МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное
учреждения высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«___» _____ 2017 г.

АНАЛИЗАТОРЫ СЕТЕВЫХ ПРОТОКОЛОВ

Методические указания к практической работе
для студентов укрупненной группы специальностей и
направлений подготовки 10.00.00 «Информационная безопасность»

Курск 2017

УДК 621.(076.1)

Составитель: М.О. Таныгин

Рецензент

Кандидат технических наук, доцент кафедры
«Информационная безопасность» И.В. Калуцкий

Анализаторы сетевых протоколов [Текст] : методические указания к практической работе/ Юго-Зап. гос. ун-т; сост.: М.О. Таныгин. – Курск, 2017. – 20 с.: ил. 13, табл. 2. – Библиогр.: с. 9.

Содержат сведения по вопросам практической работы по основам мониторинга безопасности инфокоммуникационных систем и сетей. Указывается порядок выполнения практической работы, правила оформления отчета.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по специальности.

Предназначены для студентов укрупненной группы специальностей и направлений подготовки 10.00.00 «Информационная безопасность».

Текст печатается в авторской редакции

Подписано в печать 24.11.17 Формат 60x84 1/16.
Усл.печ. л. 1,16. Уч.-изд. л. 1,05. Тираж 100 экз. Заказ. Бесплатно. 2145
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

Программное обеспечение, способное выполнять анализ проходящих через сетевой интерфейс кадров и переносимых в них пакетов сетевых протоколов, называется *анализаторами сетевых протоколов* и представляет собой один из часто используемых инструментов администратора компьютерной сети. Работа анализаторов основывается на использовании так называемого "*неразборчивого*" (*promiscuous*) режима работы сетевого интерфейсного адаптера, который позволяет захватывать и анализировать сетевые кадры и пакеты, отсылаемые и получаемые не только станцией, на которой работает программа, но и другими станциями сети. Примерами такого рода программ могут быть *tcpdump* фирмы Network Research Group, *Sniffer Pro* фирмы Network Associated Inc., *Сетевой Монитор* фирмы Microsoft, входящий в состав еѐ серверных операционных систем, и ряд других. Мы рассмотрим работу анализаторов сетевых протоколов на примере бесплатного кроссплатформенного программного обеспечения *Wireshark*, разработанного группой программистов и доступного для загрузки по адресу http://www.wireshark.org.

На рис. 1 приведен интерфейс программы с несколькими захваченными пакетами, высылаемыми утилитой ping. В верхней части окна перечислены захваченные пакеты с указанием их основных свойств: порядкового номера в захваченной последовательности, относительного времени захвата, сетевых адресов отправителя и получателя, типа протокола и общей информации о пакете. В средней части отображаются структуры данных сетевых протоколов различных уровней модели OSI, которые переносят свои данные в выделенном в верхнем окне пакете. Развернув уровни, можно увидеть детальное описание полей заголовка сетевого протокола, работающего на этом уровне. В нижней части выводится дамп пакета в виде байтовых значений в шестнадцатеричной системе исчисления и соответствующих этим значениям US-ASCII-кодов в правой части области дампа. Поэтому, если в пакете передаѐтся пользовательский текст на английском языке, то он будет здесь отображаться, символы второй половины таблиц ASCII (куда входят и русские буквы) отображаются точками.

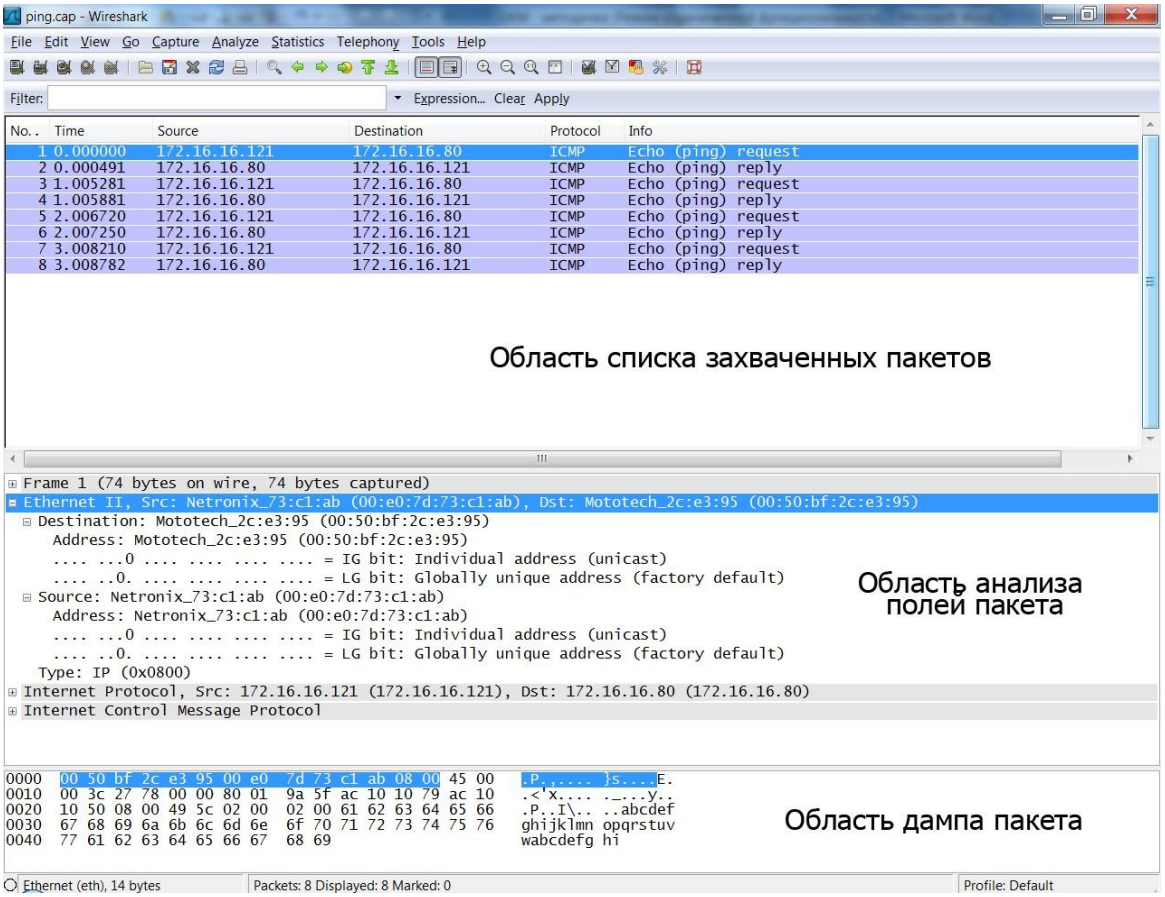

Рис. 1. Интерфейс анализатора сетевых протоколов Wireshark

При выделении в области анализа полей пакета какого-либо заголовка или поля в области дампа выделяются соответствующие ему данные. Так на рис. 1 выделен заголовок кадра канального уровня Ethernet, анализатор распознал формат этого кадра (Ethernet II) и выполнил подробный анализ полей заголовка этого кадра. В области дампа при этом выделены 14 байт, соответствующие структуре заголовка Ethernet II (DIX). Следует отметить, что первая строка области анализа полей пакета (Frame 1 (74 bytes on wire, 74 bytes captured) на рис. 1) не отображает какой-либо уровень стека протоколов, а содержит общую информацию о пакете: длину, время захвата, относительные времена и т.д. Захват кадров осуществляется командой Capture-Start и Capture-Stop (или соответствующими кнопками на Панели инструментов).

Исследование протокола разрешения адреса ARP

Изучение типов MAC-адресов в заголовках кадров Ethernet может быть выполнено путѐм захвата кадров, переносящих данные *протокола разрешения адреса* (*Address Resolution Protocol – ARP*), выполняющего отображение IP-адреса сетевого интерфейса на его адрес MAC-адрес. Проблема заключается в том, что когда высылается пакет по указанному в качестве параметра IP-адресу получателя (например, командой ping 192.168.2.1), отправителю (например, с IP-адресом (SA IP) 192.168.2.2 и MAC-адресом (SA MAC) 00-A0-C9-83-16-16) необходимо сформировать кадр Ethernet с заполнением адресных полей заголовков канального и сетевого уровней. IP и MAC-адрес отправителя могут быть заполнены, поскольку они известны сетевому интерфейсу отправителя, IP-адрес получателя заполняется значением параметра команды `ping`. А вот MAC-адрес получателя в общем случае для отправителя является неизвестным (рис. 2).

DA MAC	SA MAC	SA IP	DA IP	
???	00-A0-C9-83-16-16	192.168.2.2	192.168.2.1	Данные пакета

Рис. 2. Адресная информация в заголовках канального и сетевого уровня при отправке пакета по указанному IP-адресу

Выяснением MAC-адреса получателя занимается протокол ARP, устанавливаемый автоматически вместе со стеком TCP/IP. Он формирует и высылает в сеть ARP-запрос в поле данных широковещательного кадра Ethernet (то есть кадра с широковещательным MAC-адресом получателя FF-FF-FF-FF-FF-FF_H). В запросе указывается IP-адрес интерфейса, чей MAC-адрес выясняется. Широковещательный кадр получают все компьютеры локальной сети, однако ARP-ответ высылается в кадре с индивидуальным (однопунктовым) адресом получателя только компьютером, распознавшим свой IP-адрес в запросе (рис. 3). После получения ответа отправитель заполняет поле MAC-адрес получателя в кадре с пакетом утилиты

ping (рис. 2) и высылает его в сеть.

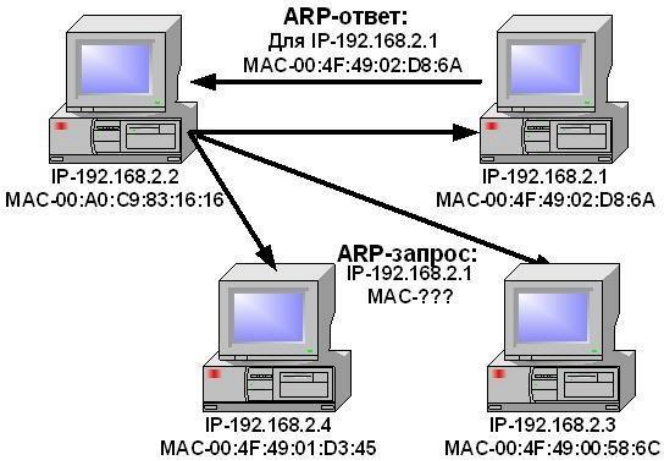

Рис. 3. Модель работы ARP

Соответствие "IP-адрес MAC-адрес" сохраняется в памяти компьютера-отправителя пакета в так называемой ARP-таблице (или ARP-кэше). При необходимости повторной высылки пакета по имеющемуся в таблице адресу широковещательный запрос не рассылается. Командой arpa можно просмотреть содержимое этой таблицы (рис. 4).

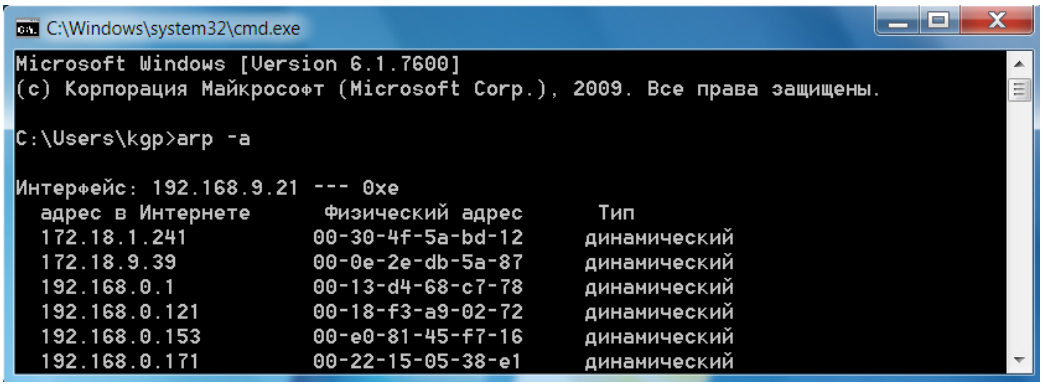

Рис. 4. Пример ARP-таблицы

На рис. 5 приведена структура кадра Ethernet с запросом/ответом ARP. Следует отметить, что рассылка широковещательных сообщений обычно производится только в пределах локальной сети (точнее сегмента сети с компьютерами с одинаковой частью сетевых адресов). Это важно, поскольку широковещательный трафик при большом количестве компьютеров сети может занимать значительную часть полосы

пропускания сети. Динамические записи создаются модулем ARP с использованием широковещательных рассылок, статические – вручную администратором командой arp -s IP-адрес MAC-адрес. Динамические записи в таблице периодически удаляются (обычно через пять минут), поскольку существует вероятность изменения IP-адресов сетевых интерфейсов, статические остаются неизменными в течение сеанса работы системы. Существует также протокол *реверсивный протокол разрешения адреса* (*Reverse Address Resolution Protocol – RARP*), решающий задачу нахождения IP-адреса по известному адресу канального уровня. Он используется при старте бездисковых рабочих станций, не знающих в этот момент своего IP-адреса, но знающих MAC-адрес.

DA	SA	T	MT	PT	MAL	PAL	OC	SMA	SPA	TMA	GPA	Pad	FCS
6	6	2	2	2	1	1	2	6	4	6	4	18	4

ARP-запрос			ARP-ответ		
Поле	Расшифровка	Значение (hex)	Примеч.	Значение (hex)	Примеч.
DA	Destination Address	FF:FF:FF:FF:FF:FF	широковещательный	00:A0:C9:83:16:16	MAC источника ARP-запроса
SA	Source Address	00:A0:C9:83:16:16	MAC отправителя	00:4F:49:02:D8:6A	MAC отправителя
T	Type	0806	ARP	0806	ARP
MT	Media Type	0001	Ethernet	0001	Ethernet
PT	Protocol Type	0800	IP	0800	IP
MAL	Media Address Length	06	байт (MAC)	06	байт (MAC)
PAL	Protocol Address Length	04	байта (IP)	04	байта (IP)
OC	Operation Code	0001	ARP-запрос	0001	ARP-ответ
SMA	Sender Media Address	00:A0:C9:83:16:16	MAC отправителя	00:4F:49:02:D8:6A	MAC отправителя
SPA	Sender Protocol Address	192.168.2.2	IP отправителя	192.168.2.1	IP отправи- теля
TM	Target Media	00:00:00:00:00:00	текущая подсеть	00:A0:C9:83:16:16	MAC полу-

A	Address				чателя
GPA	Get Protocol Address	192.168.2.1	IP получателя	192.168.2.2	IP получат е- ля
Pad	Padding	00 - 18 байт	дополнение кадра до 64 байт	00 - 18 байт	дополне ние кадра до 64 байт
FCS	Frame Check Sequence		Контрольная сумма		Контрол ьная сумма

Рис. 5. Структура кадров ARP запроса и ответа

Изучение принципа работы коммутатора Ethernet

Рассмотрим принцип работы коммутатора Ethernet на примере локальной сети, приведенной на рис. 6. Коммутатор постоянно изучает заголовки поступающих в его порты кадров и заносит в так называемую *таблицу MAC-адресов* значения MAC-адресов из поля адреса отправителя входящих в коммутатор кадров, приписывая их идентификатору порта, в который эти кадры поступают извне (Fa0/номер_порта на рис. 6).

Таблица MAC-адресов используется для нахождения номера порта, на который необходимо передать кадр, по MAC-адресу, извлекаемому из поля адреса получателя кадра. Таким образом, коммутатор передаѐт кадр со своего входящего порта на исходящий порт, ведущий к получателю кадра (с порта 3 на порт 6 на рис. 6). Широковещательные кадры коммутатор передаѐт на все свои порты, кроме порта, в который поступает кадр извне. Аналогичным образом происходит и коммутирование кадров с неизвестным для коммутатора MAC-адресом (который ещѐ не занесен в его таблицу MAC-адресов). Отметим, что заполнение таблицы обычно происходит быстро, т.к. при включении рабочих станций каждая из них стразу же высылает в широковещательном кадре своѐ сетевое имя.

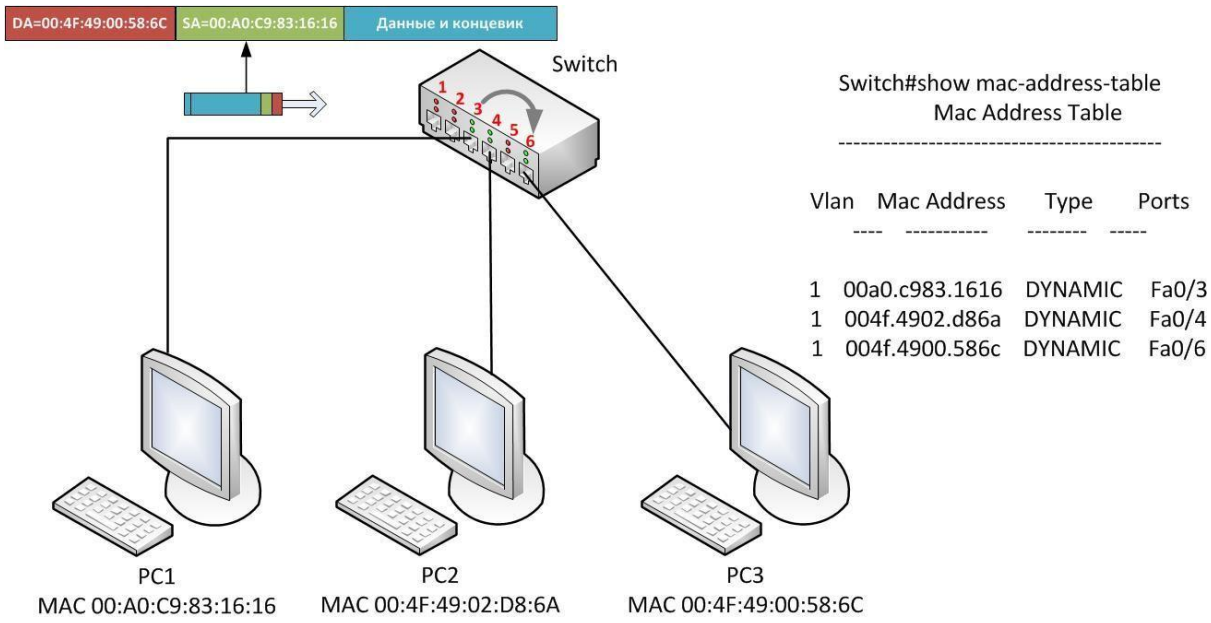

Рис. 6. Принцип работы коммутатора Ethernet

Задание для самостоятельной работы

Запустите анализатор протоколов Wireshark. Выполните захват пакетов утилиты ping, с помощью которой они посылаются на соседний компьютер. Для этого в Wireshark выполните щелчки по пунктам меню Capture (Захват) Option…(Опции…). Откроется окно настроек параметров захвата (рис. 7), в котором необходимо выбрать интерфейс, который будет захватывать пакеты (на компьютере с одним сетевым интерфейсом он выбирается автоматически). Название интерфейса и его IP-адрес будут совпадать со значениями, выводимыми командой ipconfig /all (ifconfig). Обратите внимание, что по умолчанию сетевой интерфейс захватывает пакеты в *неразборчивом режиме* (*promiscuous mode*), то есть не только пакеты, предназначаемые для него, а все, которые он видит в сети.

В строке определения фильтра захвата целесообразно указывать фильтр с целью захвата только пакетов с интересующей нас информацией. На рис. 7 указано, что захватывать необходимо только пакеты, переносящие данные протокола контрольных сообщений Интернета (Internet Control Message Protocol ICMP),

поскольку утилита ping переносит данные именно этого протокола. Достаточно часто необходимо захватывать пакеты, только отправляемые и получаемые одной рабочей станцией. В этом случае фильтр будет выглядеть host ip_адрес_станции. Wireshark обладает очень гибкой системой фильтрации, с примерами фильтров можно ознакомиться, открыв окно щелчком по кнопке Capture Filter. Выделив название фильтра в списке предопределѐнных фильтров в нижней части окна можно увидеть название этого фильтра и команду, которая задаѐт правила фильтрации. Можно изменять их, подставляя необходимые параметры. Также существует возможность создания и удаления пользовательских фильтров. Нужно отметить, что применяемые фильтры сохраняются в строке-списке фильтров захвата окна Capture Options (рис. 7).

После настройки захвата только ICMP-пакетов выполните щелчок на кнопке Start в окне Capture Options, после чего откройте окно командной строки (Пуск-Выполнить-cmd) и запустите в нѐм команду ping с указанием IP-адреса соседнего компьютера в качестве параметра. Wireshark выполнит захват пакетов в окне, приведенном на рис. 1. Для завершения захвата пакетов выполните щелчок на кнопке Остановить текущий захват (Stop the running live capture) (рис. 8).

Выделите первый из захваченных пакетов (отправленный Вашим компьютером), в области анализа полей пакета выделите заголовок Ethernet. Приведите в отчѐт шестнадцатеричный дамп этого заголовка, выделенный в нижней части окна. Выполните расшифровку полей заголовка.

Выделите второй из захваченных пакетов (полученный Вашим компьютером) и повторите предыдущее задание.

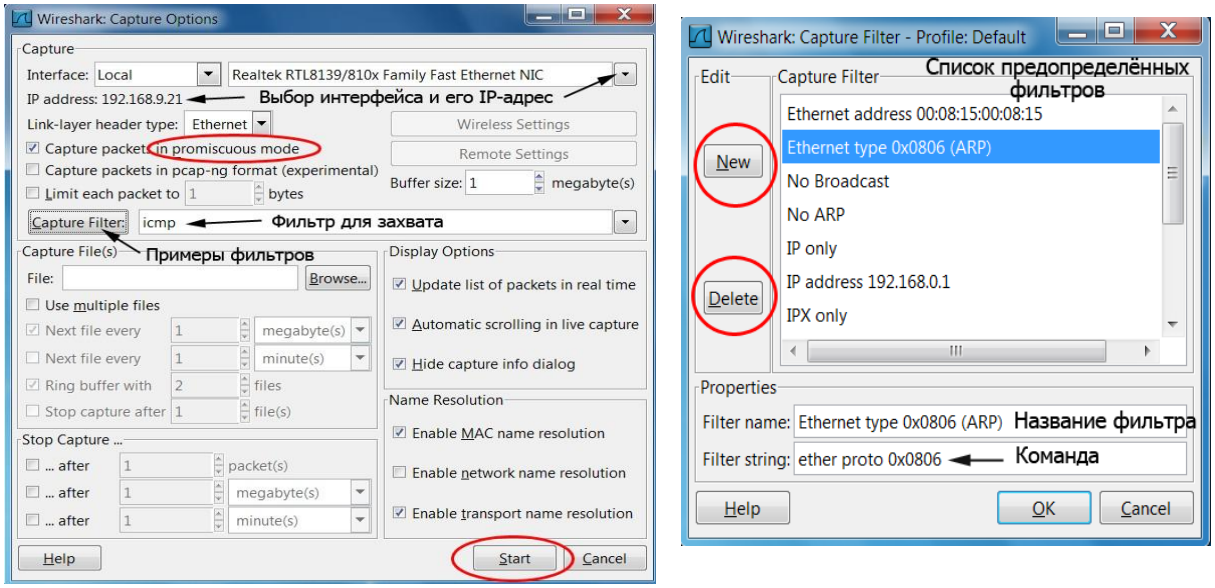

Рис. 7. Настройка параметров захвата в Wireshark

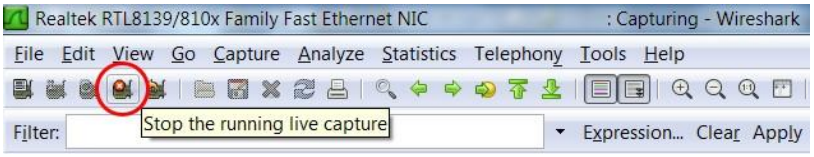

Рис. 8. Остановка захвата пакетов в Wireshark

Выполните в отчѐте расшифровку MAC-адресов отправителя и получателя, указав тип адреса (индивидуальный, групповой, широковещательный), значения *OUI* и *OUA*, является ли адрес локально уникальным или глобально уникальным. Выполните запросы к базе данных IEEE и определите по значениям *OUI* информацию о производителе контроллеров сетевых интерфейсов отправителя и получателя. Приведите полученную информацию в отчѐт.

С помощью команды arp –a просмотрите текущее состояние ARP-таблицы Вашего компьютера и приведите еѐ в отчѐт. Настройте Wireshark на захват всех пакетов, получаемых и отправляемых компьютером локальной сети, адреса которого не содержатся в ARP-таблице. Запустите захват и в командной строке с помощью утилиты ping пошлите пакеты компьютеру, адрес

которого указан в фильтре захвата. ICMP-пакетами утилиты ping должны быть захвачены два пакета: с ARP-запросом и ARP-ответом. Выделите в окне анализа полей пакета заголовок Ethernet пакета с ARP-запросом. Выполните его сравнение с ICMP-пакетом, отправленным Вашим компьютером в предыдущем задании. Опишите в отчѐте различия полей заголовка Ethernet этих кадров. Укажите, какой формат кадров Ethernet используется для транспортировки этих пакетов. Выполните анализ полей ARP-запроса и ARP-ответа и приведите его в отчѐт.

Для изучения работы коммутатора Ethernet создайте с помощью Packet Tracer модель локальной сети, состоящей из четырѐх рабочих станций с именами PC1, PC2, PC3, PC4, подсоединѐнных, соответственно, к пор- там FastEthernet0/1, 0/2, 0/3 и 0/4, коммутатора 2950-24 с именем Switch0. Задайте станциям IP-адреса 192.168.1.1, 192.168.1.2, 192.168.1.3 и 192.168.1.4, соответственно, с маской подсети 255.255.255.0. Выполните щелчок на инструменте Inspect (Инспектировать), а затем на коммутаторе, из открывшегося окна выберите команду MAC Table (Таблица MAC-адресов). Должно открыться пустое окно MAC Table for Switch0, поскольку Switch0 пока не получал кадров ни от одного компьютера.

Детальное изучение процессов, происходящих в сети, удобно выполнять в режиме Simulation (Симуляция) Packet Tracer (под симуляцией понимается моделирование программой событий, происходящих в реальной сети). Для перехода в этот режим выполните щелчок по переключателю в правом нижнем углу окна из Realtime (Режима реального времени) в режим Simulation (Симуляция). Откроется окно Event List (Список событий) в правой части окна Рабочей области (рис. 9). На Панели инструментов выберите Add simple PDU (Добавить простой PDU). Термином Протокольная единица данных Protocol Data Unit, PDU обозначается структура данных протокола любого уровня модели взаимодействия открытых систем (ПРИЛОЖЕНИЕ А), в Packet Tracer инструмент Add simple PDU (Добавить простой PDU) добавляет пакет ICMP, высылаемый с помощью утилиты ping. После выбора этого инструмента выполните щелчок вначале по станции-отправителю (например, PC1), а затем по станции-

получателю (например, PC2) пакета. Вы должны увидеть обозначающий ICMP-пакет конвертик с перемещающимися прямоугольниками возле станции-отправителя, а также первое событие в списке наличие отправляемого пакета ICMP у станции PC1. Кроме того, поскольку станции-отправителю PC1 не известен MAC-адрес станции-получателя PC2, возле неѐ также будет находиться конвертик другого цвета, обозначающий запрос ARP, соответствующее событие также будет находиться в списке событий (рис. 9).

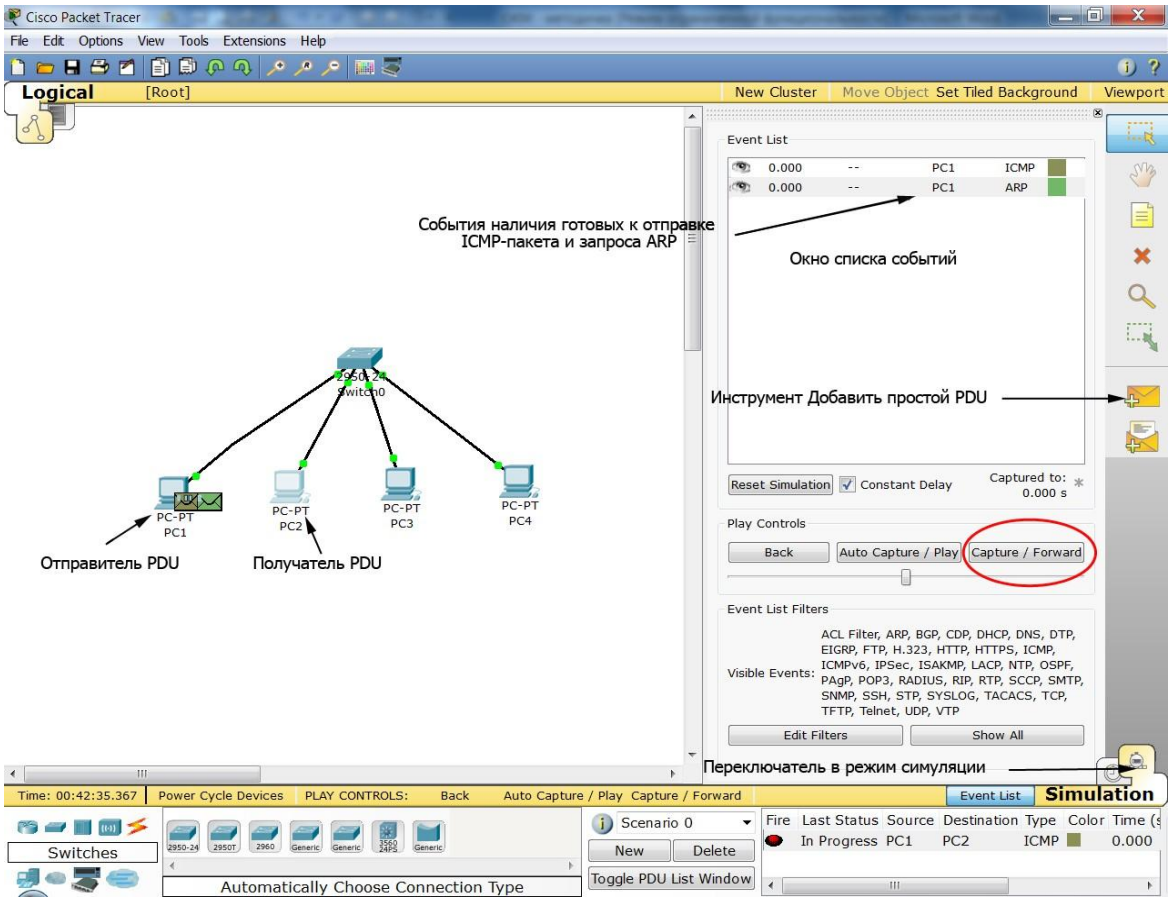

Рис. 9. Режим симуляции Wireshark

С помощью инструмента Inspect (Инспектировать) просмотрите ARP-таблицы PC1 и PC2, выбрав соответствующую команду, пока они должны быть пустыми. Выполните щелчок по кнопке Capture/Forward (Захват/Следующий шаг) и Вы увидите передачу ARP-запроса от PC1 коммутатору, обратите внимание на

новое событие, появившееся в списке. С помощью инструмента Inspect (Инспектировать) просмотрите MAC-таблицу коммутатора, в ней уже должна быть запись адресов для PC1. Выполните ещѐ один щелчок по кнопке Capture/Forward (Захват/Следующий шаг) и Вы должны увидеть отправку полученного от PC1 ARP-запроса коммутатором всем остальным рабочим станциям, то есть широковещательную рассылку. На конвертиках у PC3 и PC4 должны появиться красные крестики, означающие, что в ARP-запросе не содержится их IP-адрес, а ARP-таблице PC2 должна появиться запись для PC1. Следующий щелчок по кнопке Capture/Forward (Захват/Следующий шаг) приведѐт к отправке ARP-ответа стан- цией PC2 коммутатору. После этого шага в таблице MAC-адресов коммутатора появится запись с MAC-адресом PC2. Следующий шаг приведѐт к получению ARP-ответа станцией PC1 и добавлению записи для PC2 в еѐ ARP-таблицу.

Последующие щелчки по кнопке Capture/Forward (Захват/Следующий шаг) приведут к отправке ICMP-пакета от PC1 через коммутатор PC2 и получе- нию ICMP-отклика от PC2 через коммутатор PC1. Коммутатор знает, на каком порту находятся обе станции, поэтому коммутация выполняется без широковещательных рассылок (рис. 10).

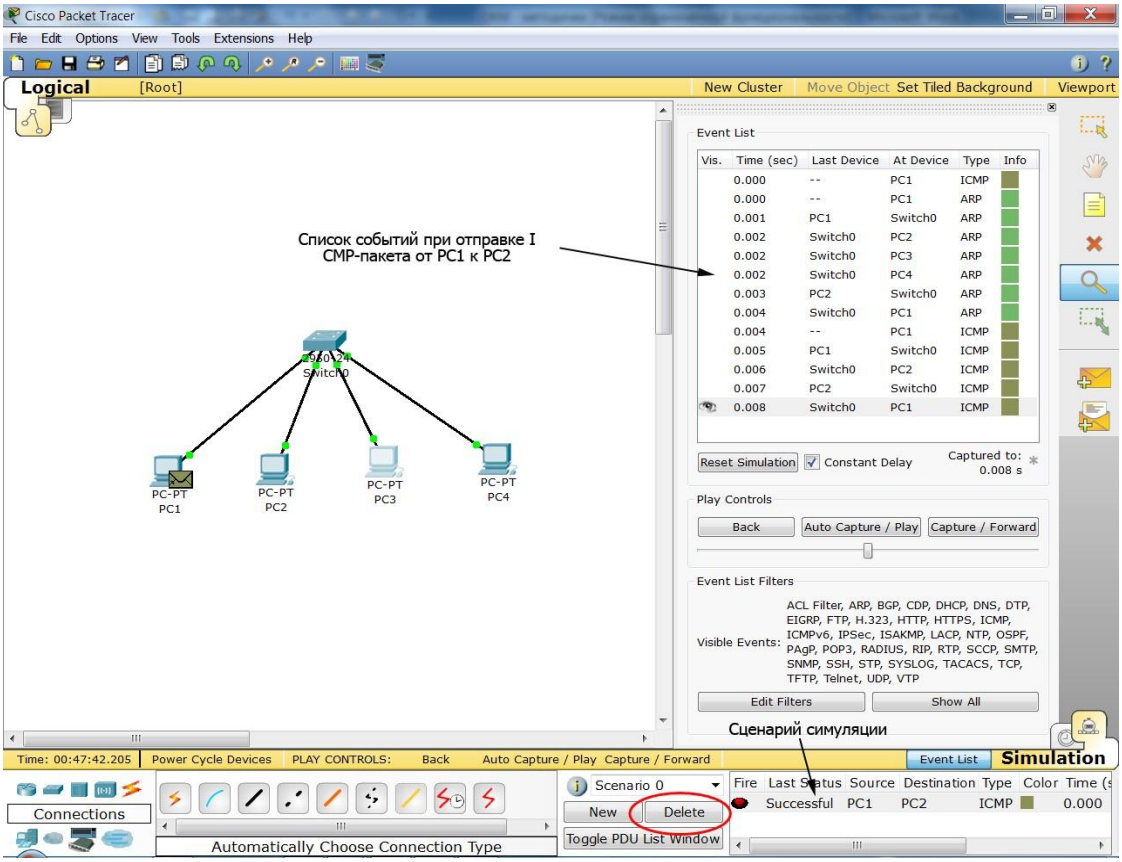

Рис. 10. Симуляция пересылки ICMP-пакетов между PC1 и PC2

Повторите выполненную симуляцию для пересылки ICMP-пакета от станции PC3 станции PC4. Занесите в отчѐт в приведенную ниже таблицу список событий и записи в ARP-таблицах PC3 и PC4 и MAC-таблице коммутатора после выполнения каждого события (табл.1).

Таблица 1

Изучение ARP и работы коммутатора

№ со-бытия	Отпра-витель	Полу-чатель	Тип пакета	ARP-таблица PC3	ARP-таблица PC4	MAC-таблица Switch0

Выполните просмотр ARP-кэшей PC3 и PC4 из командной строки каждой из них, приведите эту информацию в отчѐт.

По аналогии с предыдущим заданием выполните исследование передачи ICMP-пакетов между PC1 и PC3 и затем между PC2 и PC4 в сети с двумя коммутаторами, приведенной на рис. 11.

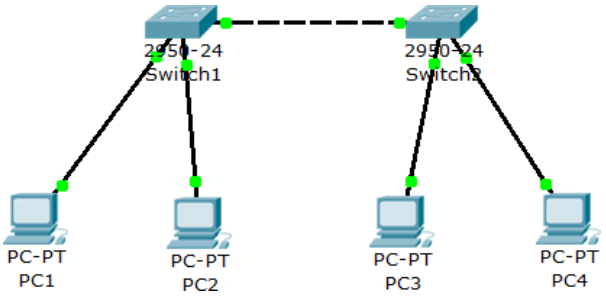

Рис. 11. Модель сети для изучения работы коммутаторов

Занесите в отчѐт в приведенную ниже таблицу список событий и записи в MAC-таблицах коммутаторов Switch1 и Switch2 после выполнения каждого события (табл.2).

Таблица 2

Изучение принципа построения MAC-таблиц двух коммутаторов

№ события	Отправитель	Получатель	Тип пакета	MAC-таблица Switch1	MAC-таблица Switch2

Существует возможность просмотра содержимого таблицы MAC-адресов коммутатора с помощью команд Cisco IOS (следует отметить, что реальные управляемые сетевые устройства могут не поддерживать графические инструментальные средства, подобные рассмотренным в процессе симуляции, но точно поддерживают управление из командной строки). Для просмотра таблицы MAC-адресов выполните щелчок на коммутаторе и откройте вкладку командной строки (Command Line Interface CLI). Нажмите Enter и Вы увидите приглашение режима пользователя (User Mode), его признаком является приглашение '>'. Из режима пользователя можно перейти в привилегированный режим (Privilege Mode), его признаком является приглашение '#'. В первом режиме можно только просматривать конфигурацию устройства, во втором – осуществлять конфигурирование. Для того, чтобы войти в

привилегированный режим необходим ввести команду enable (допускается сокращѐнная форма команды en). Справку по каждой команде можно получить посредством еѐ набора в командной строке и набора знака ? после неѐ. Для просмотра таблицы MAC-адресов коммутатора выполните в привилегированном режиме команду show mac- address-table (рис. 12).

Из привилегированного режима можно войти в *режим глобального конфигурирования* (*Global Configuration Mode*) командой configure terminal (config t), его признаком является слово (config), выводимое после имени устройства в приглашении. Выход из этого режима осуществляется командой end (или нажатием комбинации клавиш <CTL>+z).

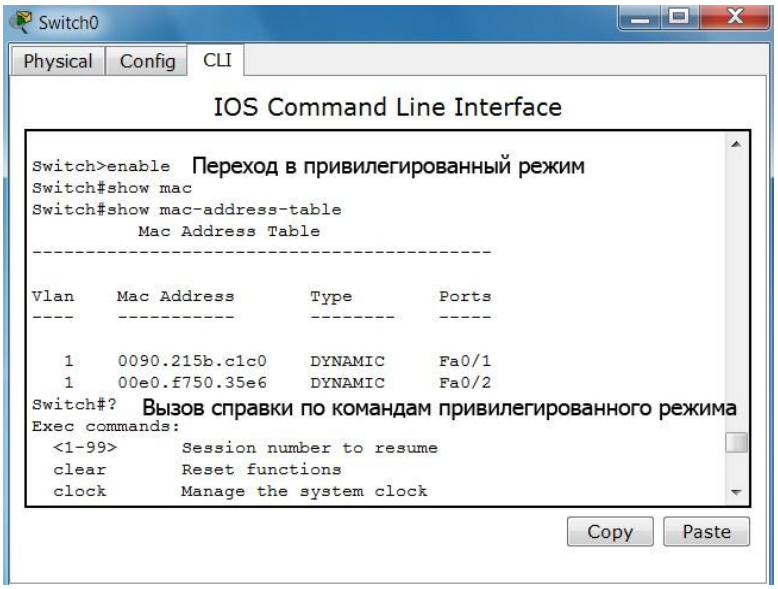

Рис. 12. Переход в привилегированный режим и просмотр таблицы MAC-адресов коммутатора командами Cisco IOS

Сетевые устройства могут иметь различные типы интерфейсов, например, token ring, FDDI, Ethernet, Serial, ISDN и др. В качестве имени интерфейса используется обычно название протокола и номер интерфейса, начиная с 0, например, ethernet0 (1 порт Ethernet), serial0 (1 последовательный порт) и т.д. Достаточно часто сетевые устройства могут иметь несколько модулей с сетевыми интерфейсами, в этом случае идентификация интерфейса

состоит из названия протокола, номера модуля/номера интерфейса, например, FastEthernet0/1. Для просмотра статуса всех интерфейсов устройства используют команду show interfaces (сокращение - sh int). Для просмотра информации об определенном интерфейсе вводится команда show interfaces <имя_интерфейса>. Из режима глобального конфигурирования можно войти в режим конфигурирования интерфейса (Interface Configuration Mode), выполнив команду interface

<имя_интерфейса>, его признаком является слово (config-if) в приглашении. В приведенном ниже примере осуществляется переход из привилегированного режима в режим общего конфигурирования, а затем переход в режим конфигурирования интерфейса FastEthernet0/1. В этом режиме подаѐтся команда no shutdown, переводящая интерфейс в активное состояние.

Команда end позволяет выйти из режима конфигурирования интерфейса.

Выполните в окне командной строки просмотр таблицы MAC-адресов коммутатора Swith0 и скопируйте сеанс работы в отчѐт.

Изучение форматов кадров, отличных от Ethernet II (DIX), на практике часто представляет сложность. Это объясняется тем, что в настоящее время стек протоколов TCP/IP вытеснил достаточно популярные ранее стеки IPX/SPX и NetBIOS (в Windows Vista/7 отсутствует их поддержка), а именно они используют формат кадра 802.3/LLC. Также достаточно сложно захватит кадры с форматом Ethernet SNAP. К счастью режим Simulation (Симуляция) Packet Tracer может нам помочь. Создайте в Packet Tracer сеть, состоящую из двух соединѐнных между собой коммутаторов, к каждому из которых подсоединена рабочая станция (рис. 13). Назначьте сетевым интерфейсам рабочих станций IP-адреса 192.168.1.1 и 192.168.1.2 с маской 255.255.255.0. Переключитесь в режим симуляции и добавьте простой PDU от одной станции к другой.

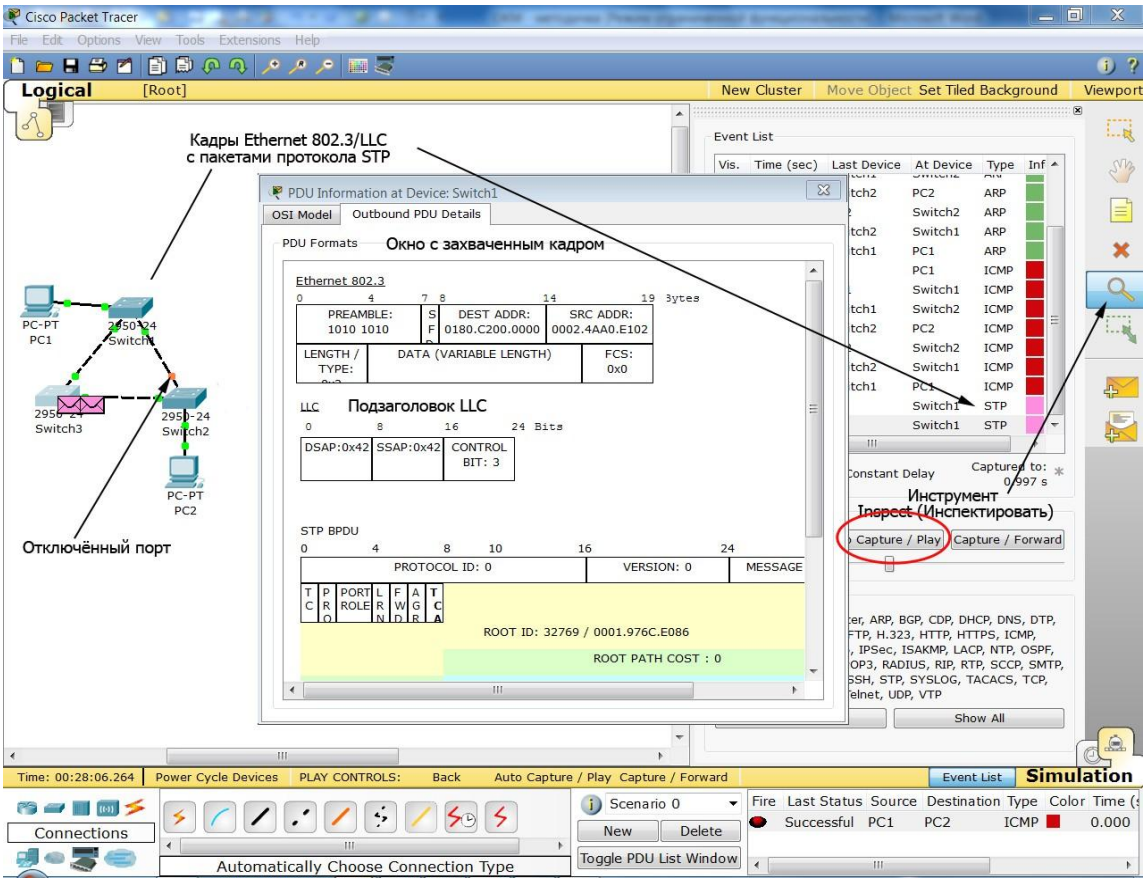

Рис. 13. Модель сети и захваченный кадр Ethernet формата 802.3/LLC

Выполните щелчок по кнопке Auto Capture/Play (Автозахват/Анимация) и Вы увидите автоматически сменяющиеся события в сети. Дождитесь появления в списке событий события с типом STP и выполните щелчок по кнопке Auto Capture/Play (Автозахват/Анимация) для остановки симуляции. *Протокол остовного дерева – Spanning Tree Protocol, STP* – это протокол, поддерживающийся коммутаторами Ethernet.