события, обратите внимание, как hub обрабатывает каждый фрейм (Ethernet фрейм, IP пакет и ICMP сообщение). Заметьте, что каждое событие отображается в **Event List**. Также заметьте, что ping-программа отображает ICMP эхо ответ от PC1.



Продолжайте нажимать кнопку Capture / Forward до тех пор пока все фреймы не будут посланы. **Обратите внимание на то, что hub отправляет фрейм через все порты, за исключением того, откуда он пришел.**

Когда ping-программа завершит отправку наших ping'ов (ICMP эхо запросы) Вы получите следующее сообщение:



Использование инструмента Simple PDU

Другим способом пингования устройства является использование инструмента **Simple PDU**. При использовании этого инструмента отпадает необходимость использовать командную строку и команду ping. Прежде, чем перейти к этому шагу закройте Desktop для PC0 кликните “X” в правом углу.

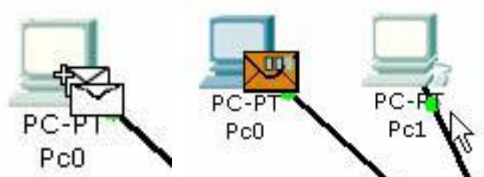


Восстановите **Event List**, если необходимо, кликнув Event List на желтой панели, слева от Simulation, и кликнув кнопку **Reset Simulation**.

Выберете инструмент **Add Simple PDU** из набора



Кликните один раз PC0, устройство отправляющее ICMP эхо запрос и затем кликните один раз PC1 (получатель)



Нажмите кнопку **Capture / Forward** и понаблюдайте за ICMP эхо запросами и ICMP эхо ответами. Заметьте, что hub рассылает фрейм по всем портам, за исключением того, откуда тот пришел.

Заметка: Этот инструмент отправляет только один ICMP эхо запрос, вместо четырех при использовании командной строки (Command Prompt).

Шаг 4: Использование Protocol Analyzer

Чтобы больше узнать о работе протоколов, кликните **Info** в **Event List**.

The screenshot displays the Protocol Analyzer interface. The main window is titled "PDU Info at Device: Pc0" and has two tabs: "OSI Model" and "Outbound PDU Details". The "Outbound PDU Details" tab is active, showing the following information:

- At Device: Pc0
- Source: Pc0
- Destination: Pc1

Below this, there are two columns: "In Layer" and "Out Layer". The "In Layer" column lists Layer7, Layer6, Layer5, Layer4, Layer3, Layer2, and Layer1. The "Out Layer" column lists Layer7, Layer6, Layer5, Layer4, Layer3, Layer2, and Layer1. The "Layer 3" row in the "Out Layer" column is highlighted, showing the IP Header Src. IP: 192.168.10.10, Dest. IP: 192.168.10.37.

At the bottom of the "Outbound PDU Details" tab, there is a text area with the following steps:

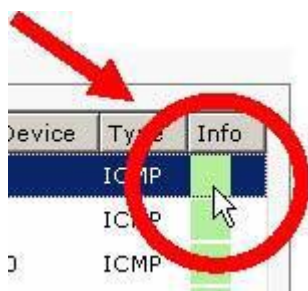
1. The Ping process starts next ping request.
2. The Ping process creates an ICMP echo request message and sends it to the lower process.
3. The source IP address is not specified. The device sets it to the port's IP address.
4. The destination IP address is in the same subnet. The device sets the next hop to destination.

At the bottom of the window, there are buttons for "Challenge Me", "<<", and ">>".

On the right side, there is an "Event List" window. It contains a table with the following columns: "<%>", "Time (s)", "Last Device", "At Device", "Type", and "Info". The table lists several ICMP events:

<%>	Time (s)	Last Device	At Device	Type	Info
0.000	--	Pc0	Pc0	ICMP	
0.004	--	Pc0	Pc0	ICMP	
0.005	--	Pc0	Hub0	ICMP	
0.006	--	Hub0	Pc1	ICMP	
0.006	--	Hub0	Pc2	ICMP	
0.006	--	Hub0	Pc3	ICMP	
0.007	--	Pc1	Hub0	ICMP	
0.008	--	Hub0	Pc0	ICMP	
0.008	--	Hub0	Pc2	ICMP	
0.008	--	Hub0	Pc3	ICMP	

At the bottom of the "Event List" window, there is a "Reset Network" button and a checkbox labeled "Constant Delay".



По умолчанию стоит третий уровень Outbound OSI Model, представление с кратким описанием того, что происходит с этим пакетом.

PDU Info at Device: Pc0

OSI Model | Outbound PDU Details

At Device: Pc0
Source: Pc0
Destination: Pc1

In Layer

Layer7

Layer6

Layer5

Layer4

Layer3

Layer2

Layer1

Out Layer

Layer7

Layer6

Layer5

Layer4

Layer 3: IP Header Src. IP: 192.168.10.10, Dest. IP: 192.168.10.37

Layer 2:

Layer1

1. The Ping process starts next ping request.
2. The Ping process creates an ICMP echo request message and sends it to the lower process.
3. The source IP address is not specified. The device sets it to the port's IP address.
4. The destination IP address is in the same subnet. The device sets the next hop to destination.

Challenge Me << >>

Нажмите на закладку Outbound PDU Details, чтобы увидеть Ethernet фрейм второго уровня и IP пакет третьего уровня, а также ICMP сообщение.

PDU Info at Device: Pc0

OSI Model | Outbound PDU Details

PDU Formats

Ethernet II

0	4	8	14	19	Bytes
PREAMBLE: 1010 1010		DEST MAC: 0002.16AB.5C50		SRC MAC: 00D0.58C6.B8BA	
TYPE: 0x800		DATA (VARIABLE LENGTH)			FCS: 0x0

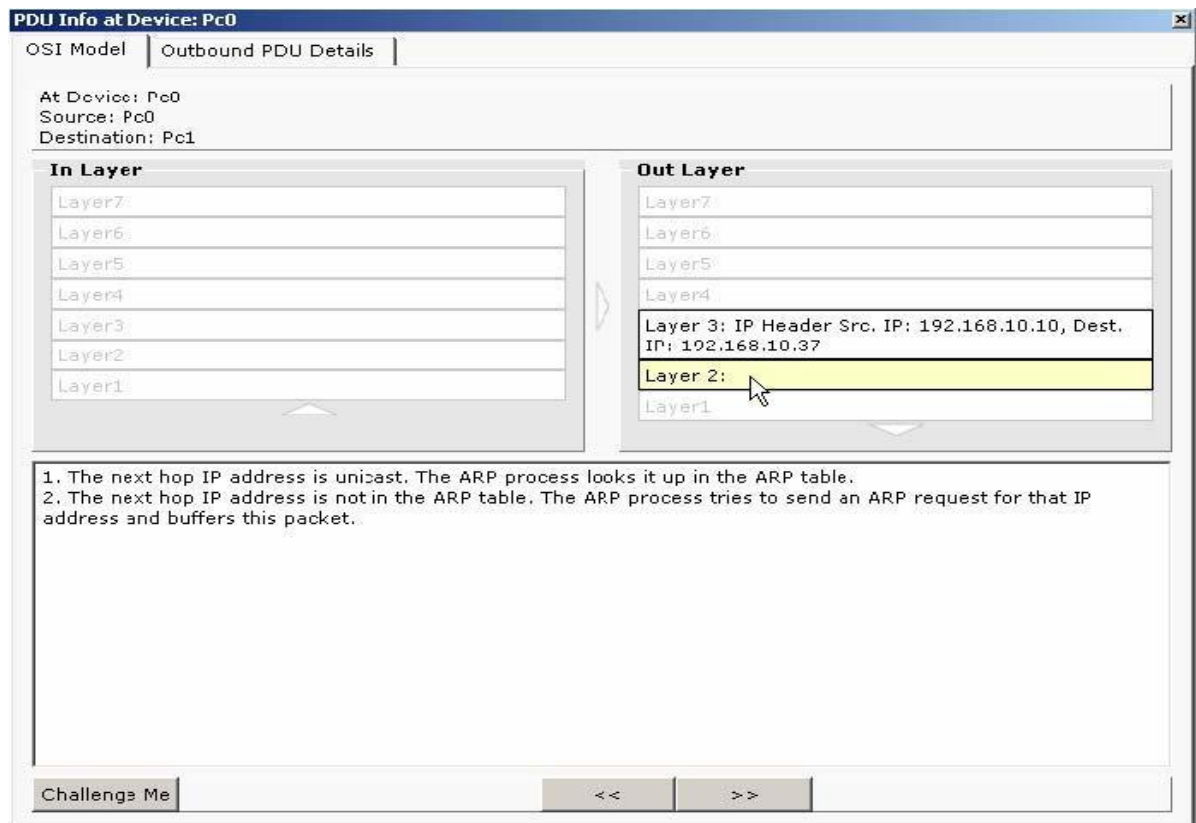
IP

0	4	8	16	19	31	Bits
4		IHL		TOS: 0x0		TL: 0x0
ID: 0x0				FRAG OFFSET: 0x0		
TTL: 32		PRO: 0x1		CHKSUM: 0x0		
SRC IP: 192.168.10.10						
DST IP: 192.168.10.37						
OPT: 0x0				0x0		
DATA (VARIABLE LENGTH)						

ICMP

0	8	16	31	Bits
TYPE: 0x8		CODE: 0x0		CHECKSUM: 0x0

Кликните второй уровень (layer 2) Outbound OSI Model, чтобы посмотреть краткое описание того, что происходит на втором уровне.



Действие:2 Просмотрим на Switch Algorithm и Switch MAC Address таблицы.

Шаг 1: Откройте файл lab1_switch.pkt. Не сохраняйте изменения касающиеся данной сети. Заметьте сходство с предыдущей топологией – hub первого уровня был заменен на switch второго уровня.

Нажмите на иконку **Simulation** для переключения в режим моделирования.

Шаг 2: Просмотр Switch MAC Address таблицы

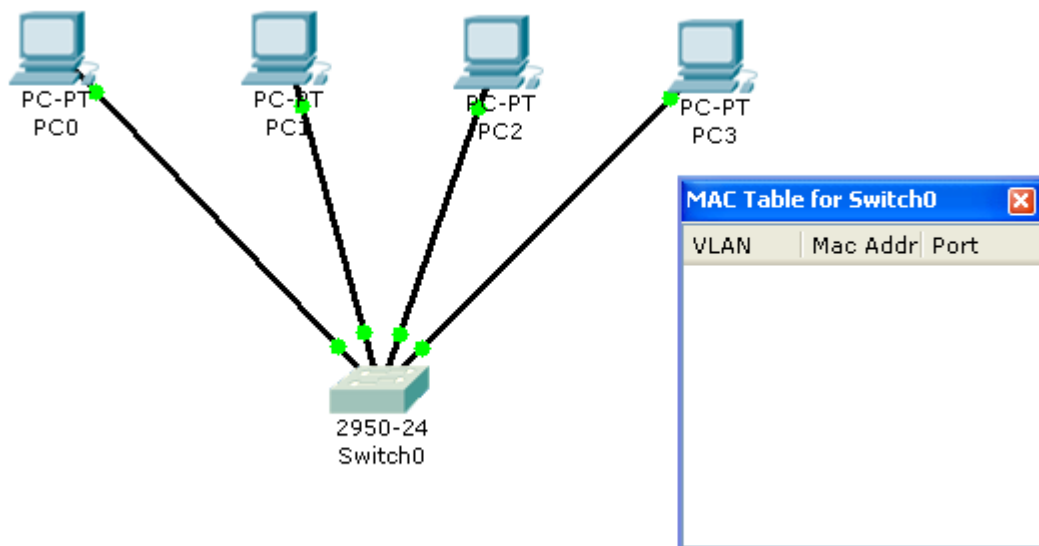
Используйте инструмент **Select** чтобы посмотреть информацию по IP и MAC адресам на различных хостах.



Используйте инструмент **Inspect** чтобы посмотреть таблицу MAC адресов switch'a

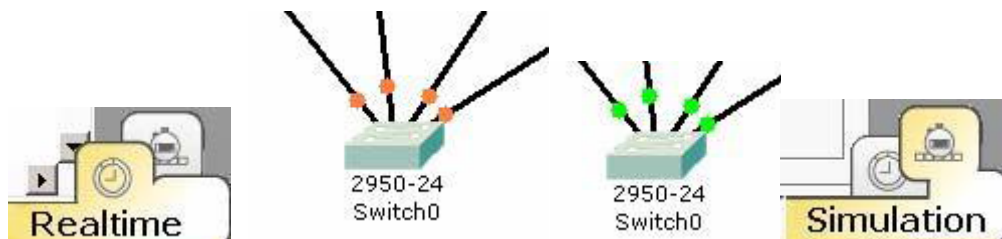


Таблица MAC адресов пуста, поскольку в нее не было внесено ни одного MAC адреса источника.



Ожидание STP

Заметка: Из-за того, как Packet Tracer работает со Spanning Tree Protocol, время от времени свитч может показывать желтые огоньки на своих интерфейсах. Для устранения этого выберите режим **Realtime**, дождитесь, пока цвет сменится на зеленый, затем снова выберите режим **Simulation**.



Шаг 3: Проблема пингования и просмотр таблицы MAC адресов

Установите Event List Filters следующим образом

Event List Filters		
<input checked="" type="checkbox"/> ARP	<input type="checkbox"/> CDP	<input type="checkbox"/> DHCP
<input type="checkbox"/> EIGRP	<input checked="" type="checkbox"/> ICMP	<input type="checkbox"/> RIP
<input type="checkbox"/> TCP	<input type="checkbox"/> UDP	<input type="checkbox"/> All/None

Хост, которому нужно выполнить отображение IP-адреса на локальный адрес, формирует ARP запрос, вкладывает его в кадр протокола канального уровня, указывая в нем известный IP-адрес, и рассылает запрос широкоэвещательно. Все узлы локальной сети получают ARP запрос и сравнивают указанный там IP-адрес с собственным. В случае их совпадения узел формирует ARP-ответ, в котором указывает свой IP-адрес и свой локальный адрес и отправляет его уже направленно, так как в ARP запросе отправитель указывает свой локальный адрес. ARP пакет предшествует ICMP пакету.

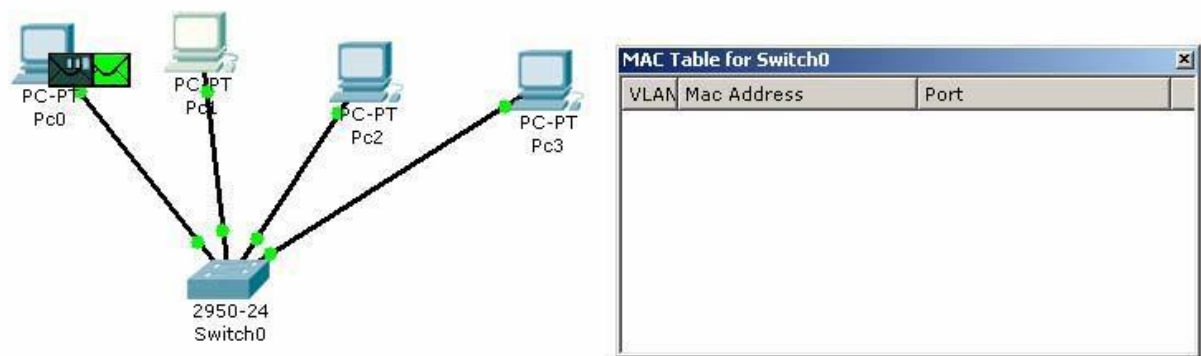
Используя Add Simple PDU осуществите ping с PC0 до PC1. Выберите **Add Simple PDU** из набора инструментов:



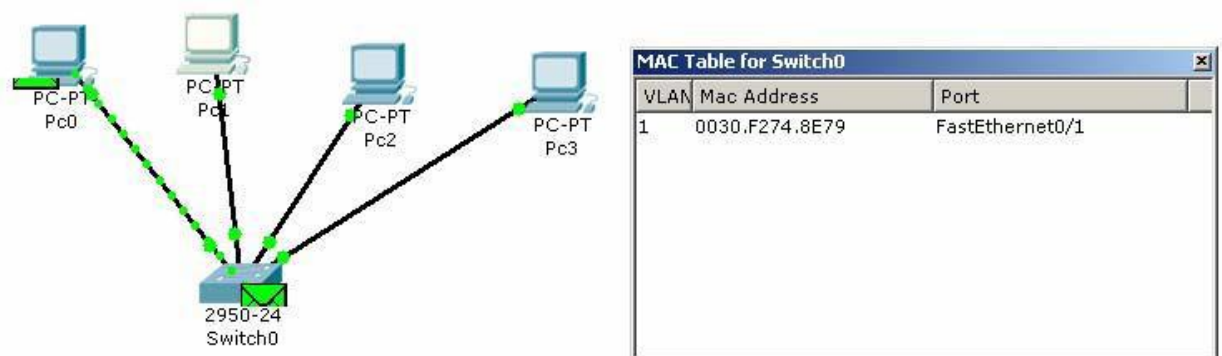
Кликните один раз PC0, устройство, которое осуществляет ping (ICMP эхо запрос и затем кликните один раз PC1 (назначение ICMP эхо запроса)

Включите моделирование используя кнопку Capture / Forward.

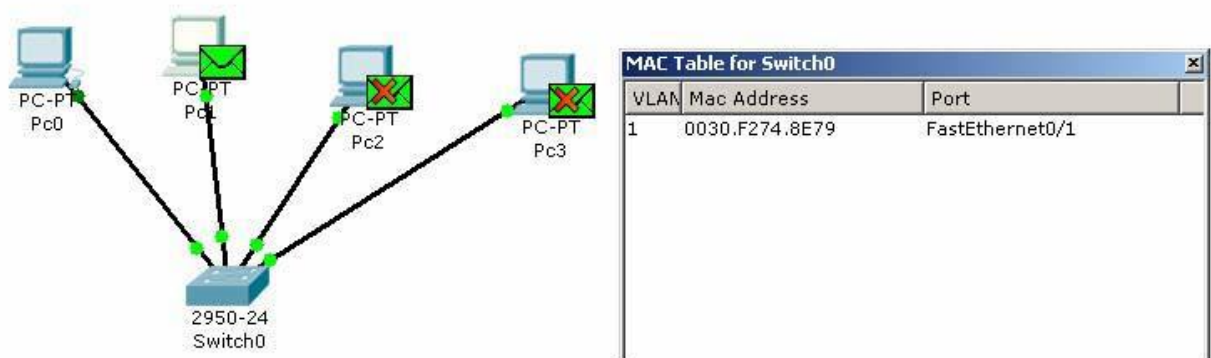
PC0 посылает кадр, который содержит ARP запрос на Switch0



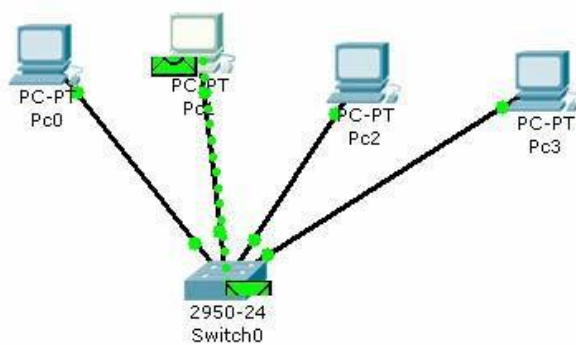
Заметьте, как Switch узнает MAC адрес отправителя из кадра.



Пакет рассылается по всем портам, потому что таблица MAC адресов свитча не содержит адреса назначения Ethernet кадра. PC2 и PC3 игнорируют кадр:

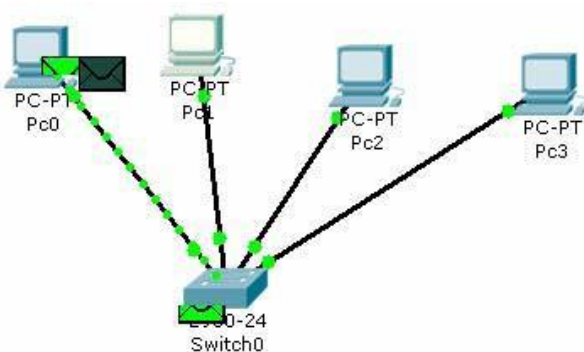


PC1 возвращает ARP ответ. Теперь Switch0 узнает MAC адрес PC1



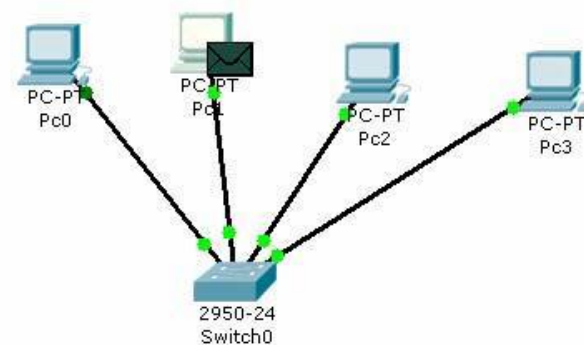
VLAN	Mac Address	Port
1	0001.C798.4163	FastEthernet0/2
1	0030.F274.8E79	FastEthernet0/1

Поскольку MAC адрес отправителя (PC0) свитч узнал раньше, при поиске MAC адреса получателя кадра Switch0 отфильтрует кадр, отсылая его только на FastEthernet port 0/1



VLAN	Mac Address	Port
1	0001.C798.4163	FastEthernet0/2
1	0030.F274.8E79	FastEthernet0/1

Остальные кадры с IP пакетами включающими ICMP эхо запросы с PC0 к PC1 и кадры с IP пакетами включающими ICMP эхо ответы с PC1 к PC0 фильтруются свитчем и отправляются только на нужный интерфейс (порт).



VLAN	Mac Address	Port
1	0001.C798.4163	FastEthernet0/2
1	0030.F274.8E79	FastEthernet0/1

Шаг 4 Создание собственных топологий.

Что бы приступить к созданию своей сети, откройте вкладку File и выберете New. Затем обратите внимание на левый нижний угол окна программы. В крайнем левом окошке Вы увидите набор компонентов, доступных для создания сети. Для большей конкретизации намерений воспользуйтесь окошком правее. Что бы добавить элемент, кликните один раз на него, затем один раз в окне программы, предназначенном для создания и моделирования сетевых топологий. Затем свяжите добавленные компоненты, пропишите необходимые параметры. Посмотрите, как это сделано в ранее рассмотренной топологии.

Лучшим способом изучения нового программного обеспечения является экспериментирование. Попробуйте различные инструменты, посмотрите на разные протоколы с помощью Event List и Info box. Также используйте Help и Tutorials.