

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

ОТЧЕТ

ПО ЛАБОРАТОРНОЙ РАБОТЕ № 1

Знакомство с Cisco Packet Tracer

дисциплина: Администрирование локальных систем

Студенты: Нгуен Дык Ань

Номер: 1032215251

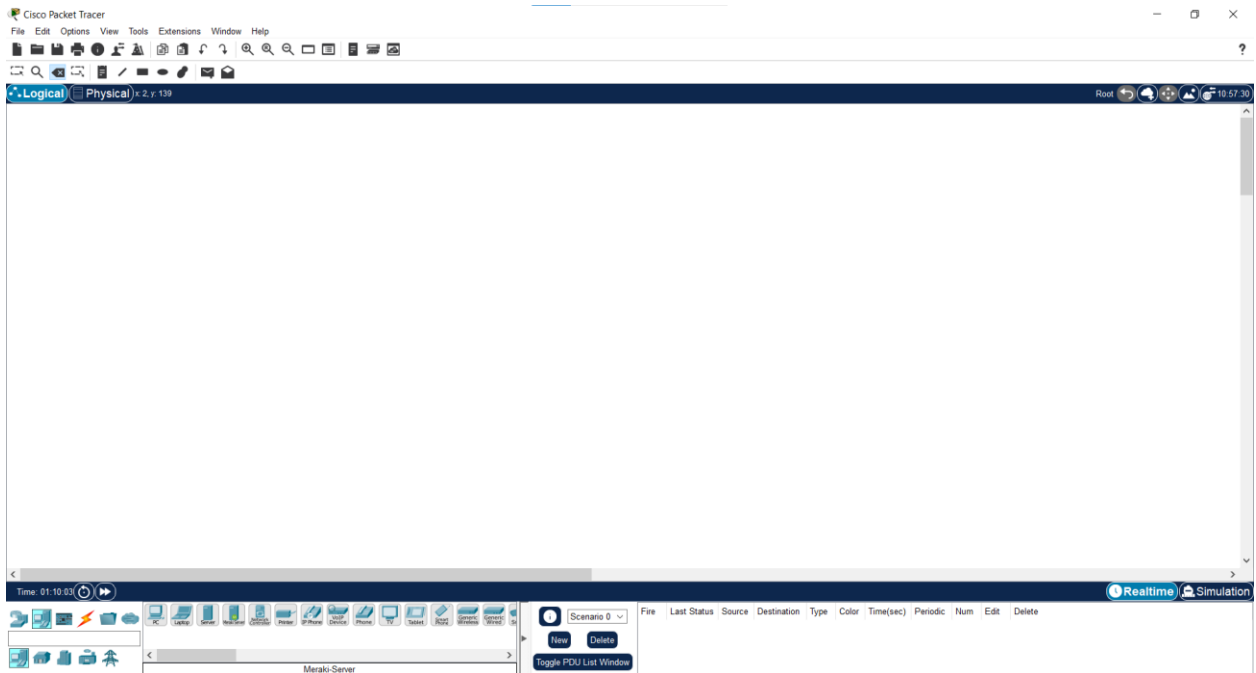
Группа: НКНбд-01-21

МОСКВА

2024

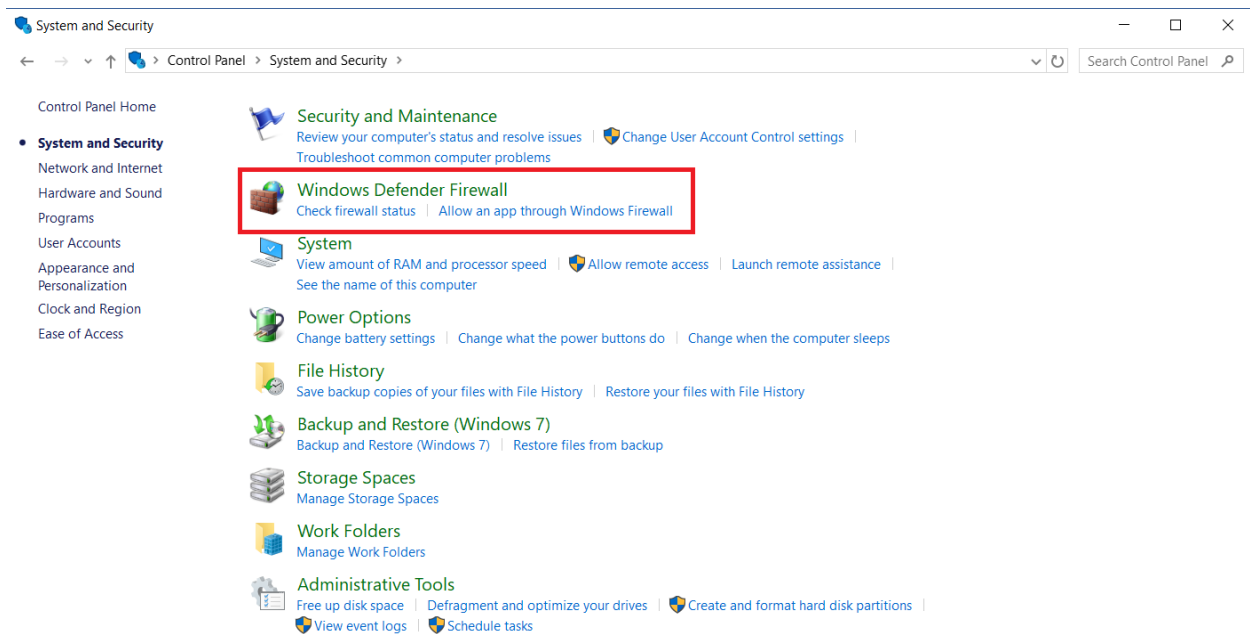
Задание 1: Установить Cisco Packet Tracer на устройстве

- Установить Cisco Packet Tracer.

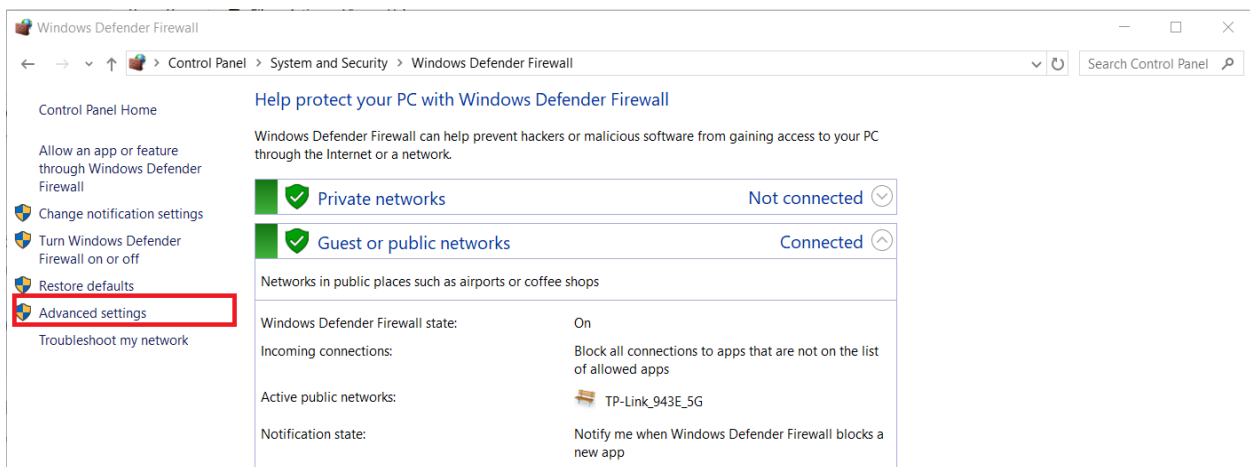


(рис. Интерфейс Cisco Packet Tracer)

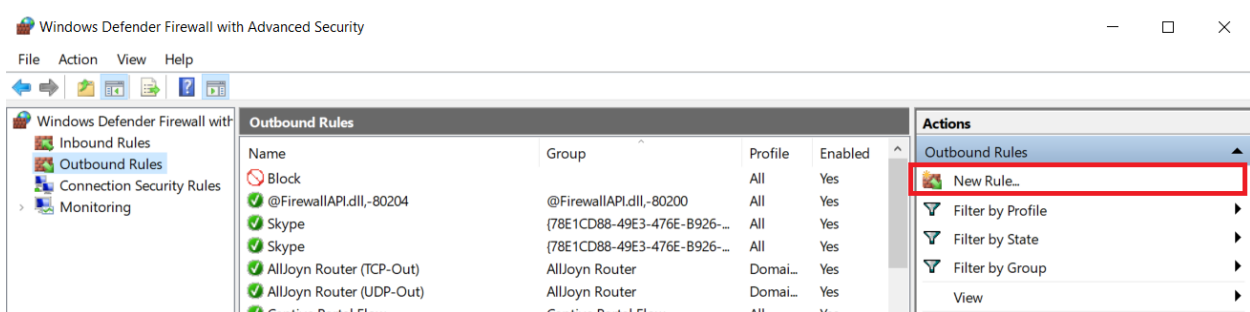
- После установки надо блокировать доступ в Интернете для Cisco Packet Tracer, чтобы пропустить аутентификацию, когда мы запустим Packet Tracer
- Открыть “Control Panel”, в разделе “System and Security” выбрать “Window Defender Firewall”



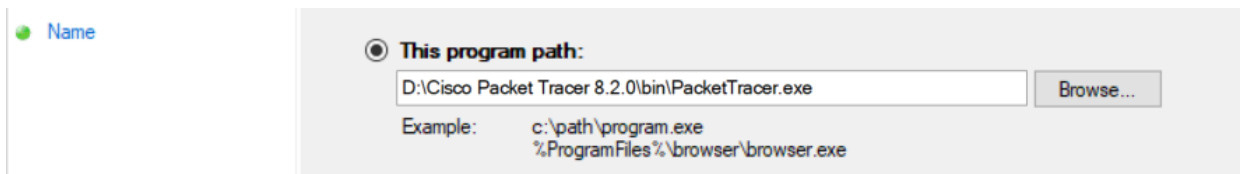
- После этого выбрать “Advanced Settings”, и открывается новое окно.



- Потом в разделе “Outbound Rules” выбрать “New Rule”



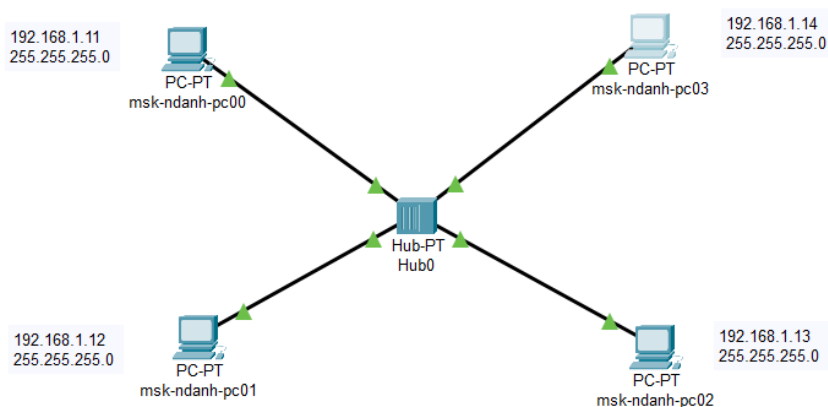
- В новом окне выбрать тип правила – “Program”, потом поставить путь программы Packet Tracer на это разделе.



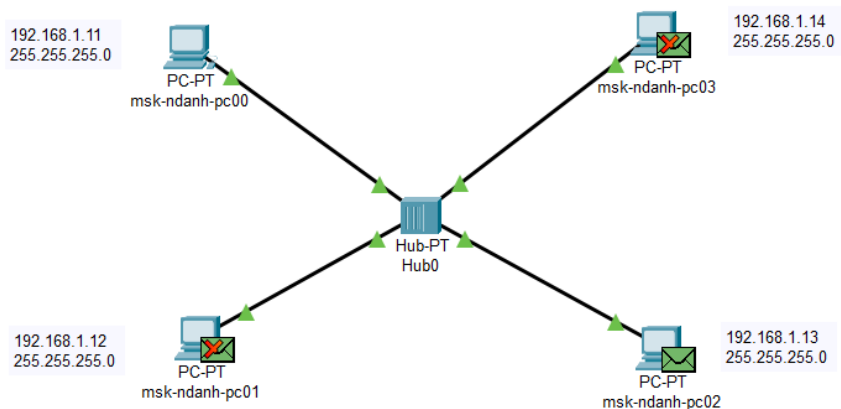
- Потом выбрать “Block the connection” действие, и это правило применяется при подключении к своему корпоративному домену, к частной сети и к общедоступной сети.
- После этих шагов, мы успешно запустим Packet Tracer без аутентификации.

Задание 2: Построить простейшую сеть, провести простейшую настройку оборудования в Cisco Packet Tracer

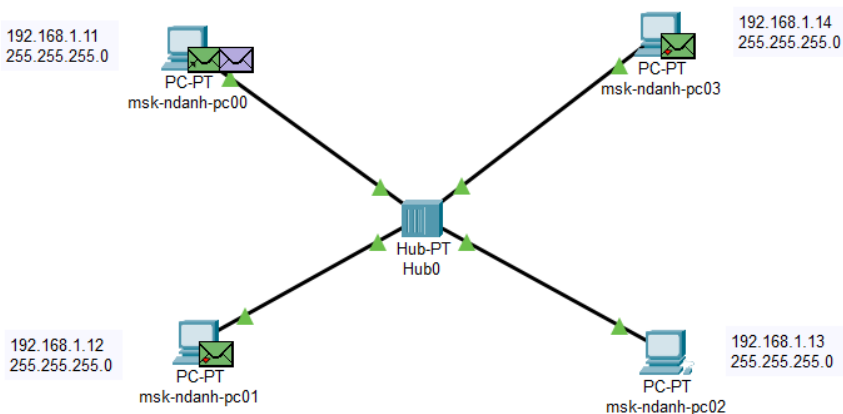
- Создать новый проект, и в рабочем пространстве разместить концентратор и 4 оконечных устройства, как на рисунке



- Попробовать присылать пакеты ARP, ICMP между оконечными устройствами, здесь я отправляю пакеты от устройства pc00 устройству pc02. Пакеты двигается от устройства pc00 и останавливается в хабе, и отсюда пакеты были отправлены устройствам pc01, pc02, pc03. Поскольку целевой IP-адрес запроса соответствует IP-адресу принимающего порта (устройство pc02), поэтому другие устройства удалили кадр, а только устройство pc02 принимал пакеты (рис. 1), и ответный пакеты только от устройства pc02 двигается в хабе, и от хаба ответный пакеты отправлен устройствам pc00, pc01, pc03. И только устройство pc00 принимал пакеты (рис. 2).



(рис. 1)

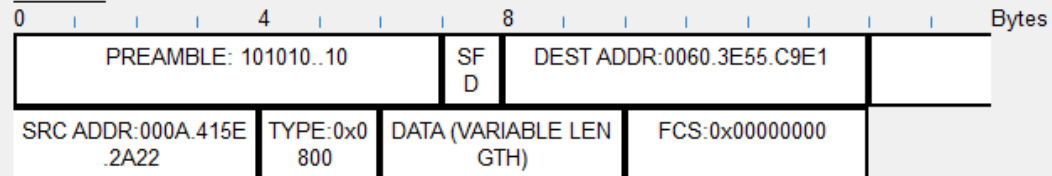
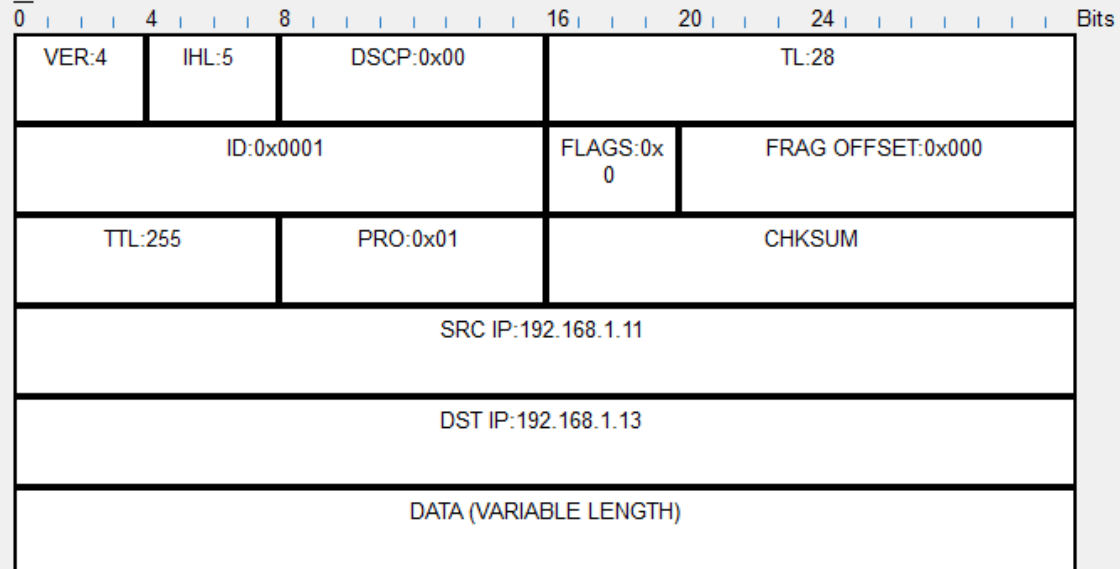
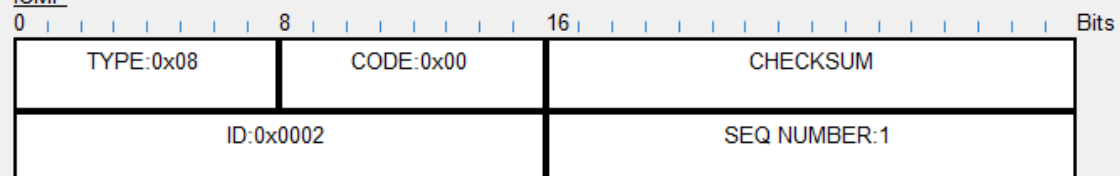
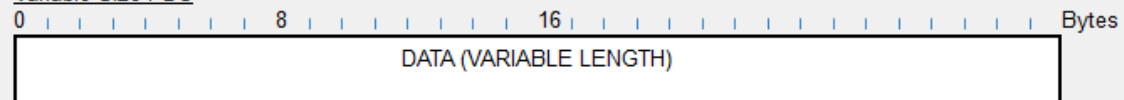


(рис. 2)

- Анализируем информации о PDU (рис 3):
 - Как мы видим на , заголовок ICMP-сообщения состоит из 64 бит:
 - Type (8 бит) – числовой идентификатор типа сообщения: 0 или 8, на тип – это 8, то это запрос ICMP (если 0, то это ответ ICMP)
 - Code (8 бит) – числовой идентификатор, более точно определяющий тип ошибки, здесь код – это 0, то нет ошибки
 - контрольная сумма (16 бит) – вычисляется для всего ICMP-сообщения
 - Оставшиеся 32 бит и поле данных зависит от значений полей типа и кода
 - Структура кадра Ethernet состоит из 7 полей, которая может изменяться от 72 до 1526 байт

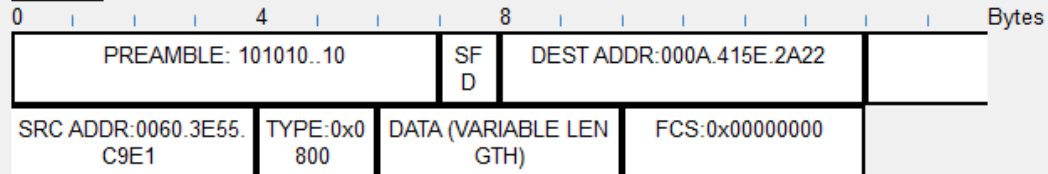
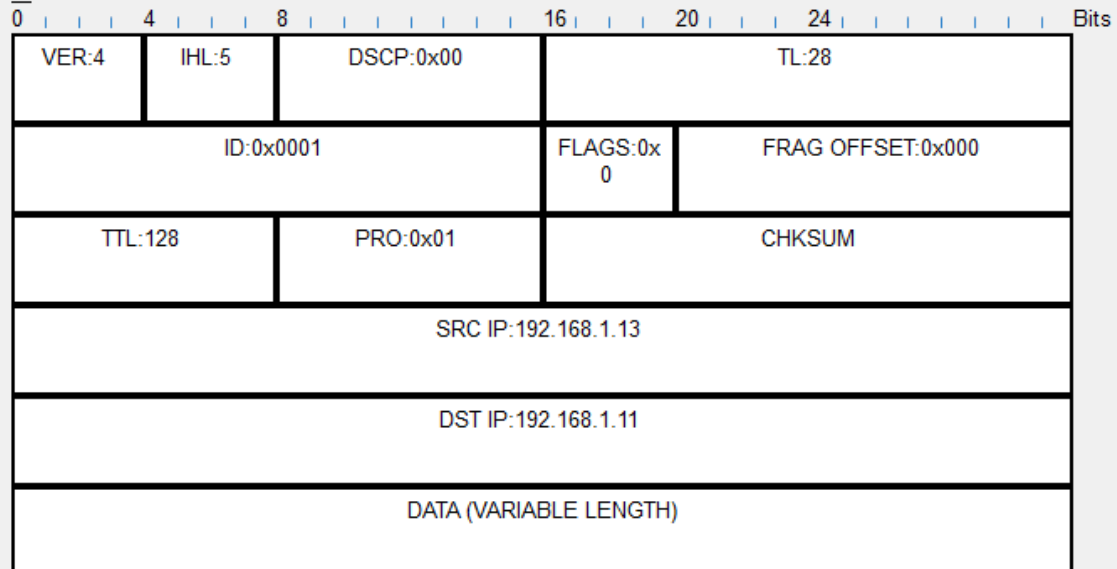
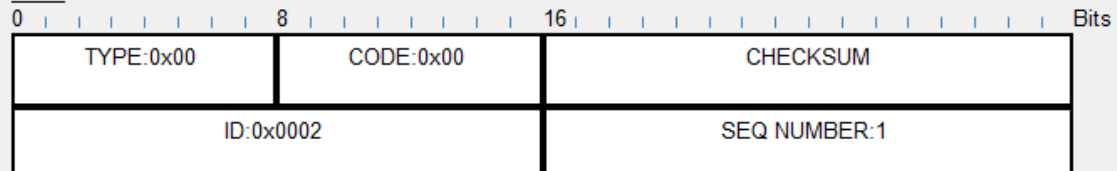
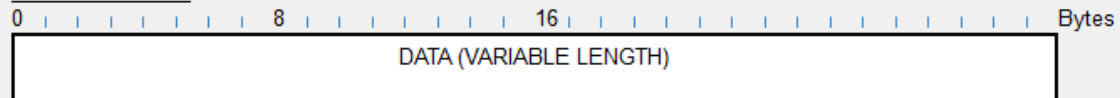
- Preamble: Имеет значение 10101010, первые 7 байт преамбулы служат для пробуждения принимающих адаптеров и синхронизации их часов с часами отправителя.
 - SDF (Start-Frame Delimite): Это 1-байтовое поле, для которого всегда установлено значение 10101011. SFD указывает, что последующие биты начинают кадр, который является адресом назначения.
 - Конечный MAC-адрес: Поле из шести байт, содержащее адрес конечного узла. Адрес получателя - может быть длиной 2 или 6 байт (MAC-адрес получателя). Первый бит адреса получателя - это признак того, является адрес индивидуальным или групповым: если 0, то адрес указывает на определенную станцию, если 1, то это групповой адрес нескольких (возможно всех) станций сети (здесь мы получим 0 - то адрес указывает на определенную станцию)
 - Исходный MAC-адрес: Поле из 6 байт, содержащее адрес исходного узла. Адрес отправителя- 2-х или 6-ти байтовое поле, содержащее адрес станции отправителя
 - Type: Поле типа позволяет распознавать множество протоколов, которые могут передаваться через Ethernet, будь то IPv4, ARP, IPv6, IPX, AppleTalk и т. д. (здесь это тип 0x0800 – IPv4)
 - Data: Данные пакета
 - FCS (Frame Check Sequence): Поле, содержащее четыре контрольных байта, сгенерированных кодом циклического контроля избыточности. Поле FCS используется для обнаружения ошибок в данных, содержащихся в кадре
- Сравниваем информации в кадре Ethernet при передвижении пакета (рис. 3 и рис. 4), мы видим Исходный MAC-адрес и Конечный MAC-адрес были инвертированными.

PDU Formats

EthernetIIIPICMPVariable Size PDU

(рис. 3)

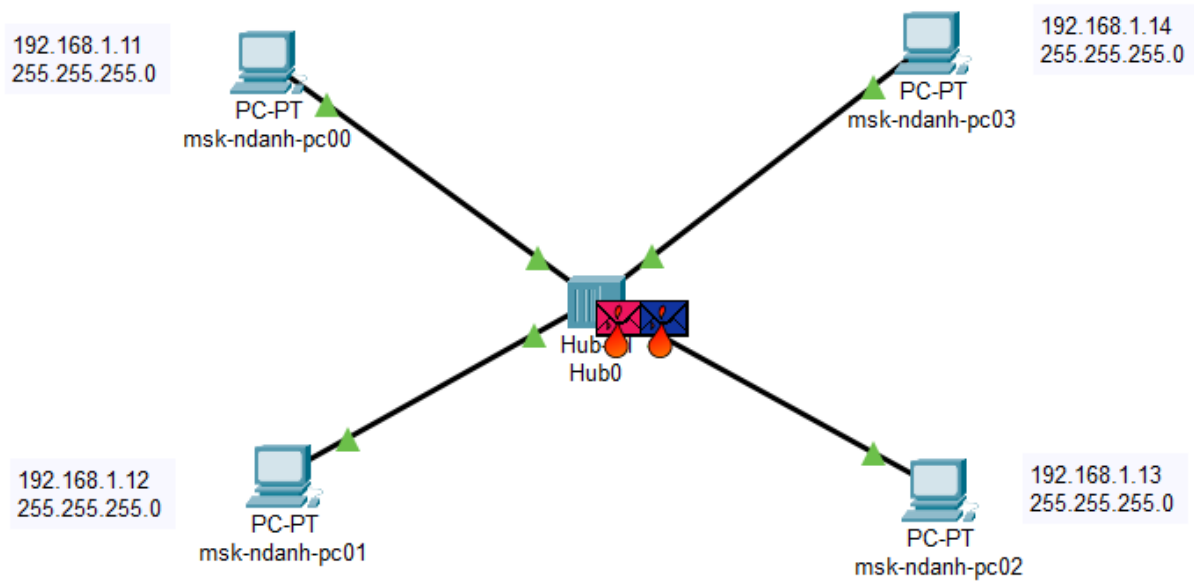
PDU Formats

EthernetIIIPICMPVariable Size PDU

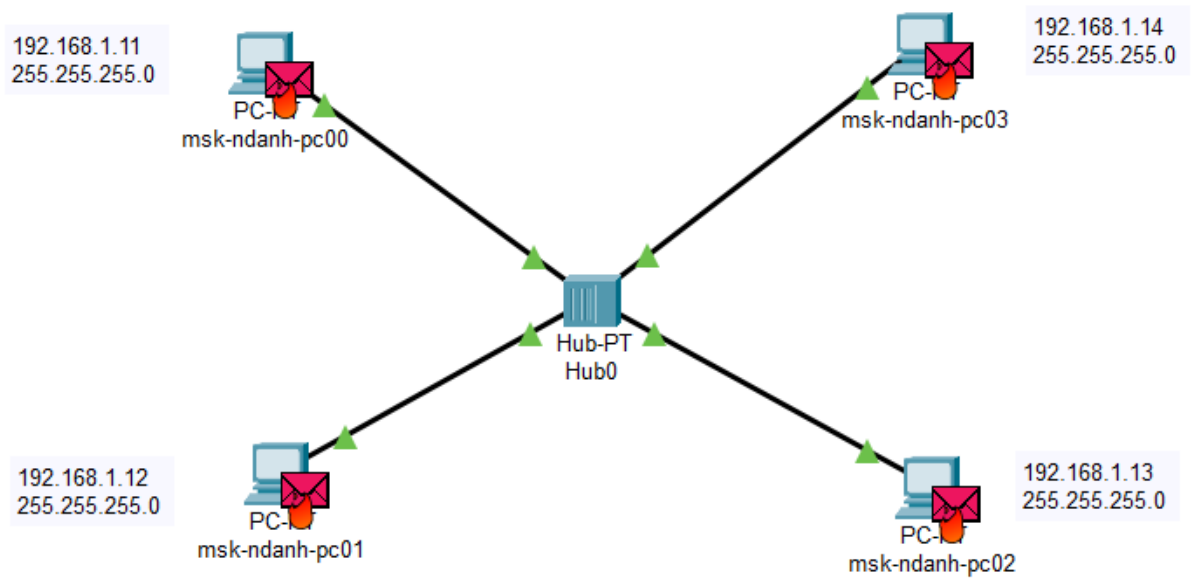
(рис. 4)

- В проекте мы отправляем пакет от устройства pc00 устройству pc02 и наоборот, от устройства pc02 устройству pc00. Как мы видим, пакеты двигаются от устройств в хаб, и производит коллизия (рис. 5), потом

пакеты отправятся от хаба всем устройствам, и ни одного устройства получит данные пакетов (рис. 6).



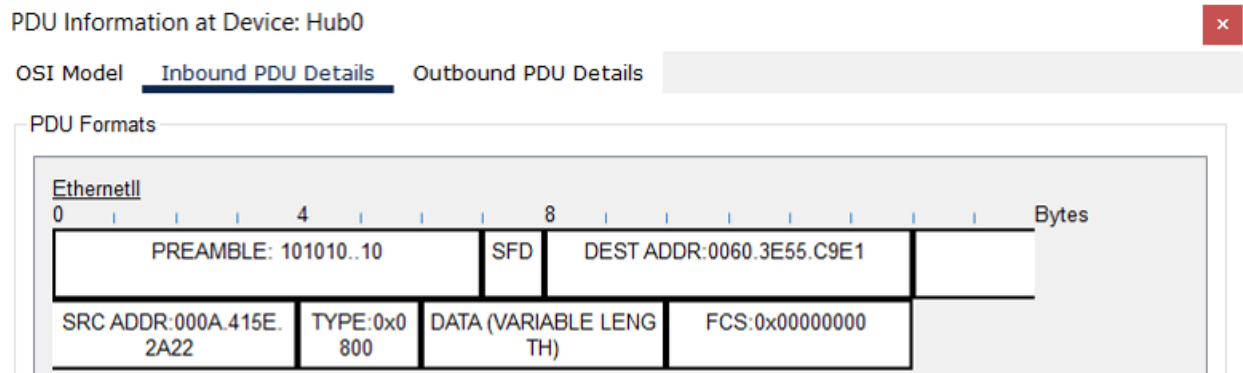
(рис. 5)



(рис. 6)

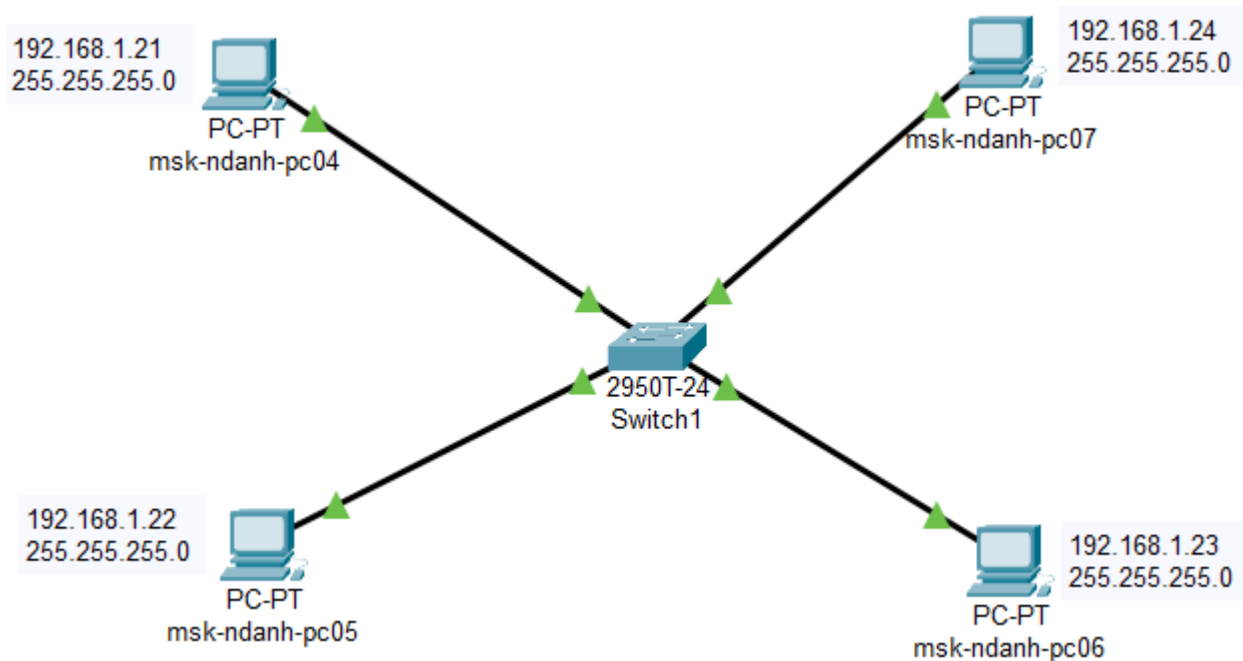
- Анализируем событие коллизии между пакетами:

Мы видим на информации о PDU (рис. 7), видно, что обо пакета имеют тип 8 – запрос пакет, то обе устройства в режиме “отправить пакет”, и поскольку устройства не получают данные пакета, устройства сбрасывают кадр.



(рис. 7)


- Создать сеть, состоящая из 4 оконечных устройства и коммутатора, как на рис. 8.



(рис. 8)

- Попытать отправить пакеты от устройства pc04 устройству pc06, на рис. 9, мы можем видеть процесс движения пакетов, пакет ARP от pc04

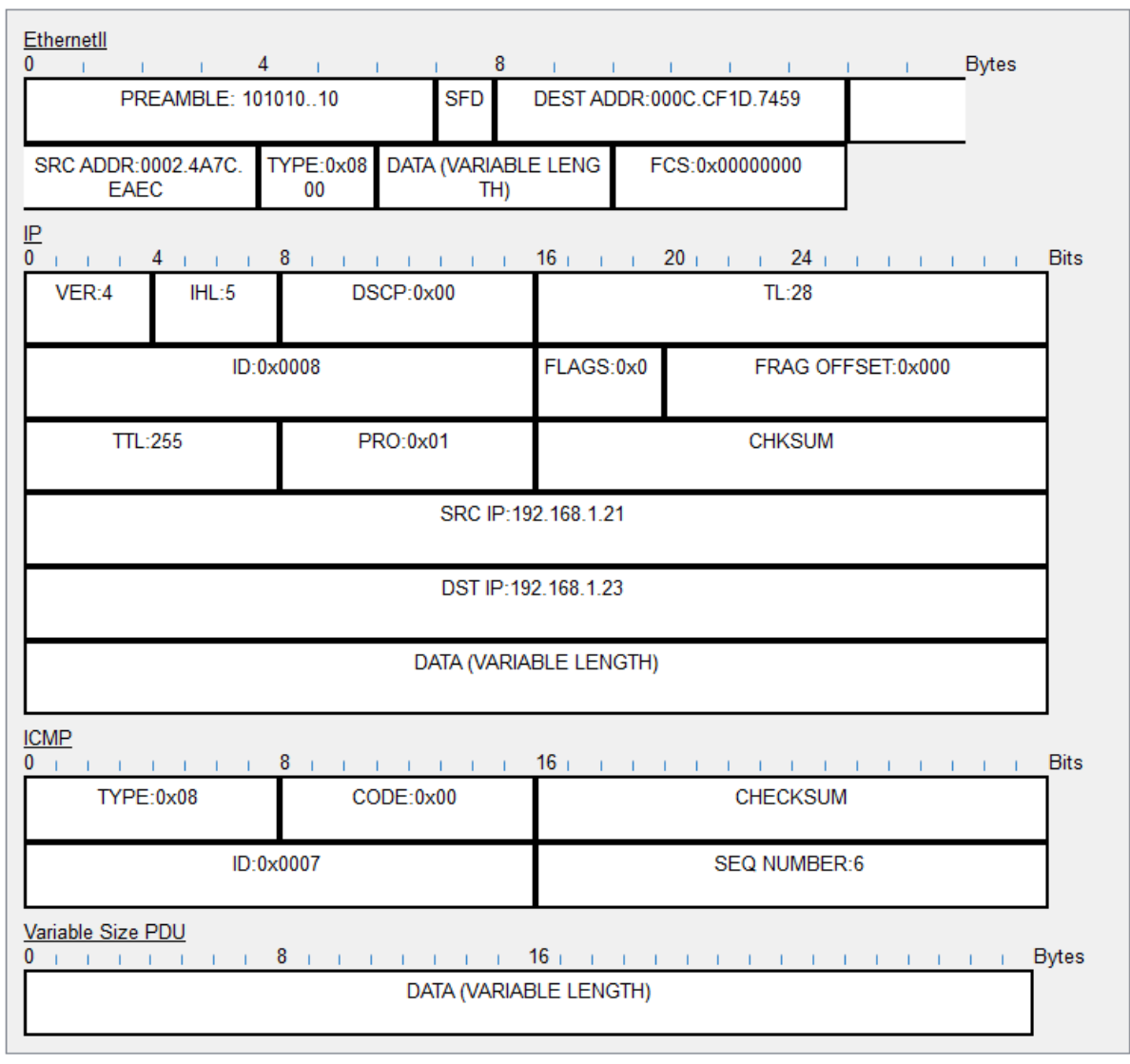
двигается в коммутатор, и отсюда пакеты отправят всем устройствам, и от pc06 пакет движется в коммутатор и прямо отправляет устройству pc04. Пакет ICMP отправляет от устройства pc04 коммутатору и от коммутатора устройству pc06 и наоборот

Event List				
Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	msk-ndanh-pc04	ICMP
	0.000	--	msk-ndanh-pc04	ARP
	0.001	msk-ndanh-pc04	Switch1	ARP
	0.002	Switch1	msk-ndanh-pc07	ARP
	0.002	Switch1	msk-ndanh-pc05	ARP
	0.002	Switch1	msk-ndanh-pc06	ARP
	0.003	msk-ndanh-pc06	Switch1	ARP
	0.004	Switch1	msk-ndanh-pc04	ARP
	0.004	--	msk-ndanh-pc04	ICMP
	0.005	msk-ndanh-pc04	Switch1	ICMP
	0.006	Switch1	msk-ndanh-pc06	ICMP
	0.007	msk-ndanh-pc06	Switch1	ICMP
	0.008	Switch1	msk-ndanh-pc04	ICMP
	1.997	--	Switch1	STP

(рис. 9)

- Анализируем информации о PDU (рис. 10):
 - Заголовок ICMP:
 - Type – это 8, то это запрос ICMP
 - Code – это 0, то нет ошибки
 - Структура кадра Ethernet:
 - MAC-адрес: Первый бит адреса – это 0 - то адрес указывает на определенную станцию
 - Type: 0x0800 – это IPv4

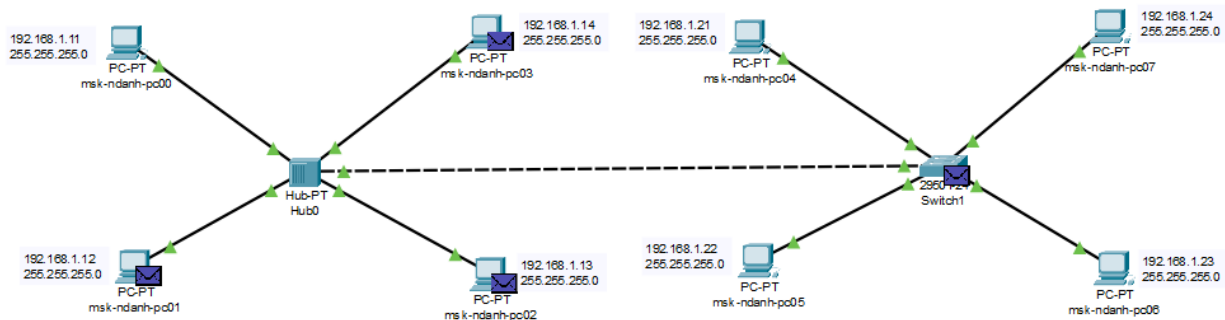
PDU Formats



(рис. 10)

- В ситуации 2 устройства пытаются отправить данные по одному и тому же общему каналу одновременно, коллизия не бывает. Потому что, каналы с коммутаторами являются полнодуплексными, без общих каналов. Поэтому коллизия невозможно.
- В ситуации мы соединим 2 простых сети и попытаем отправить данные между 2 устройствами одновременно, сначала возникает коллизия, но и потом успешно достигают пункта назначения. Потому что, коммутатор

отключается на случайный период времени перед повторной передачей кадра в буфер.



Контрольные вопросы:

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

a. Определение:

- Концентратор (Hub): Это устройство, которое в кабельной сети, построенной по топологии «звезда», принимает на порт пакеты данных и передает его далее на все остальные порты.
- Коммутатор (Switch): Это устройство, предназначенное для соединения нескольких узлов компьютерной сети в пределах одного или нескольких сегментов сети.
- Маршрутизатор (Router): Это устройство, которое соединяет вычислительные устройства и сети с другими сетями.
- Шлюз (Gateway): Это сетевое устройство, которое соединяет несколько сетей и выполняют функции маршрутизации пакетов.

b. Использование каждого типа сетевого оборудования зависит от конкретных потребностей сети:

- Концентраторы обычно используются в небольших сетях, где нет необходимости в высокой пропускной способности и нет требований к сетевому управлению.
- Коммутаторы предпочтительны в средних и больших сетях, где требуется высокая скорость передачи данных, доставка только на нужные порты и улучшенное управление сетью.

- Маршрутизаторы используются для соединения сетей различных протоколов и обеспечения передачи данных между ними.
- Шлюзы используются для связи между локальной сетью и другими сетями, такими как Интернет или другие удаленные сети.

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

- IP-адрес: Это уникальный идентификатор, присваиваемый каждому устройству, подключенному к сети, для обеспечения их идентификации и связи в сети.
- Сетевая маска: Это числовой параметр, используемый вместе с IP-адресом для определения размера сети и идентификации сети и хостов внутри нее.
- Broadcast-адрес: Это специальный IP-адрес, который используется для отправки данных одновременно на все устройства в конкретной сети.

3. Как можно проверить доступность узла сети?

Для проверки доступности узла в сети можно использовать различные методы:

- Пинг (Ping): Это команда, которая отправляет небольшие пакеты данных на устройство в сети и ждет ответа. Если получен ответ, значит узел доступен.
- Traceroute: Это команда, которая позволяет отследить маршрут следования пакетов данных до указанного узла в сети, показывая промежуточные узлы и время передачи данных до каждого из них.
- Проверка соединения на порт с помощью утилит, таких как Telnet или nc (netcat), которые могут проверить доступность определенного порта на удаленном узле.