ФЕДЕРАЛЬНОЕ АГЕНТСТВО ВОЗДУШНОГО ТРАНСПОРТА
(РОСАВИАЦИЯ)

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ
УНИВЕРСИТЕТ ГРАЖДАНСКОЙ АВИАЦИИ» (МГТУ ГА)

Кафедра вычислительных машин, комплексов, систем и сетей

О.Г. Феоктистова, И.В. Дровосеков

СЕТИ И ТЕЛЕКОММУНИКАЦИИ

Учебно-методическое пособие
по проведению лабораторных работ № 1, 2

для студентов III–IV курсов
направления 09.03.01
очной формы обучения

Москва
ИД Академии Жуковского
2021

УДК 004.7
ББК 6Ф7.3
Ф42

Рецензент:
Черкасова Н.И. – канд. физ.-мат. наук, доцент

Феоктистова О.Г.
Ф42 Сети и телекоммуникации [Текст] : учебно-методическое пособие по проведению лабораторных работ № 1, 2 / О.Г. Феоктистова, И.В. Дровосеков. – М.: ИД Академии Жуковского, 2021. – 36 с.

Данное учебно-методическое пособие издается в соответствии с рабочей программой учебной дисциплины «Сети и телекоммуникации» по учебному плану для студентов III–IV курсов по направлению подготовки 09.03.01 очной формы обучения.

Рассмотрено и одобрено на заседаниях кафедры 28.09.2021 г. и методического совета 28.09.2021 г.

УДК 004.7
ББК 6Ф7.3

В авторской редакции

Подписано в печать 08.11.2021 г.
Формат 60x84/16 Печ. л. 2,25 Усл. печ. л. 2,09
Заказ № 844/1004-УМП14 Тираж 30 экз.

Московский государственный технический университет ГА
125993, Москва, Кронштадтский бульвар, д. 20

Издательский дом Академии имени Н. Е. Жуковского
125167, Москва, 8-го Марта 4-я ул., д. 6А
Тел.: (495) 973-45-68
E-mail: zakaz@itsbook.ru

1. Лабораторная работа № 1
1.1. «История ЛВС. Основы VPN подключения. Основные протоколы, использующиеся для VPN соединения»

Цель лабораторной работы: вспомнить историю создания локальных вычислительных сетей и формата Ethernet. Познакомиться с понятием VPN, и с основными протоколами, для создания VPN соединения. Подключение компьютера к местной локальной сети, и настройка доступа в Интернет, с помощью VPN.

Введение

История возникновения локальных сетей

Трудно в настоящее время не признать, что основной движущей силой развития локальных вычислительных сетей в мире является международный Институт инженеров по электротехнике и радиоэлектроники (IEEE).

История его начинается в девятнадцатом столетии, в 1884 г., когда был основан Американский институт инженеров по электротехнике (AIEE). Следующий шаг был сделан в 1912-м, и снова в США: Институт радиоинженеров (The Institute of Radio Engineers) создал свой комитет стандартов. В 1958 г. сначала объединились комитеты стандартов Американского института инженеров по электротехнике и Института радиоинженеров, а затем в 1963 г. и сами эти институты, породив IEEE.

В 1962 г. ARPA создало департамент технологий обработки информации (Information Processing Techniques Office, IPTO), которому было поручено изучить технологии контроля и управления. Этот департамент и руководил работами в области компьютерных наук. В 1961 г. работу, посвященную коммутации пакетов и послужившую темой для будущей диссертации опубликовал в Массачусетском технологическом институте Леонард Клейнрок (Leonard Kleinrock). В 1963 г. в США был создан Институт инженеров по электротехнике и радиоэлектронике (IEEE) - ставший впоследствии главным разработчиком массовых стандартов в области ЛВС. Тогда же защитил диссертацию Леонард Клейнрок, будущий создатель Интернета и главный теоретик.

В августе 1964 г. Пауль Баран (Paul Baran), сотрудник корпорации RAND, опубликовал меморандум "On Distributed Communications: IX Security, Secrecy, and Tamper-Free Considerations", где впервые высказал идею построения распределенной сети передачи данных, не имеющей управляющего центра.

Через год агентство ARPA Министерства обороны США финансировало изучение работы компьютеров в общей сети в режиме разделения времени.

Первые ЛВС

Первую в мире ЛВС создал в 1967 г. Дональд Дэвис (Donald Davies) в Национальной физической лаборатории Великобритании (British National Physics Laboratory).

К началу 70-х сеть работала с пиковой скоростью 0,25 Мбит/с, обслуживая около 200 пользователей.

В США в 1968 г. в Лаборатории Белла исследователь В. Чу (W. W. Chu) вводит термин "Asynchronous Time Division Multiplexing" - так зарождается технология ATM. В 1969-м исследования, финансировавшиеся IPTO, директором которого в это время был Роберт Тейлор, привели к тому, что в Калифорнийском университете в Лос-Анджелесе Леонард Клейнрок создал ARPANET - первый узел будущего Интернета. Спустя год, в 1970-м, на Гавайских островах Норман Абрамсон (Norman Abramson) создал сеть ALOHA - прообраз будущих и Ethernet, и IEEE 802.11. Это была первая в мире пакетная радиосеть, использовавшая удивительно простой метод доступа к среде передачи: пакеты передавались в эфир, когда в этом возникала необходимость..

Появление Ethernet

В начале 1973 г. на одной из северных баз ВВС в США прошло совещание, в котором среди прочих приняли участие все главные действующие лица в области компьютерных сетей: Ларри Робертс (ARPA), Норман Абрамсон (создатель сети ALOHA), Боб Меткалф (Robert Metcalfe, будущий изобретатель Ethernet), Лен Клейнрок и Фоуад Тобаги (Fouard Tobagi). Обсуждались протоколы доступа к каналу передачи данных. У своеобразной "тайной вечери", о которой через тридцать лет рассказал Ф.Тобаги, оказались удивительно далеко идущие последствия. После него база ВВС почему-то меняет свое название на Rockwell International, а Боб Меткалф 22 мая подает в фирме Xerox записку с предложением создать Ethernet!

Первая ЛВС Ethernet, созданная Бобом Меткалфом и Дэвидом Боггсом в исследовательском центре PARC (Palo Alto Research Centre) фирмы Xerox, работала со скоростью 2,944 Мбит/с и соединяла друг с другом два компьютера. Позже Меткалф сформулировал так называемый закон Меткалфа: стоимость ЛВС с ростом числа узлов растет линейно, а ценность - пропорционально квадрату числа узлов.

Лока́льная вычисли́тельная сеть (*Local Area Network, LAN*) — компьютерная сеть, покрывающая обычно относительно небольшую территорию или небольшую группу зданий (дом, офис, фирму, институт). Можно сказать, что л*окальная сеть* - коммуникационная система, состоящая из нескольких компьютеров, соединенных между собой посредством кабелей (телефонных линий, радиоканалов), позволяющая пользователям совместно использовать ресурсы компьютера: программы, файлы, папки, а также периферийные устройства: принтеры, плоттеры, диски, модемы и т.д.

VPN

Связь с удалённой локальной сетью, подключенной к глобальной сети, из дома/командировки/удалённого офиса часто реализуется через VPN. При этом устанавливается VPN-подключение к пограничному маршрутизатору.

VPN (*Virtual Private Network* — виртуальная частная сеть) — обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет).

Особенно популярен следующий способ организации удалённого доступа к локальной сети:

1. Обеспечивается подключение снаружи к маршрутизатору, например, по протоколу PPPoE, PPTP или L2TP (PPTP+IPSec).
2. Так как в этих протоколах используется PPP, то существует возможность назначить абоненту IP-адрес. Назначается свободный (не занятый) IP-адрес из локальной сети.
3. Маршрутизатор (VPN, Dial-in сервер) добавляет proxyarp — запись на локальной сетевой карте для IP-адреса, который он выдал VPN-клиенту.

Рассмотрим подробнее протокол PPP и протоколы, работающие на его основе: PPPoE, PPTP и L2TP.

PPP (*Point-to-Point Protocol*) - двухточечный протокол канального уровня (Data Link) сетевой модели OSI. Обычно используется для установления прямой связи между двумя узлами сети, причем он может обеспечить аутентификацию соединения, шифрование и сжатие данных. Используется на многих типах физических сетей: нуль-модемный кабель, телефонная линия, сотовая связь и т. д.

Каждый кадр PPP всегда начинается и завершается флагом 0x7E. Затем следует байт адреса и байт управления, которые тоже всегда равны 0xFF и 0x03 соответственно. В связи с вероятностью совпадения байтов внутри блока данных с зарезервированными флагами, существует система автоматической корректировки «проблемных» данных с последующим восстановлением.

Флаг 0x7E	**Адрес 0xFF**	**Управление 0x03**	**Данные**	**Контрольная сумма**	**Флаг 0x7E**
1	1	1	1494	2	1

Поля «Флаг», «Адрес» и «Управление» (заголовок кадра HDLC) могут быть опущены и не передаваться, но это если PPP в процессе конфигурирования (используя LCP), договорится об этом. Если PPP инкапсулирован в L2TP-пакеты, то поле «Флаг» не передается.

Поле «Данные», PPP кадра, в свою очередь разбиты ещё на два поля: флаг протокола (который определяет тип данных до конца кадра), и сами данные.

Протокол 0xXXXX	Данные
1 или 2	0 и более

- Флаги протокола от 0x0XXX до 0x3XXX идентифицируют протоколы сетевого уровня. Например, популярному IP протоколу соответствует флаг 0x0021, а Novell IPX — 002B.
- Флаги протокола от 0x4XXX до 0x7XXX идентифицируют протоколы с низким уровнем трафика.
- Флаги протокола от 0x8XXX до 0xBXXX идентифицируют протокол управления сетью (NCP).
- Флаги протокола от 0xCXXX до 0xEXXX идентифицируют управляющие протоколы. Например, 0xC021 обозначает, что кадр содержит данные протокола управления соединением LCP.

Фазы работы PPP :

- *Link Dead.* Эта фаза наступает, когда связь нарушена, либо одной из сторон указали не подключаться (например, пользователь завершил модемное соединение.)
- *Link Establishment Phase*. В данной фазе проводится настройка Link Control. Если настройка была успешной, управление переходит в фазу аутентификации, либо в фазу Network-Layer Protocol, в зависимости от того, требуется ли аутентификация.
- *Authentication Phase*. Данная фаза является необязательной. Она позволяет сторонам проверить друг друга перед установкой соединения. Если проверка успешна, управление переходит в фазу Network-Layer Protocol.
- *Network-Layer Protocol Phase*. В данной фазе вызывается NCP для желаемого протокола. Например, IPCP используется для установки IP сервисов. Передача данных по всем успешно установленным протоколам также проходит в этой фазе. Закрытие сетевых протоколов тоже включается в данную фазу.
- *Link Termination Phase*. Эта фаза закрывает соединение. Она вызывается в случае ошибок аутентификации, если было настолько много ошибок контрольных сумм, что обе стороны решили закрыть соединение, если соединение неожиданно оборвалось, либо если пользователь отключился. Данная фаза пытается закрыть все настолько аккуратно, насколько возможно в данных обстоятельствах.

PPPoE (*Point-to-point protocol over Ethernet*) - сетевой протокол канального уровня передачи кадров PPP через Ethernet. В основном используется xDSL-сервисами. Предоставляет дополнительные возможности (аутентификация, сжатие данных, шифрование).

Стандартное MTU(максимальный размер полезного блока данных одного пакета) протокола ниже (1492 байт), чем на стандартном Ethernet (1500 байт), что иногда вызывает проблемы с плохо настроенными межсетевыми экранами.

PPPoE - это туннелирующий протокол, который позволяет настраивать (или инкапсулировать) IP, или другие протоколы, которые настраиваются на PPP, через соединения Ethernet, но с программными возможностями PPP-соединений, и поэтому используется для виртуальных «звонков» на соседнюю Ethernet-машину и устанавливает соединение точка-точка, которое используется для транспортировки IP-пакетов, работающее с возможностями PPP.

Это позволяет применять традиционное PPP-ориентированное ПО для настройки соединения, которое использует не последовательный канал, а пакетно-ориентированную сеть (как Ethernet), чтобы организовать классическое соединение с логином, паролем для Интернет-соединений. Также IP-адрес по другую сторону соединения назначается, только когда PPPoE соединение открыто, позволяя динамическое переиспользование IP-адресов.

Работа PPPoE осуществляется следующим образом. Существует Ethernet-среда, то есть несколько соединённых сетевых карт, которые адресуются MAC-адресами. Заголовки Ethernet-кадров содержат адрес отправителя кадра, адрес получателя кадра и тип кадра. Одну из карт слушает PPPoE-сервер. Клиент посылает широковещательный Ethernet-кадр, на который должен ответить PPPoE-сервер (адрес отправителя кадра — свой MAC-адрес, адрес получателя кадра — FF:FF:FF:FF:FF:FF и тип кадра — PPPoE Active Discovery Initiation). PPPoE-сервер посылает клиенту ответ (адрес отправителя кадра — свой MAC-адрес, адрес получателя кадра — MAC-адрес клиента и тип кадра — PPPoE Active Discovery Offer). Если в сети несколько PPPoE-серверов, то все они посылают ответ. Клиент выбирает подходящий сервер и посылает ему запрос на соединение. Сервер посылает клиенту подтверждение с уникальным идентификатором сессии, все последующие кадры в сессии будут иметь этот идентификатор. Таким образом, между сервером и клиентом создается виртуальный канал, который идентифицируется идентификатором сессии и MAC-адресами клиента и сервера. Затем в этом канале устанавливается PPP-соединение, а уже в PPP-пакеты упаковывается IP-трафик.

Преимущества PPPoE:

- IP-заголовки в Ethernet-среде игнорируются. То есть пользователь может назначить IP-адрес своей сетевой карте, но это не приведет к

«обвалу» сети (теоретически при работе с сетевым концентратором не должно произойти «обвала» и при смене пользователем MAC-адреса даже на адрес сервера, а при работе с сетевым коммутатором все зависит от конструкции коммутатора).

- Каждое соединение отделено от других (работает в своем канале).
- Настройки (IP-адрес, адрес шлюза, адреса DNS-серверов) могут передаваться сервером.
- PPP-соединение легко аутентифицируется и обсчитывается (например, при помощи RADIUS).
- PPP-соединение можно шифровать. Например, при работе с сетевым концентратором (когда на каждой сетевой карте может быть виден весь Ethernet-трафик) прочитать чужой IP-трафик весьма затруднительно.

PPTP (*Point-to-Point Tunneling Protocol*) — туннельный протокол типа точка-точка, позволяющий компьютеру устанавливать защищённое соединение с сервером за счёт создания специального туннеля в стандартной, незащищённой сети. PPTP помещает (инкапсулирует) кадры PPP в IP-пакеты для передачи по глобальной IP-сети, например Интернет. PPTP может также использоваться для организации туннеля между двумя локальными сетями. PPTP использует дополнительное TCP-соединение для обслуживания туннеля.

PPTP обеспечивает безопасную передачу данных от удаленного клиента к отдельному серверу предприятия путем создания в сети TCP/IP частной виртуальной сети. PPTP может также использоваться для организации тунеля между двумя локальными сетями. PPTP работает, устанавливая обычную PPP-сессию с противоположной стороной с помощью протокола Generic Routing Encapsulation (GRE). Второе соединение на TCP порту 1723 используется для инициации и управления GRE-соединением. Для защиты данных PPTP-траффика может быть использован протокол MPPE. Для аутентификация клиентов могут использоваться различные механизмы, наиболее безопасные из них — MSCHAPv2 и EAP-TLS.

Для обеспечения работы клиента по протоколу PPTP, необходимо установить IP-соединение с туннельным сервером PPTP. Все передаваемые по этому соединению данные могут быть защищены и сжаты. По туннелю PPTP могут передаваться данные различных протоколоыв сетевого уровня (TCP/IP, NetBEUI и IPX).

Преимущества протокола PPTP:

- Использование частного IP-адреса. Пространство IP-адресов частной сети не должно координироваться с пространством глобальных (внешних) адресов.
- Поддержка множества протоколов. Можно осуществлять доступ к частным сетям, использующим различные комбинации TCP/IP или IPX.

- Безопасность передачи данных. Для предотвращения несанкционированного подключения используются протоколы и политики обеспечения безопасности сервера удаленного доступа.
- Возможность использования аутентификации и защиты данных при передачи пакетов через Интернет.

L2TP (*Layer 2 Tunneling Protocol*) - протокол туннелирования уровня 2 (канального уровня). Объединяет протокол L2F (Layer 2 Forwarding), разработанный компанией Cisco, и протокол PPTP корпорации Microsoft. Позволяет организовывать VPN с заданными приоритетами доступа, однако не содержит в себе средств для защиты данных и механизмов аутентификации.

Протокол L2TP использует сообщения двух типов: управляющие и информационные сообщения. Управляющие сообщения используются для установления, поддержания и ликвидации туннелей и вызовов. Для обеспечения доставки ими используется надежный управляющий канал протокола L2TP. Информационные сообщения используются для инкапсулирования кадров PPP, передаваемых по туннелю. При потере пакета он не передается повторно.

Структура протокола описывает передачу кадров PPP и управляющих сообщений по управляющему каналу и каналу данных протокола L2TP. Кадры PPP передаются по ненадежному каналу данных, предварительно дополняясь заголовком L2TP, а затем - по транспорту для передачи пакетов, такому как Frame Relay, ATM и т.п. Управляющие сообщения передаются по надежному кправляющему каналу L2TP с последующей передачей по тому же транспорту для пересылки пакетов.

Все управляющие сообщения должны содержать порядковые номера, используемые для обеспечения надежной доставки по управляющему каналу. Информационные сообщения могут использовать порядковые номера для упорядочивания пакетов и выявления утерянных пакетов.

Преимущества протокола L2TP:

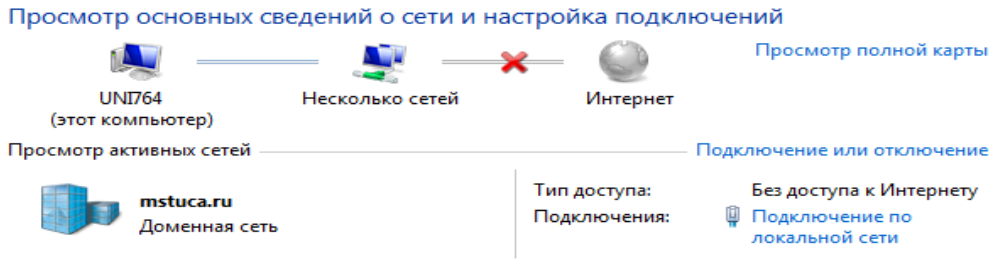
- Разнообразие протоколов. Так как используется кадрирование PPP, удаленные пользователи могут использовать для доступа к корпоративому узлу большое количество различных протоколов, таких как IP, IPX и т.д.
- Создание туннелей в различных сетях. L2TP может работать как в сетях IP, так и в сетях ATM, Frame Relay и др.
- Безопасность передачи данных. При этом, пользователь не должен иметь никакого специального программного обеспечения.
- Возможность аутентификации пользователей.

Проверка подключения компьютера к локальной сети

Для подключения компьютера в локальную сеть, необходимо, чтобы в компьютере была минимум одна сетевая карта, с установленным сетевым драйвером.

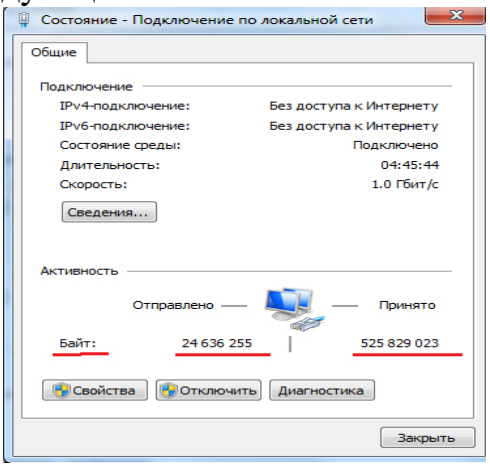
Для проверки соединения с сервером в локальной сети необходимо выполнить следующие действия:

Открыть панель управления, найти центр управления сетями и общим доступом в разделе «Сеть и Интернет»



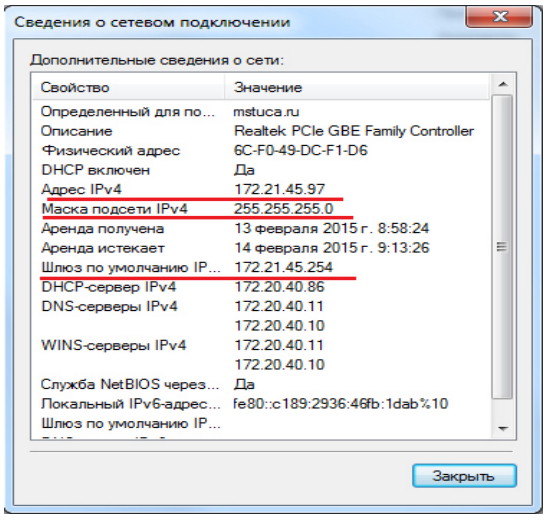
Убедившись, что у нас появилось подключение по локальной сети (в нашем случае имя данной сети mstuca.ru), нужно кликнуть мышкой на «Подключение по локальной сети».

Должно открыться следующее окно:



Если мы видим, что количество отправленных и принятых пакетов есть число, отличное от нуля, значит, подключение успешное, и мы можем пользоваться услугами данной сети (Создавать VPN подключения, обмениваться файлами в локальной сети и т.д.).

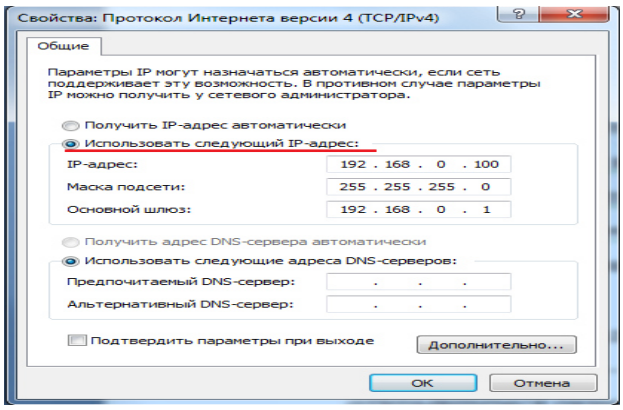
Если количество отправленных или принятых пакетов равно 0, необходимо нажать кнопку «Сведения». Откроется следующее окно:



В нем необходимо обратить внимание на поля IP адрес, Маска подсети и Шлюз по умолчанию. Если ваш IP не попадает в диапазон, допустимых IP адресов для вашей сети, необходимо обратиться к сетевому администратору или компании, предоставляющей услуги по подключению вас к локальной сети.

Данный пример был рассмотрен на примере локальной сети использующей DHCP сервер.

Для настройки подключения к локальной сети с выделенным IP адресом, необходимо в окне «Состояние – Подключение по локальной сети» нажать кнопку «Свойства», в открывшемся окне выбрать «Протокол интернета версии 4 (TCP/IPv4)» и так же нажать кнопку «Свойства». В открывшемся окне, необходимо выбрать «Использовать следующий IP-адрес»

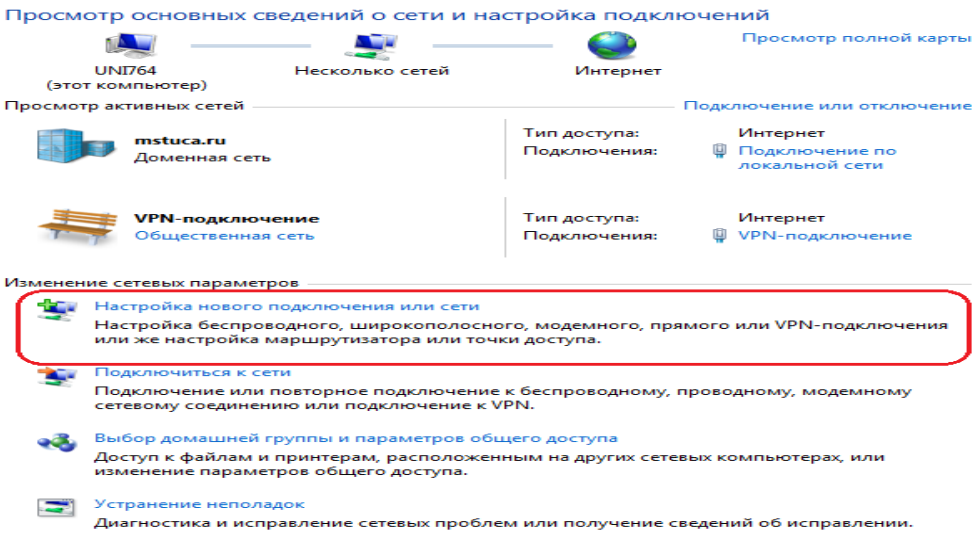


Затем узнать у сетевого администратора или компании предоставляющей услуги по подключению локальной сети непосредственно сам IP-адрес, Маску подсети и Основной шлюз и заполнить эти данные в таблицу, и нажать «ОК».

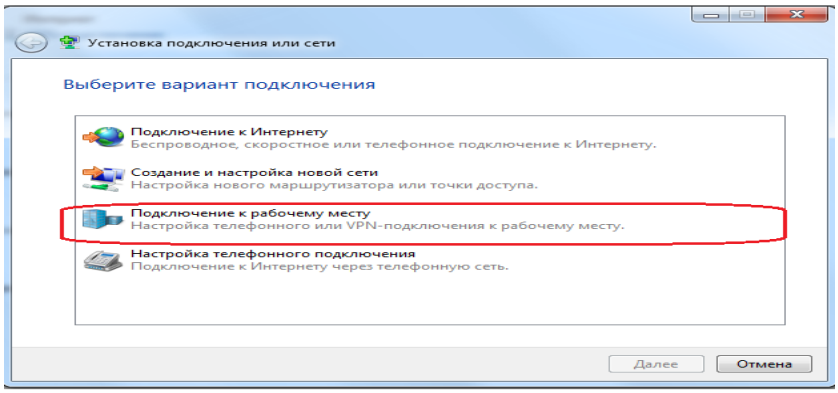
После успешной настройки локальной сети, мы можем перейти к настройке VPN соединения.

Настройка VPN подключения в Windows 7

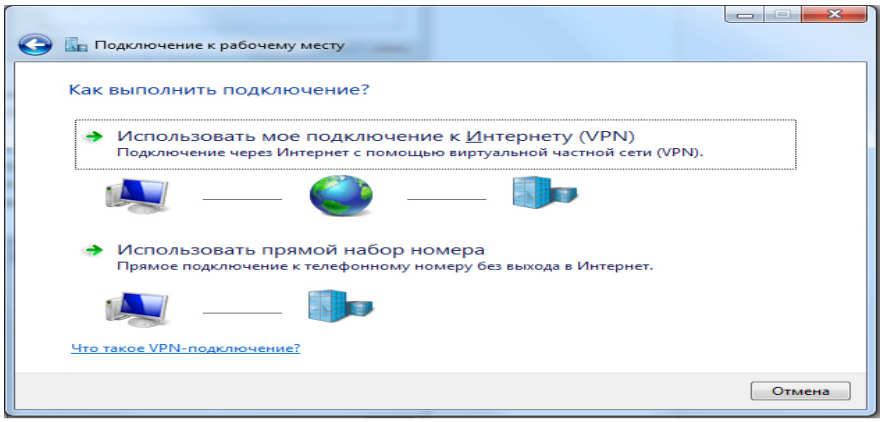
Для настройки VPN соединения в Windows 7, Первым делом вам понадобиться открыть панель управления, найти центр управления сетями и общим доступом в разделе «Сеть и Интернет» и кликнуть мышкой по пункту «Настройка нового подключения или сети».



В открывшемся окне вам будет предложено выбрать вариант подключения. Поскольку вы хотите создать VPN - соединение, то лишь один пункт будет удовлетворять вашим требованиям – «Подключение к рабочему месту», в пояснении к которому указано, что этот вариант позволяет настроить телефонное или VPN - подключение.

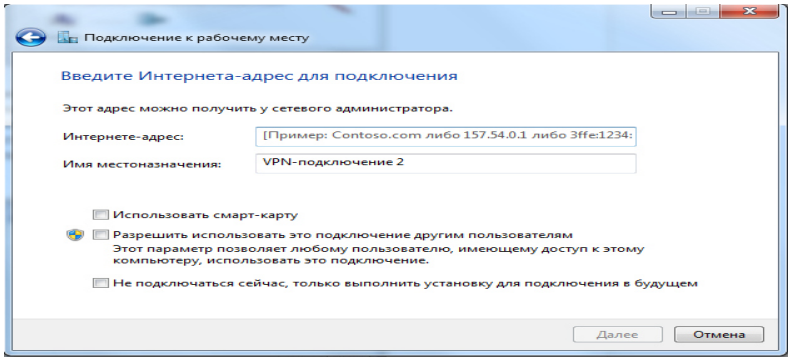


На следующем этапе необходимо указать будет ли VPN - подключение к частной сети выполняться посредством прокладывания тоннеля поверх имеющегося Интернет-соединения, либо для него имеется специальный выделенный телефонный номер, по которому необходимо будет дозваниваться с помощью простого модема.

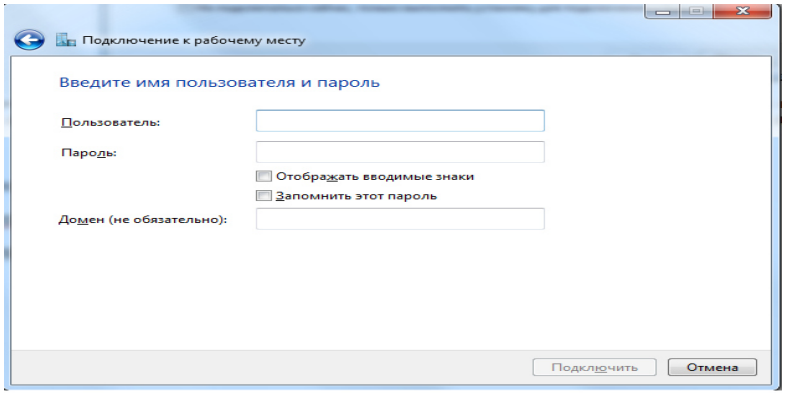


На практике, подавляющее число созданных VPN - соединений осуществляется при помощи первого варианта, поэтому, если вы не уверены в чем-то на этом этапе, лучше выбирать именно его (Это подключение потребуется нам для выполнения заданий лабораторной работы).

На четвертом этапе настройки VPN - соединения в Windows 7 предлагается ввести IP - адрес либо имя компьютера, к которому будет осуществляться подключение посредством VPN тоннеля. Эти данные можно получить у сетевого администратора или у того, кто предоставляет вам непосредственно саму услугу. Имя место назначения можно оставить без изменения со стандартным значением «VPN - подключение».

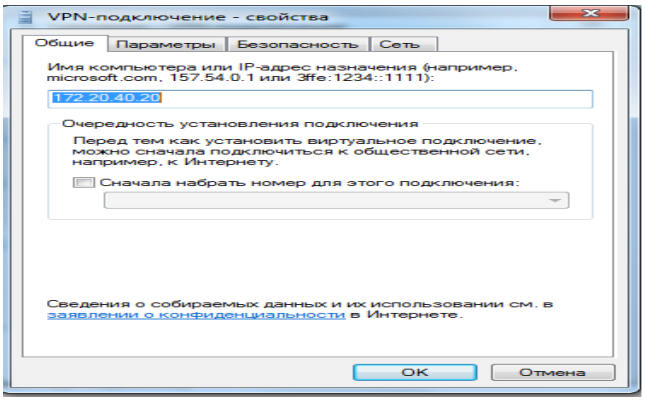


На последнем этапе остается только ввести данные вашей учетной записи (имя пользователя и пароль), которые необходимы для доступа к новой сети и должны были быть предоставлены вам системным администратором или поставщиком данной услуги.



После ввода имени пользователя и пароля, необходимо нажать кнопку «Подключить». Откроется окно пробного подключения к соединению, его необходимо просто закрыть и перейти в настройки параметров подключения.

Созданное соединение появится в «Центр управления сетями и общим доступом». Для дальнейших настроек подключения необходимо кликнуть мышкой на «VPN подключение» напротив нашего подключения. Затем нажать на кнопку «Свойства» вы перейдете к возможности настройки дополнительных параметров подключения.



1.2. Задание на выполнение лабораторной работы:

1. Подключить компьютер к локальной сети.
2. Настроить подключение к локальной сети.
3. Настроить VPN подключение к интернету (необходимые данные для детальной настройки взять у преподавателя).
4. Проверить доступность интернет – ресурсов и скорость соединения к сети Интернет.
5. Подключить компьютер к локальной сети с помощью роутера.
6. Настроить VPN подключение к интернету с помощью роутера (Необязательно, тому, кто выполнит данное задание, будет задан 1 вопрос на защите лабораторной работы вместо 3).
7. Сбросить настройки роутера и подключить компьютер непосредственно к локальной сети, как в п.1(Данный пункт выполнять только в случае успешного выполнения п. 6)

Отчет должен содержать:

1. Титульный лист.
2. Сведения при подключении компьютера к локальной сети.
3. Данные для подключения компьютера к сети Интернет.
4. Вывод по лабораторной работе.

1.3. Контрольные вопросы:

2. История возникновения ЛВС.
3. Определение ЛВС, первые ЛВС.
4. История создания Ethernet.
5. Что такое VPN и его предназначение.
6. Протокол PPP: определение, формат кадра, фазы работы протокола.
7. Определение, описание работы и преимущества протокола PPPoE.
8. Определение, описание работы и преимущества протокола PPTP.
9. Определение, описание работы и преимущества протокола L2TP.
10. Как подключить компьютер к локальной сети и проверить её работоспособность?
11. Как настроить VPN соединение?

2. Лабораторная работа № 2

2.1. "Знакомство с программой - анализатором трафика Wireshark"

Цель работы: Познакомиться с инструментом для анализа сетевого

трафика Wireshark.

Введение

Что такое Wireshark?

Wireshark (ранее - Ethereal) - программа-анализатор трафика для компьютерных сетей Ethernet и некоторых других. Имеет графический пользовательский интерфейс.

Его задача состоит в том, чтобы перехватывать сетевой трафик и отображать его в детальном виде. Анализатор сетевого трафика можно сравнить с измерительным устройством, которое используется для просмотра того, что происходит внутри сетевого кабеля, как например вольтметр используется электриками для того чтобы узнать что происходит внутри электропроводки (но, конечно, на более высоком уровне). В прошлом такие инструменты были очень дорогостоящими и неоткрытыми. Однако, с момента появления такого инструмента как Wireshark ситуация изменилась. Wireshark – это один из лучших анализаторов сетевого трафика, доступных на сегодняшний момент.

Wireshark работает на основе библиотеки pcap. Библиотека Pcap (Packet Capture) позволяет создавать программы анализа сетевых данных, поступающих на сетевую карту компьютера. Она написана для использования языка C/C++ так что другие языки, такие как Java, .NET и скриптовые языки использовать не рационально. Для Unix-подобных систем используют libpcap библиотеку, а для Microsoft Windows NT используют WinPcap библиотеку.

Для чего используется Wireshark?

•Системные администраторы используют его для решения проблем в сети; Аудиторы безопасности используют его для выявления проблем в сети; Разработчики используют его для отладки сетевых приложений; Обычные пользователи используют его для изучения внутреннего устройства сетевых протоколов.

Так каковы же возможности Wireshark?

- Перехват трафика сетевого интерфейса в режиме реального времени. Wireshark может перехватывать трафик различных сетевых устройств, отображая его имя (включая беспроводные устройства). Поддерживаемость того или иного устройства зависит от многих факторов, например от операционной системы.
- Сохранение и открытие ранее сохраненного сетевого трафика.
- Импорт и экспорт файлов из других пакетных анализаторов. Wireshark может сохранять перехваченные пакеты в большое количество форматов других пакетных анализаторов, например: libpcap, tcpdump, Sun snoop, atmsnoop, Shomiti/Finisar Surveyor, Novell LANalyzer, Microsoft Network Monitor, AIX's iptrace.
- Позволяет фильтровать пакеты по множеству критерий.
- Позволяет искать пакеты по множеству критерий.
- Позволяет подсвечивать захваченные пакеты разных протоколов.

- Позволяет создавать разнообразную статистику.

Неужели Wireshark умеет делать все?

К сожалению нет. Ниже перечислены некоторые вещи, которые Wireshark делать не умеет.

- Wireshark – это не система обнаружения вторжений. Он не предупредит о том, если кто-то делает странные вещи в сети. Однако если это происходит, Wireshark поможет понять что же на самом деле случилось.
- Wireshark не умеет генерировать сетевой трафик, он может лишь анализировать имеющийся. В целом, Wireshark никак не проявляет себя в сети, кроме как при резолвинге доменных имен, но и эту функцию можно отключить.

Первый шаг. Как "расположить" Wireshark.

После осознания проблемы и принятия решения о использовании Wireshark, первый шаг должен быть решением гле разместить Wireshark. Для этого следует иметь точную схему сети (по крайней мере той части сети которя имеет отношение к нашему тестированию). Принцип заключается в поиске устройства которое вы хотите контролировать, подключении ноутбука с Wireshark к тому же самому коммутатору и конфигурирования зеркального порта или монитора для контроля устройства.

Эта операция позволяет наблюдать весь трафик наблюдаемого устройства как входящий, так и исходящий. Вы можете мониторить LAN порт, WAN порт, порт сервера или маршрутизатора, или любое другое устройство подключенное к сети.

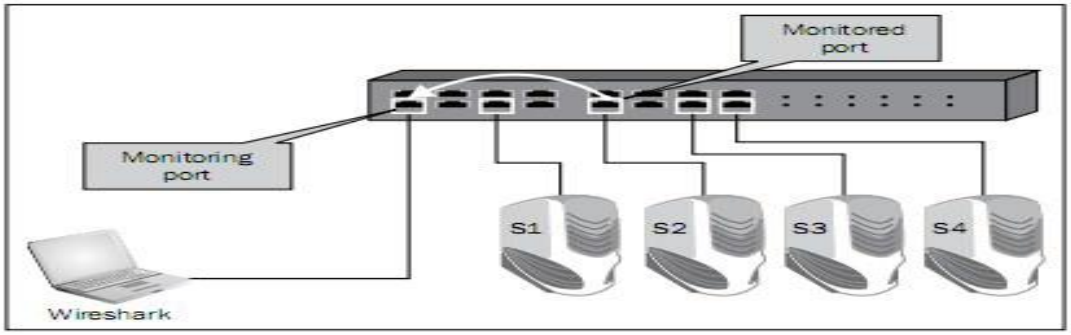


Рис.1.

Рисунок 1 показывает ПО Wireshark (установленное на компьютере слева) и зеркальный порт, так же называемый портом мониторинга (настраиваемый на коммутаторе в направлениях показанных на рисунке), которое будет мониторить весь трафик входящий и исходящий с сервера S2.

Конечно, можно установить Wireshark непосредственно на самом сервере, и наблюдать трафик непосредственно на нём.

Виды мониторинга

1. *Мониторинг сервера*

Это одно из наиболее распространённых требований с которым придётся сталкиваться. Может быть выполнено либо путём конфигурирования порта мониторинга для сервера или путём установки Wireshark непосредственно на сам сервер.

2. *Мониторинг маршрутизатора*

Для мониторинга маршрутизатора, мы можем мониторить порт LAN или WAN порт. Мониторинг LAN порта весьма прост - просто сконфигурируйте портмонитор на контролируемый порт. Для мониторинга WAN порта требуется подключить коммутатор между портом маршрутизатора и сетью поставщика услуг (ISP) и сконфигурировать портмонитор на этом коммутаторе, как показано на рисунке 2.

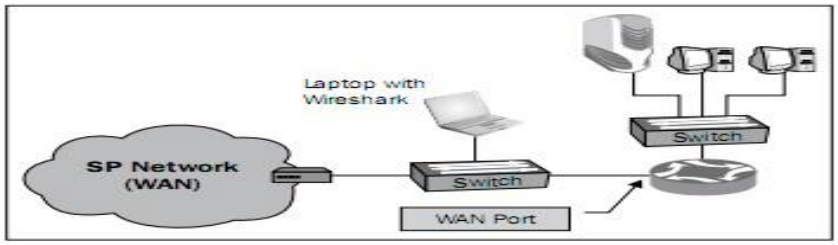


Рис.2.

Подключение коммутатора между маршрутизатором и ISP является операцией прерывающей связь; однако, когда вы полностью подготовлены, она занимает менее минуты.

При мониторинге маршрутизатора не стоит забывать, что не все пакеты входящие в маршрутизатор будут переправляться. Некоторые пакеты могут быть потеряны, сброшены в буфер маршрутизатора или направлены обратно на тот же порт с которого они пришли.

Можно использовать два дополнительных устройства TAP и HUB

TAP **-** Вместо подключения коммутатора на линк который вы хотите мониторить, вы можете подключить устройства называемое тестовая точка доступа (Test Access Point (TAP)), которая является простым трёхпортовым устройством, и в данном случае будет играть ту же роль, что и коммутатор.

Концентраторы (HUB) **-** Вы можете просто подключить концентратор параллельно к контролируемому линку, и поскольку концентратор является полудуплексным устройством, каждый пакет передаваемый между маршрутизатором и сетью ISP будет наблюдаться на Wireshark.

3. *Мониторинг брандмауэра*

Мониторинг брандмауэра может различаться в зависимости от того мониторится ли внутренний или внешний порт. На внутреннем порту вы увидите все внутренние адреса и весь трафик инициированный пользователями, работающими в нутренней сети, в то время, как на внешнем порту вы будете видеть внешние адреса с которых мы выходим (транслируемые с помощью NAT с внутренних адресов); вы не увидите

запросы внутренней сети которые были блокированы брандмауэром. Если кто-то атакует брандмауэр из сети интернет, вы будете видеть это только на внешнем порту.

Коммутатор локальной сети пересылает пакеты следующим образом:

1. Коммутатор постоянно изучает MAC адреса подключенных к нему устройств.
2. Теперь, если посылается к MACадресу назначения, то он будет направлен только на тот физический порт на котором, по данным коммутатора находится данный MAC адрес.
3. Если отправляется широковещательный запрос, он будет направляться на все порты коммутатора.
4. Если отправляется групповой запрос (мультикаст), а протокол CGMP (Cisco Group Management Protocol) или IGMP (Internet Group Management Protocol) отключен, то он будет пересылаться на все порты коммутатора (Протоколы CGMP и IGMP позволяют направлять мультикаст пакеты только на устройства конкретной многоадресной группы).
5. Если пакет передаётся на MAC адрес неизвестный коммутатору (случай весьма редкий), он будет передан на все порты коммутатора.

Поэтому, когда вы конфигурируете портмонитор на конкретном порту, вы увидите весь его входящий/исходящий трафик. Если вы подключите свой компьютер к сети ничего не настраивая, вы увидите только входящий/ исходящий трафик своего компьютера, и кроме того широковещательный и групповой трафик сети.

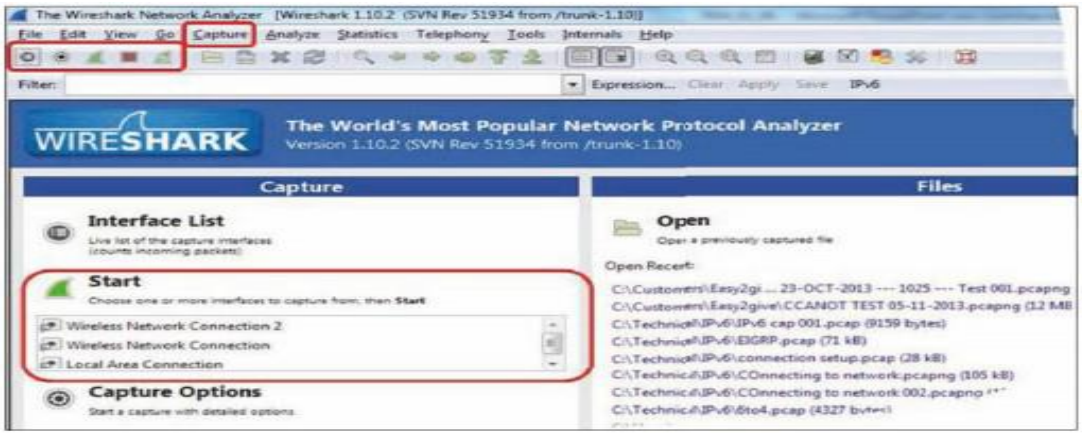
Инсталяция Wireshark

Для начала работы с Wireshark, перейдите на сайт Wireshark и загрузите последнюю версию инструмента. Обновлённая версия Wireshark может быть найдена на сайте http://www.wireshark.org/, в подзаголовке Download. Загрузите последний стабильный релиз Wireshark доступный по адресу http://www.wireshark.org/download.html.

Каждый пакет Wireshark для Windows содержит последний стабильный релиз WinPcap, который требуется для живого захвата пакетов. WinPcap драйвер это Windows версия библиотеки libpcap систем Unix предназначенной для захвата трафика.

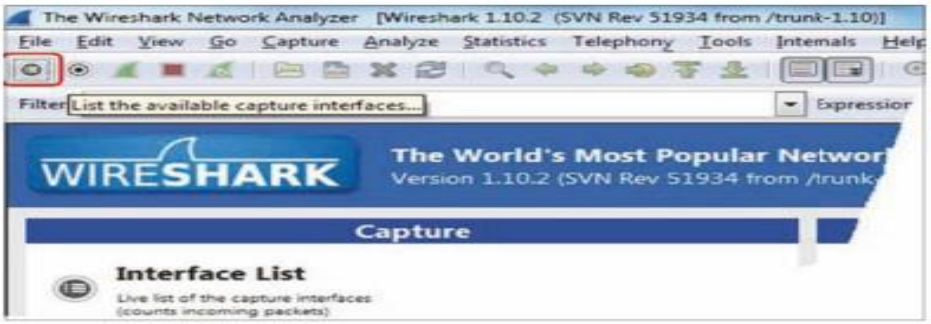
Запуск захвата данных

После инсталляции Wireshark на своём компьютере, единственное что остаётся сделать - запустить анализатор с рабочего стола, из Program Files или с панели быстрого запуска. После запуска откроется следующее окно

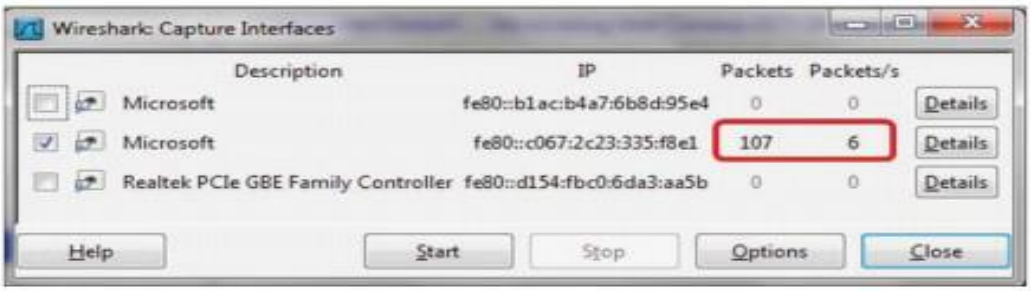


Вы можете начать захват из меню Capture или с панели быстрого запуска выбрав кнопку с символом захвата, или из центрального левого окна Capture на основном экране. Если вы просто нажмёте на третью справа зелёную иконку, и начнёте захват, Wireshark начнёт захват с интерфейса по умолчанию, в соответствии с конфигурацией программного обеспечения.

Для того, чтобы выбрать интерфейс на котором вы хотите произвести захват, нажмите на иконку Список интерфейсов доступных для захвата (List the available capture interfaces) и Wireshark откроет окно Интерфейсы захвата (Wireshark Capture Interfaces).

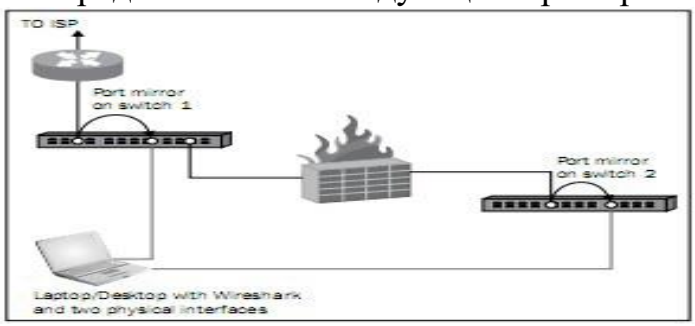


Лучший способ разобраться какой интерфейс активен просто посмотреть на правую часть окна интерфейсов, где виден проходящий трафик. Здесь вы увидите общее число пакетов (Packets) видимых Wireshark, и число пакетов в секунду (Packets/sec) на каждом интерфейсе.

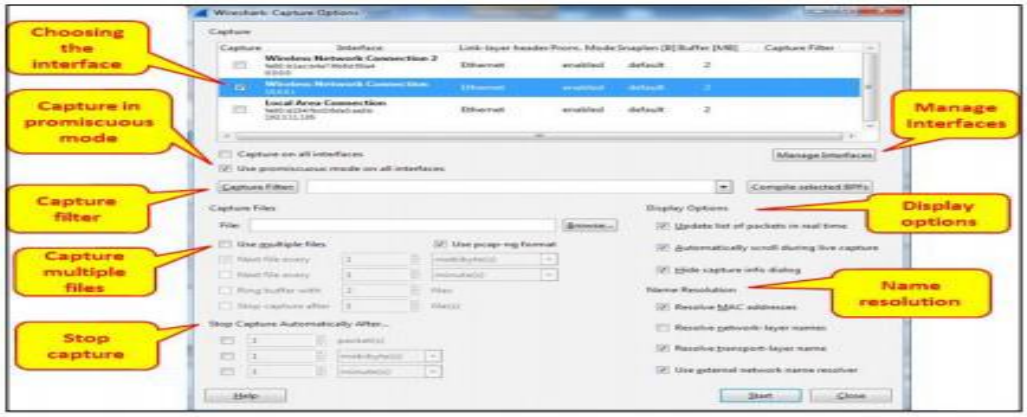


Начиная с версии 1.10.2, вы можете выбрать один или несколько интерфейсов для захвата. Это бывает полезно во многих случаях: например, когда у вас есть несколько физических сетевых карт, вы можете мониторить порт на двух различных серверах, два порта на

маршрутизаторе или несколько различных портов одновременно. Типовая конфигурация сети представлена на следующем примере:



Для конфигурирования интерфейса, с которого вы планируете захватывать данные, выберите пункт Опции (Options) из меню захвата (Capture). Откроется следующее окно:



В этом окне вы можете настроить следующие параметры:

1. В верхней части окна, выберите интерфейс с которого планируете выполнять захват данных.
2. В левой стороне окна имеется флаг Использовать неразборчивый режим на всех интерфейсах (Use promiscuous mode on all interfaces). Когда он установлен, Wireshark будет захватывать все пакеты получаемые компьютером. Если флаг снят, будут фиксироваться только пакеты предназначенные данному компьютеру.
3. В некоторых случаях, когда этот флаг установлен, Wireshark не будет захватывать данные на беспроводном интерфейсе; так что, если вы начинаете захват данных на беспроводном интерфейсе и ничего не видите снимите этот флаг.
4. В среднейлевой области окна имеется поле Файлы захвата (Capture Files). Здесь вы можете записать имя файла, и Wireshark будет сохранять файл захвата с этим именем, и с дополнением 0001, 0002, и так далее, по указанному вами пути. Эта особенность крайне важна когда производится захват большого объёма данных; например, когда производится захват данных на сильно нагруженном интерфейсе, или в течение длительного периода времени. Вы можете

указать программе открывать новый файл после указанного интервала времени, размера файла или числа пакетов

5. В нижнейлевой части окна имеется область отмеченная как Автоматическая остановка захвата (Stop Capture Automatically), показанная на предыдущем снимке. В этой области вы можете указать программе, что необходимо остановить захват данных после указанного интервала времени, при достижение указанного размера файла или числа пакетов.
6. В средней правой области окна вы можете менять опции отображения (Display) и выбрать флаги Обновлять список пакетов в реальном времени (Update list of packets in real time), Автоматически прокручивать вывод захвата (Automatically scroll during live capture) и Скрыть диалог информации захвата (Hide capture info dialog), закрывающее раздражающее окно объявления захвата (всплывающее в момент начала захвата). В большинстве случаев здесь не требуется вносить изменения.
7. В нижней правой части окна, вы можете настроить опции разрешения для MAC адресов, IP DNS имён, и номеров портов TCP/UDP. Наконец флаг Использовать разрешение имён из внешней сети (Use external network name resolver), используется для настройки разрешения имён (в большинстве случаев DNS), для разрешения сетевых имён.

В случаях, когда важно время проведения захвата, и вам требуется произвести захват данных на одном или более интерфейсах, с учётом синхронизации времени с сервером который вы мониторите, вы можете использовать сетевой протокол времени (Network Time Protocol NTP) для синхронизации Wireshark и контролируемого сервера с центральным источником времени. Это важно в том случае, если вам необходимо сопоставить файл захвата файлу журнала сервера (logфайлу) и отыскать совпадающие события.

Например, если вы видите повторные передачи в файле захвата и, в то же время ошибки приложения в журнале наблюдаемого сервера, вы можете понять, что повторные передачи возникают из-за ошибок сервера, а не из-за проблем сети.

Программа Wireshark получает время от часов ОС (Windows, Linux и прочих). Для конфигурации операционной системы для работы с сервером времени вам следует обратиться к соответствующему руководству по вашей операционной системе.

В Microsoft Windows 7 настройка производится следующим образом:

1. Перейдите в панель управления
2. Выберите Время, Язык и Регион
3. На вкладке Дата и время, выберите Установить время и дату и выберите закладку Время Интернет.
4. Щёлкните на кнопке Сменить настройку.

5. Укажите сервер времени или IP адрес.

[*В Microsoft Windows 7 и более новых версиях есть настройка по умолчанию для сервера времени. Пока все устройства настроены на него, вы можете использовать его, как любой другой сервер времени.*]

NTP это сетевой протокол используемый для синхронизации времени. Когда вы настраиваете свои сетевые устройства (маршрутизаторы, коммутаторы, брандмауэры и прочие) и сервера на один и тот же источник времени, они синхронизируются по времени этого источника. Точность синхронизации зависит от точности сервера времени, измеряемой в уровнях и стратумах.

Более высокий уровень является наиболее точным. Самым высоким является уровень 1. Обычно, вам придётся иметь дело с уровнями от 2 до 4. Сначала, NTP был стандартизирован в RFC 1059 (NTPv1), а затем в RFC 1119 (NTPv2); в последнее время общепринятыми версиями являются NTPv3 (RFC1305) и NTPv4 (RFC 5905).

На различных сайтах вы можете получить список серверов NTP, в том числе:

http://support.ntp.org/bin/view/Servers/StratumOneTimeServers

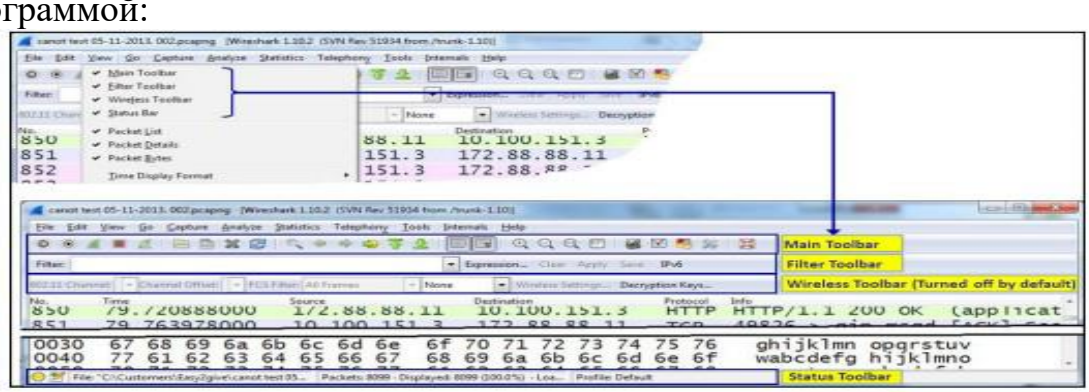
http://wpollock.com/AUnix2/NTPstratum1PublicServers.htm

Настройка стартового окна

Есть несколько параметров, которые здесь можно изменить, чтобы настроить стартовое окно в соответствии с вашими потребностями:

- Настройка панели инструментов
- Настройка основного окна
- Настройка формата времени
- Разрешение имён
- Колоризация списка пакетов
- Автоскроллинг живого захвата
- Увеличение
- Конфигурация столбцов
- Правила колоризации

Сначала, давайте рассмотрим панели инструментов используемые программой:



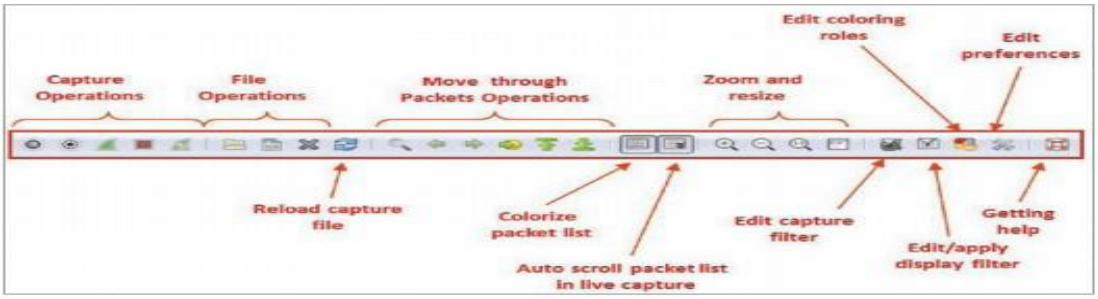
Рассмотрим следующие панели инструментов:

- Главная панель инструментов (Main Toolbar)

- Панель инструментов фильтров отображения (Display Filter Toolbar)
- Строка состояния (Status Bar)

1. *Главная панель инструментов*

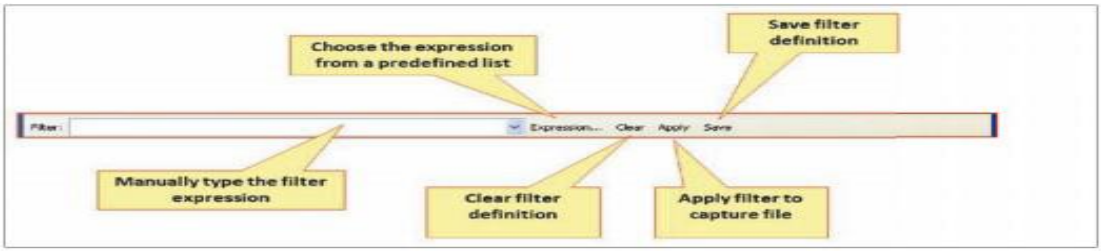
Главная панель инструментов содержит иконки показанные на следующем снимке:



Пять самых левых символов используются для управления захватом, затем идут иконки для управления файлом, управления увеличением и "переходом к пакету", колоризацией и автоскролингом, увеличением и измением размера, фильтры, настройки и помощь.

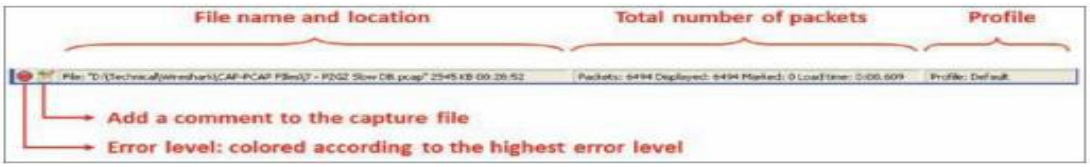
2. *Панель инструментов фильтров отображения*

В панели фильтров отображения имеются следующие поля:



3. *Строка состояния*

В статусная строке находящейся в нижней части окна Wireshark, вы можете видеть данные показанные на следующем снимке:

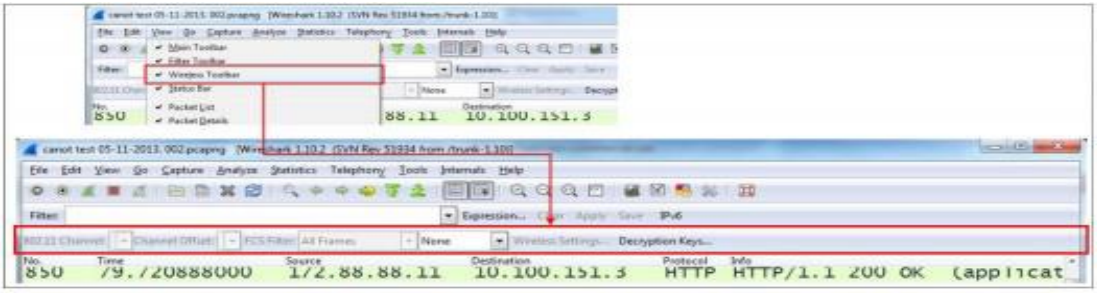


На показанном снимке вы можете видеть:

- Ошибки в экспертной системе.
- Опции для добавления комментариев в файл.
- Имя файла захвата (в процессе захвата будет показано временное имя назначенное программой).
- Общее количество перехваченных пакетов, отображаемые пакеты (те которые на самом деле отображаются на экране) и отмеченные пакеты (те которые вы отметили).

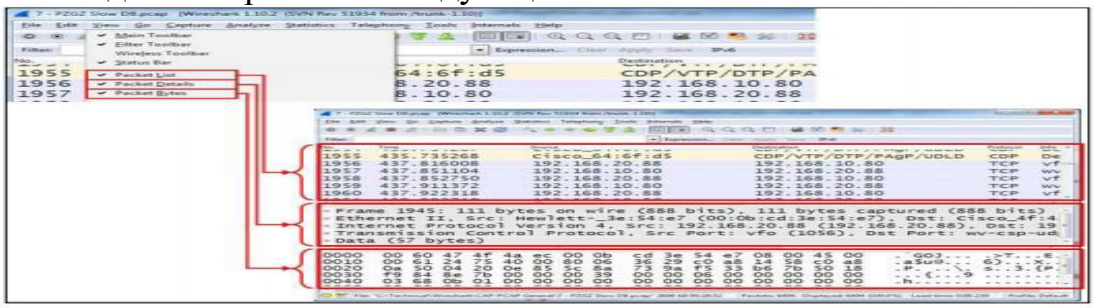
Конфигурация панели инструментов

Обычно, для регулярного захвата пакетов, вам не придётся ничего менять. Но всё меняется, когда вам необходимо захватить данные беспроводной сети (не только с вашего ноутбука); вам потребуется включить панель инструментов беспроводной сети, и вы сможете это сделать, щёлкнув по нему в меню Вид (View), как показано на следующем снимке:



Настройка основного окна

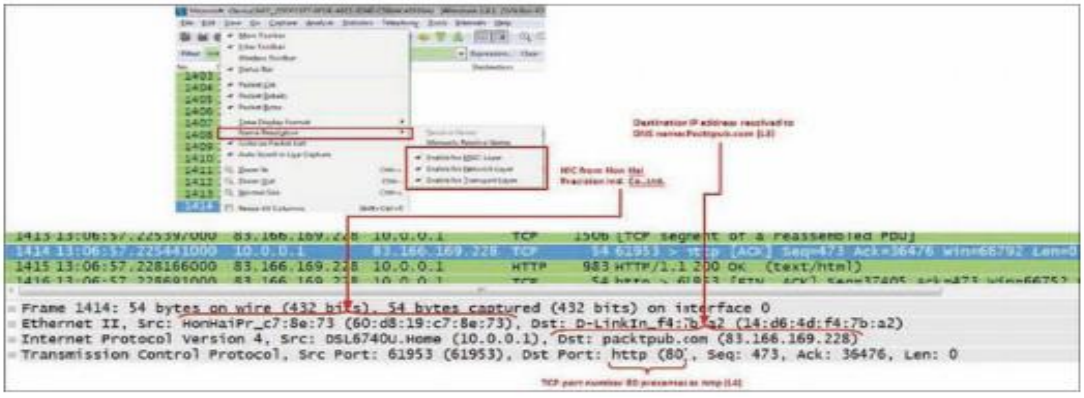
Настраивая главное меню для захвата, вы можете сконфигурировать Wireshark для отображения следующих окон:



В большинстве случаев вам не потребуется что то здесь менять. В некоторых случаях, вы можете закрыть байты пакеты, если они вам не требуются и получить больше места для списка пакетов и деталей пакета.

Разрешение имён

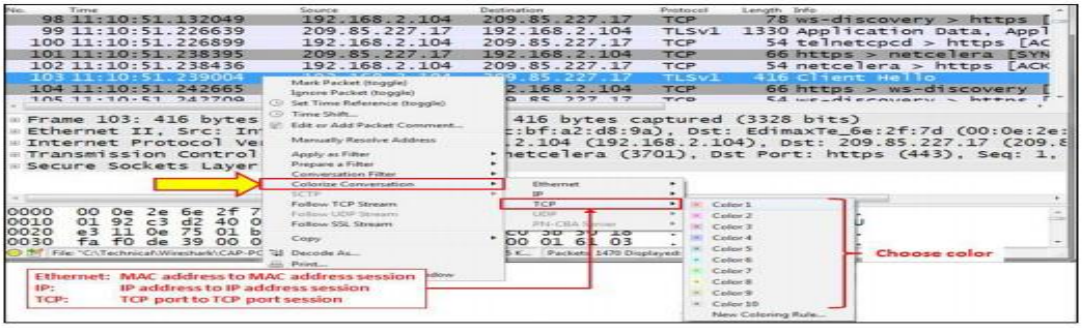
Разрешение имён это трансляция уровня 2 (MAC адресов), уровня 3 (IP адресов) и уровня 4 (Номера портов) в более значимую информацию.



На предыдущем снимке, вы можете видеть MAC адрес 60:d8:19:c7:8e:73 (с Hon Hai Precision Ind, используемым Lenovo), webсайт (Packtpub.com) и номер порта HTTP (80).

Колоризация списка пакетов

Обычно, вы начинаете захват с целью определения основного профиля нормального вида трафика вашей сети. В процессе захвата, вы рассматриваете захваченные данные и можете найти TCP соединения, IP или Ethernet подключения, которые захотите выделить другим цветом. Для того, чтобы сделать это, щёлкните правой кнопкой мыши на пакете, цвет которого вы хотите изменить, выберите Ethernet, IP или TCP/UDP (появление TCP или UDP будет зависеть от типа пакета), и выберите соответсвующий цвет обозначения. В примере вы видите, что мы хотим выделить цветом определения Transport Layer Security (TLS).



Для отмены правил колоризации:

1. Перейдите в меню Вид (View)
2. В нижней части меню выберите Reset Coloring 110 или просто нажмите Ctrl+Пробел.

Настройка правил колоризации и способы навигации

Правила колоризации определяют то, как Wireshark будет окрашивать протоколы и события в захваченных данных. Работа с правилами колоризации значительно облегчит вашу работу с решением сетевых проблем, так как у вас появится возможность выделять различные протоколы и различные события различными цветами.

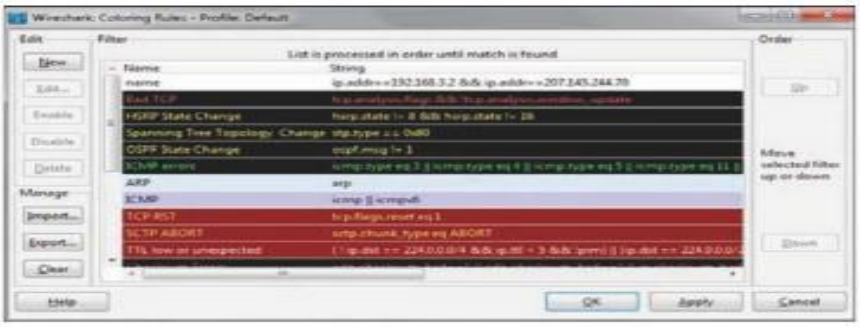
Правила колоризации позволяют настроить новые правила в соответствии с различными фильтрами. Это позволяет настраивать различные схемы колоризации для различных сценариев и сохранять их в различных профилях. Следовательно, вы можете настроить одни правила колоризации для решения вопросов TCP, другие правила для решения проблем телефонии и SIP, и так далее.

[*Вы можете настроить профили Wireshark для сохранения конфигурации Wireshark; например предопределённые цвета, фильтры и прочее. Для этого перейдите в Конфигурацию профилей (Coniguration Proiles) меню Редактирование (Edit).***]**

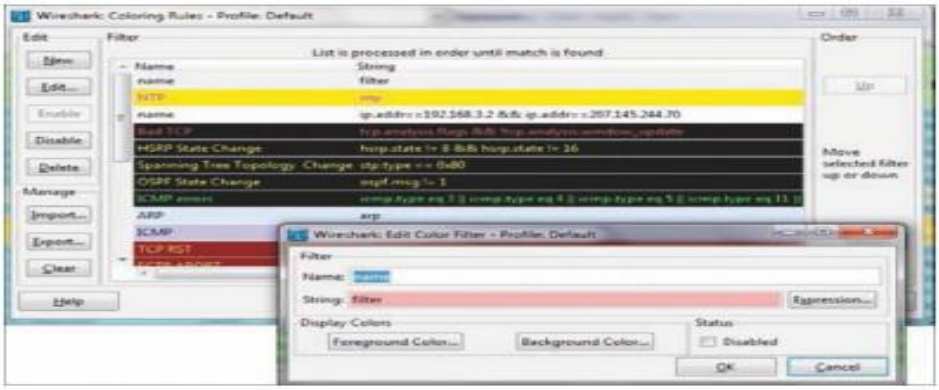
Для начала работы с правилами колоризации, выполните следующие действия:

1. Перейдите в меню Вид (View).

2. В нижней части меню выберите Правила колоризации (Coloring Rules). Вы должны увидеть следующее окно:



Теперь перейдём к правилам колоризации:
Щёлкните на кнопке Новое (New), и вы должны увидеть следующее окно:



Для настройки нового правила колоризации, выполните следующие действия:

1. В поле Имя (Name), введите имя правила. Например, наберите NTP для сетевого протокола времени.
2. В поле Строка (String), заполните строку фильтра, т.е. то, что должно показывать это правило. Вы можете щёлкнуть на кнопке выражения и получить список преднастроенных фильтров.
3. Щёлкните на кнопке Цвет переднего плана (Foreground Color) и выберите цвет переднего плана для правила. Это будет основной цвет пакета в списке пакетов.
4. Щёлкните на кнопке Цвет заднего плана (Background Color) и выберите цвет фона для правила. Это будет цвет фона пакета в списке пакетов.
5. Щёлкните на кнопку Редактирование (Edit) если вы хотите отредактировать существующие правила. Так же, вы можете щёлкнуть по кнопке Импорт (Import) для импорта существующей цветовой схемы, или щёлкнуть по кнопке Экспорт правила (Export rule) для экспортирования текущей схемы.

[*Существует важность порядка правил колоризации. Убедитесь, что покрядок правил колоризации соответствует порядку реализации. Например, протоколы прикладного уровня должны идти до TCP или UDP, так чтобы цвета Wireshark соответствовали их цветам, а не цветам регулярного TCP или UDP.***]**

Различные типы схем колоризации, наряду со многими другими

примерами, вы можете найти на http://wiki.wireshark.org/ColoringRules, и простым поиском в сети Интернет

Автоскроллинг живого захвата

Для настройки автосскроллинга пакетов живого захвата, сделайте следующее:

1. Перейдите в меню Вид (View).
2. Отметьте пункт Auto Scroll (автоскроллинг) в элементе Live Capture (живой захват).
3. Увеличить (Zoom)

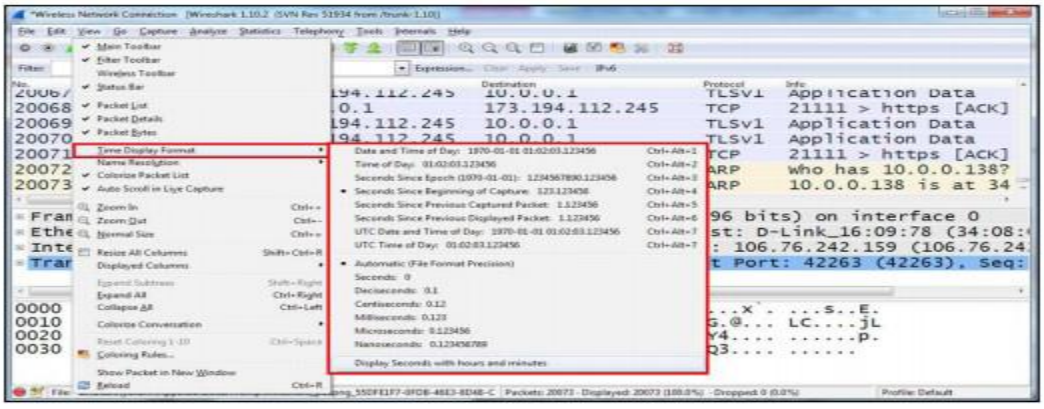
Для увеличения и уменьшения масштаба :

1. Перейдите в меню Вид (View)
2. Щёлкните на Zoom in или нажмите Ctrl + "+" для увеличения.
3. Щёлкните на Zoom out или нажмите Ctrl + "-" для уменьшения масштаба.

Использование значений времени и сводок

Конфигурация времени говорит о том, как будут представлены данные в столбце времени (второй слева в конфигурации по умолчанию). В некоторых сценариях этому придаётся существенное значение; например, в соединениях TCP, вы хотите видеть временные интервалы между пакетами, когда вы захватываете данные из нескольких источников и вы хотите видеть точное время каждого пакета и так далее.

Для настройки формата времени, перейдите в меню Вид (View), и в подменю Time Display Format (формат отображения времени) вы увидите:



Вы можете выбрать один из следующих вариантов:

- *Date and Time of Day* (дата и время дня первые два варианта): Это хорошая конфигурация когда вы решаете проблему сети связанную с событиями зависящими от времени, например, когда вы знаете о событии которое происходит в указанное время и хотите посмотреть то, что происходит в данный момент в сети.
- *Second Since Epoch* (секунд с начала эпохи): Время в секундах с 1 января 1970 года. Эпоха это произвольная дата выбранная в качестве начала отсчёта времени системы, и 1 января 1970 года выбрано для Unix и Unixподобных систем.
- *Second Since Beginning of Capture* (секунд с начала захвата):

Конфигурация по умолчанию.

- Seconds Since Previous Captured Packet (секунд с предыдущего захваченного пакета): Общая возможность, позволяющая увидеть разницу во времени между пакетами. Может быть полезна при мониторинге трафика чувствительного ко времени (когда разница во времени между пакетами является важной), например соединения TCP, живого потокового видео, вызовы VoIP и прочее.
- *Seconds Since Previous Displayed Packet* (секунд с предыдущего отображённого пакета): Полезная функция, которая может использоваться при настройке фильтра отображения, когда представляются только выделенные части данных захвата (например поток TCP). В этом случае, вы увидите разницу во времени между пакетами, что может быть важно в некоторых приложениях.
- *UTC* Date and Time of Day (Дата UTC и время дня): Представление относительно времени UTC. В нижней части подменю предоставлен формат отображения времени. Изменяйте его только в том случае, если требуется более точное представление времени.

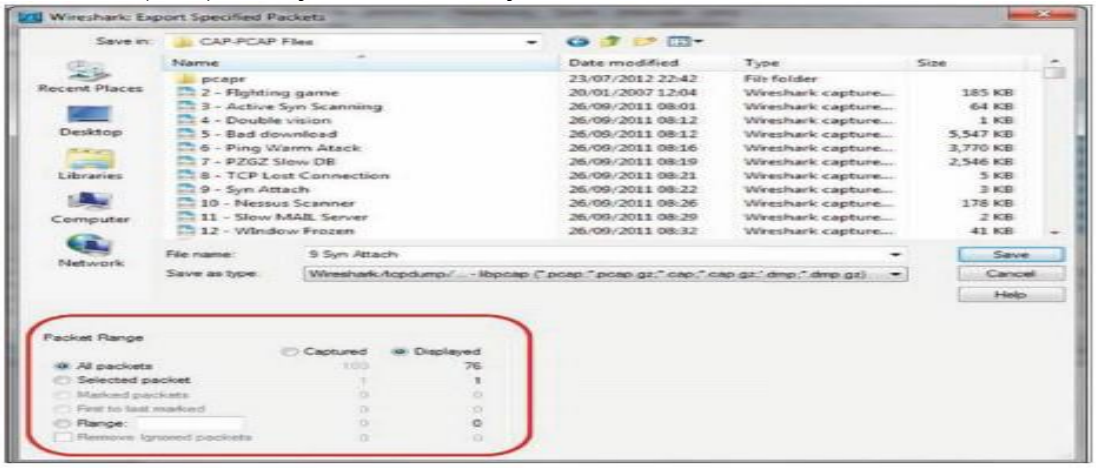
Кроме того, вы можете использовать Ctrl+Alt+<любую цифровую клавишу> для различных варинтов.

Сохранение, печать и экспорт данных

Мы можем сохранить целый файл и экспортировать специфические данные в различных форматах и типах файлах. В следующих параграфах мы увидим как это сделать. Для сохранения всего файла с захваченными данными, выполните следующие действия:

1. В меню Файл (File), щёлкните по кнопке Сохранить (Save) или нажмите Ctrl+S для сохранения файла с новым именем.
2. В меню Файл (File), щёлкните на кнопке Сохранить как... (Save as...) или нажмите Shift+Ctrl+S для сохранения файла с новым именем.

Для сохранения части файла, например, только отображённых данных перейдите к Экспорт указанных пакетов (Export Specified Packets) в меню Файл (File). Вы увидите следующее окно:



1. В нижней левой части окна, вы увидите, что имеется возможность выбрать, какую часть данных вы хотите сохранить.

2. Для сохранения всех захваченных данных, выберите Все пакеты и Захваченные (All packets and Captured).
3. Для сохранения только отображаемых данных, выберите Все пакеты и Отображённые (All packets and Displayed).
4. Для сохранения только выбранных пакетов из файла (выбранные пакеты - просто пакеты которые вы отметили щелчком), укажите Выбранные пакеты (Selected packet).
5. Для сохранения отмеченных (маркированных) пакетов (т.е. пакетов которые были отмечены щелчком правой кнопки на них в списке пакетов, и выбором переключателя Маркировать пакет (Marked packet) из контекстного меню), выберите Маркированные пакеты (Marked packet).
6. Для сохранения пакетов между двумя маркированными пакетами, выберите опцию С первого до последнего отмеченного (First to last marked).
7. Для сохранения диапазона пакетов, выберите Диапазон (Range) и укажите диапазон пакетов который необходимо сохранить.
8. В окне списка пакетов, вы можете вручную выбрать игнорируемые пакеты. В окне Экспорт (Export) вы можете игнорировать эти пакеты и не сохранять их. Во всех упоминаемых опциях, вы можете выбрать пакеты из всего файла захвата или из пакетов отображаемых на экране (пакеты отображаются в списке пакетов после применения фильтра отображения).

Сохранение данных в различных форматах

Вы можете сохранить данные полученные с помощью Wireshark в различных форматах, для дальнейшего анализа с помощью других инструментов.

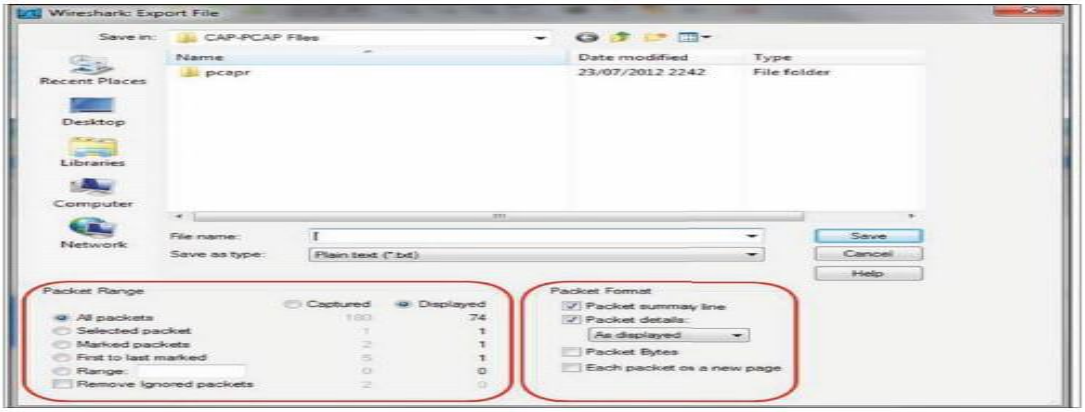
Вы можете сохранить файл в следующих форматах:

- Обычный текст (plain text, *.txt): экспорт пакетов данных в простом ASCII.
- PostScript (*.ps): экспорт данных в формате PostScript.
- Значения разделённые запятыми (Comma Separated Values, *.csv):экспорт пакетов в файле формата CSV, для использования с программами табличных процессоров (например Microsoft Excel).
- C Arrays to Packet Bytes (*.c): экспорт байт пакетов в Си массив, для импортирования программ Си.
- PSML or XML Packet Summary (*.psml): экспорт данных пакетов в PSML, формат на основе XML, включающий только итоговые пакеты. Более подробная информация:

http://www.nbee.org/doku.php?id=netpdl:psml_specification.

•PDML XML Packet Details (*.pdml): экспорт данных пакетов в PDM, формат на основе XML, включающий детали пакетов. Более подробная информация: http://www.nbee.org/doku.php?id=netpdl:pdml_specification.

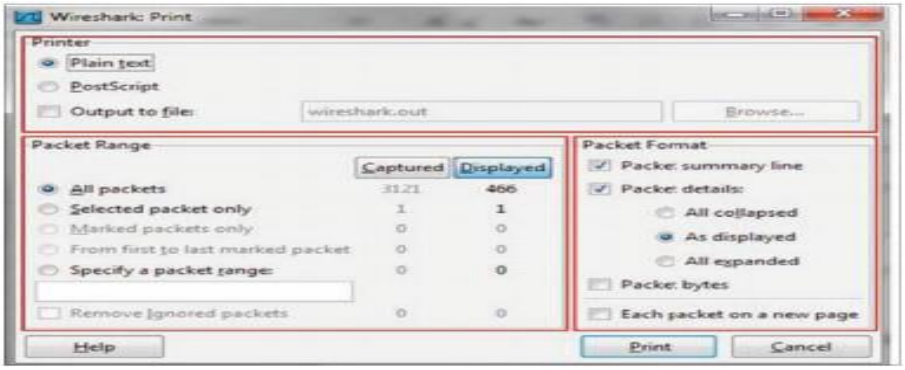
Для сохранения файла, выберите Export Packet Dissections из меню Файл (File) и вы должны увидеть следующее окно:



В предыдущем снимке, маркированный список в левой стороне окна предоставляет выбор пакетов которые вы хотите сохранить. Процесс выглядит так же, как и в предыдущем рецепте. В маркированном списке справа, вы указываете формат файла для сохранения.

Как печатать данные

Для того, чтобы напечатать данные, щёлкните на кнопку Печать (Print) в меню Файл (File), и вы получите следующее окно:



Окно печати Wireshark предоставляет следующие опции:

- В верхней части окна выберите формат файла для печати.
- В нижней левой части окна, выберите пакеты для печати (аналогично окну Export).
- В нижней правой части окна выберите формат печати данных и данные панели для печати из окна Wireshark:
- Панель Итоги пакета (Packet Summary)
- Панель Детали пакета (Packet Detail)

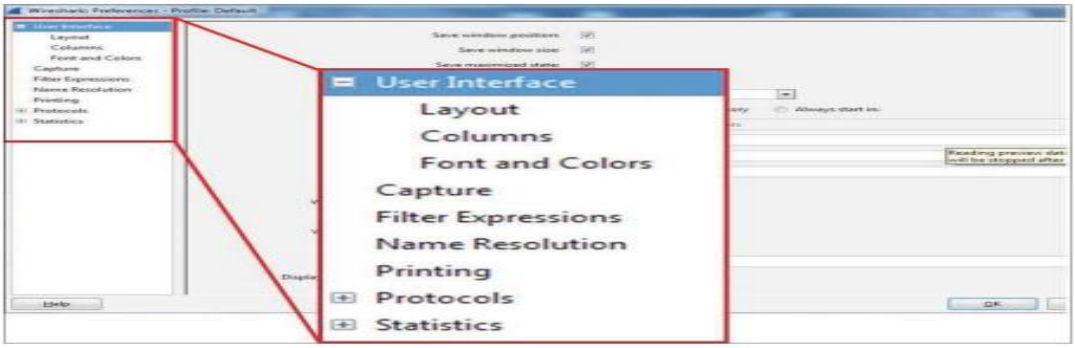
Данные могут печататься в текстовом формате, postscript (для принтеров поддерживающих postscript) или в файл. После настройки этого окна и щелчка на кнопке Print, появится стандартное окно печати, и вы сможете выбрать принтер.

Настройка пользовательского интерфейса в меню Настройки (Preferences)

Существует большое количество параметров, которые вы можете изменить в окне Preferences, включая представление данных, место, где по

умолчанию сохраняются файлы, интерфейс Wireshark, по умолчанию используемый при захвате данных и прочее.

Для настройки пользовательского интерфейса, выберите пункт Preferences из меню Редактирования (Edit). Будет открыто следующее окно:

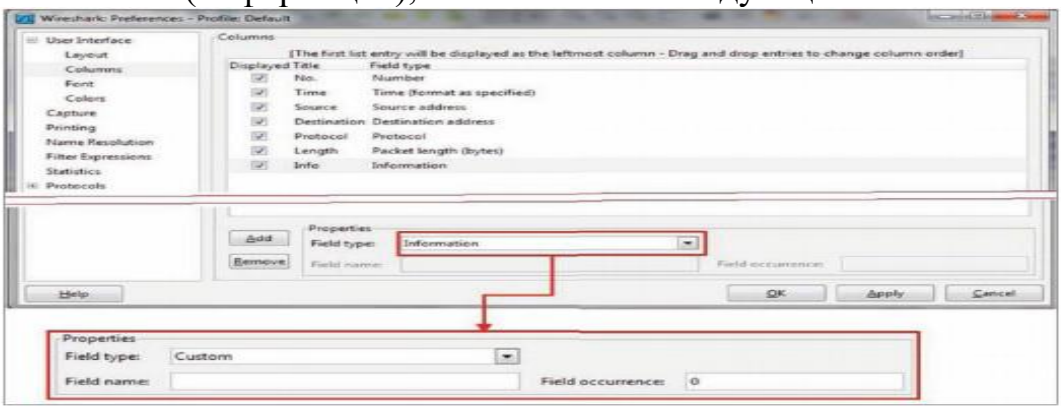


Мы увидим настройки следующих параметров:

- Столбцы
- Захват
- Разрешение имён

Изменение и добавление столбцов

Столбцы по умолчанию, которые мы видим в панели пакетов, это столбцы number (номер), time (время), source (адрес источника) and destination addresses(адрес назначения), protocol (протокол), length (длина), and information (информация), показанные на следующем снимке:



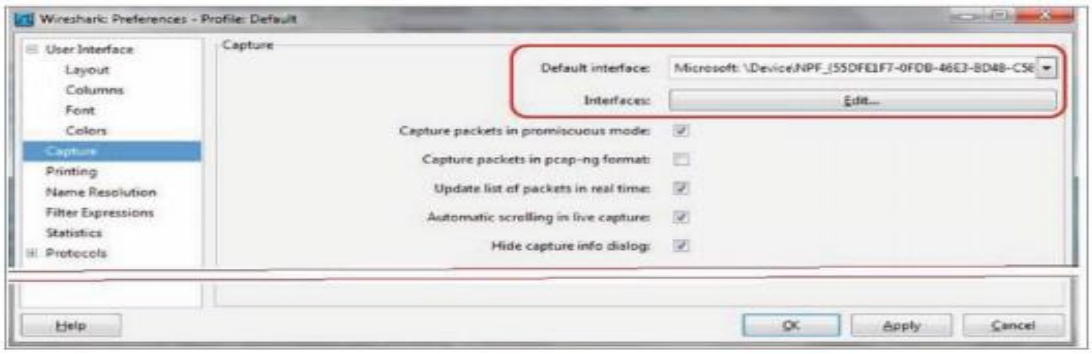
Для добавления нового столбца к панели пакета:

1. Вы можете выбрать один из предопределённых параметров, который будет добавлен в виде нового столбца указанного в Field type (Типе поля). Среди этих параметров time delta (дельта времени), значение IP DSCP, port numbers (номер порта), и другие.
2. Очень важная возможность появится, когда в Filed type вы укажите Custom. В этом случае, вы можете заполнить строку поля Field name (Имя поля) любым фильтром. Например, вы можете добавить следующее:
    - Добавьте строку tcp.window_size для просмотра размера окна TCP (значение влияет на производительность).
    - Добавьте строку ip.ttl для просмотра параметра IP TTL (TimeToLive время жизни) каждого пакета.

- Добавьте rtp.marker для просмотра каждого экземпляра установленного маркера в пакете RTP.

Смена конфигурации захвата

Есть некоторые параметры, которые можно настроить до начала захвата данных. В окне Preferences выберите меню Capture (Захват) и вы увидите следующее окно:



Для изменения интерфейса по умолчанию с которого производится захват, просто нажмите кнопку Редактирования (Edit) и отметьте интерфейс который желаете использовать по умолчанию. Конечно, вы можете изменять его каждый раз вручную, это значение просто используется по умолчанию.

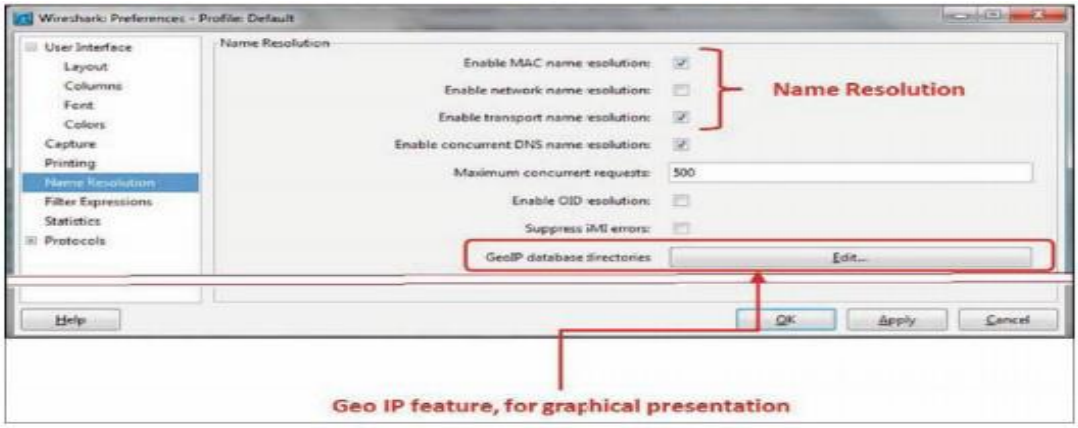
Настройка разрешения имён

Wireshark поддерживает разрешение имён на трёх уровнях:

Уровень 2: разрешается первая часть MAC адреса с именем производителя. Например, 14:da:e9 будет представлено, как AsusTeckC (ASUSTeK Computer Inc.).

Уровень 3: разрешается IP адрес в имена DNS. Например 157.166.226.46 будет разрешён в www.edition.cnn.com.

Уровень 4: разрешается номер порта TCP/UDP в имя порта. Например порт 80 будет разрешён как HTTP, а порт 53 как DNS.



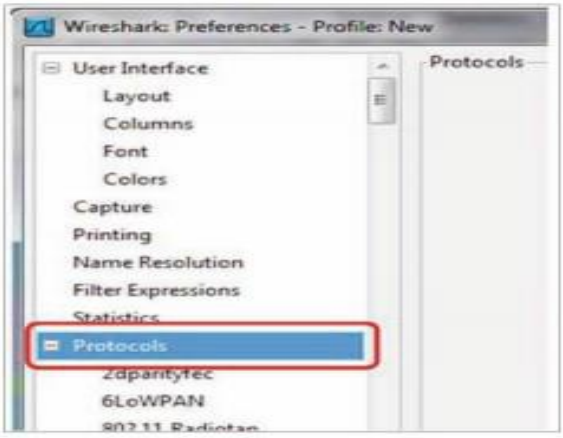
[*В TCP и UDP, имеет смысл только порт назначения, который клиент изначально открывает для сессии. Порт источника, на котором открывается соединение, представляет собой случайное число (большее 1024), а следовательно, не имеет смысла трансляция имени этого порта.*]

По умолчанию, Wireshark разрешает MAC адрес на уровне 2 и номер

порта TCP/UDP на уровне 4. Разрешение IP адресов может привести к замедлению Wireshark, что связано с большим количеством используемых DNS запросов, следовательно, используйте его аккуратно.

Настройка особенностей протоколов

Настройка особенностей протоколов предоставляет возможность изменить способ, которым Wireshark осуществляет захват и представляет общие протоколы. В этом рецепте, мы узнаем, как настраивать наиболее общие протоколы. Перейдите к пункту Preferences меню Edit и вы увидите следующее окно:



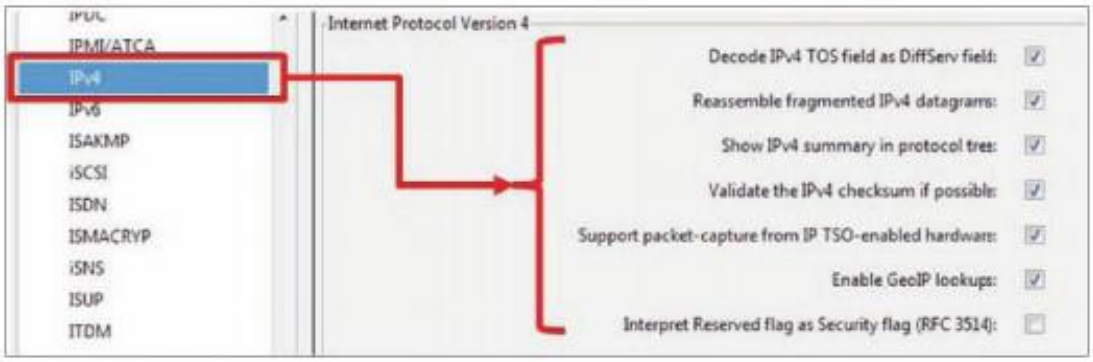
Щёлкните по знаку + слева от Протоколов (Protocols), что приведёт к открытию списка протоколов. В списке протоколов вы обнаружите общие и более редкие протоколы.

Мы будем говорить о следующих базовых протоколах (слово "базовые" означает их повсеместное использование, а не простоту устройства):

- IPv4 и IPv6
- TCP и UDP

Настройка особенностей IPv4 и IPv6

Когда вы начнёте настраивать параметры IPv4 или IPv6, вы увидите следующее окно:



Вы можете изменить следующие параметры:

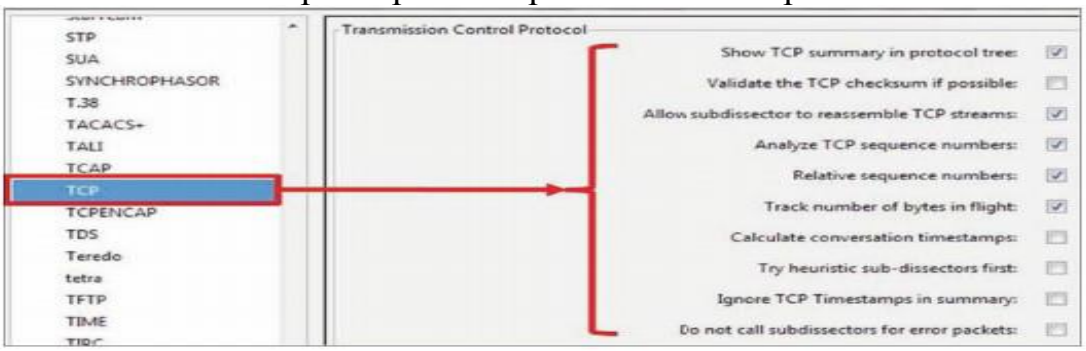
Decode IPv4 ToS field as DiffServ Field (Декодировать поле ToS IPv4 как поле DiffServ): в оригинальном протоколе IP имеется поле названное Type Of Service (Тип сервиса ToS), для включения качества IP сервиса через сеть. В начале 90х годов стандарт Differentiated Services (DiffServ) изменил

способ, которым IP устройства рассматривают это поле. Снятие этого флага будет представлять это поле в соответствии с оригинальным стандартом IP.

Enable GeoIP lookups (Включить выборки GeoIP): GeoIP представляет собой базу данных, позволяющую Wireshark представлять IP адреса как географические локации. Включение этой функции в IPv4 и IPv6 включит подобное представление. Данная функция так же включает в себя разрешение имён и поэтому, может замедлить захват пакетов в реальном времени.

Настройка TCP и UDP

В UDP не так много параметров которые можно изменить. Это очень простой протокол, с весьма простой конфигурацией. С другой стороны, в TCP есть несколько параметров которые можно настроить.



Большинство изменений, которые можно сделать в настройках TCP направлены на то как Wireshark разбирает захваченные данные.

Validate the TCP checksum if possible (Прверять контрольную сумму TCP если возможно): в некоторых сетевых картах вы можете видеть множество "ошибок контрольной суммы". Это связано с тем, что разгрузка контролной суммы TCP часто реализуется на некоторых сетевых картах. Проблемой может стать то, что конроллер фактически добавляет контрольную сумму ПОСЛЕ того, как Wireshark захватывает пакет, следовательно, если вы видите множество ошибок контрольной суммы TCP, первое что необходимо сделать отключить эту опцию убедиться, что это не проблема.

Analyze TCP Sequence numbers (Анализ порядковых номеров TCP): этот флаг должен быть установлен Wireshark, чтобы предоставить анализ TCP, одной из основных и наиболее важных особенностей.

Relative Sequence Numbers (Относительные порядковые номера): когда TCP открывает соединение, оно начинается со случайного порядкового номера. Когда данный флаг установлен, Wireshark будет нормализовать его как "0", таким образом вы будете видеть не реальные номера, а номера начинающиеся с 0 и приращиваемые на 1. В большинстве случаев, относительные порядковые номера гораздо проще в обращение.

Calculate conversations timestamps (Вычисление временных меток переговоров): При установке данного флага, разбор TCP покажет вам время с начала соединения в каждом из пакетов. Это может оказаться

полезно в случаях очень быстрого подключения, когда время является критически важным.

Использование настройки Protocols из меню Preferences добавляет больше возможностей анализа в Wireshark. Однако, будьте осторожны, что бы не переборщить с возможностями, поскольку это может снизить скорость захвата пакетов и анализа.

2.2. Задание на выполнение:

1. Скачать и установить Wireshark и Pcap на ваш компьютер.
2. Ознакомиться с панелью инструментов Wireshark, просмотреть список разрешенных имен.
3. Синхронизировать время копьютера с временем в интернете.
4. Настроить правила колоризации.
5. Начать захват трафика с вашего компьютера.
6. Сохранить данные, полученные при захвате трафика в различных форматах.
7. Если в аудитории подключен сетевой принтер, распечатать одну страницу с полученными данными.

Отчет должен содержать:

- Титульный лист
- Алгоритм выполнения и скриншот выполнения каждого пункта из заданий.
- Вывод

2.3.Вопросы для защиты лабораторной работы:

1. Что такое Wireshark?
2. Возможности и недостатки Wireshark?
3. Что такое расположение Wireshark?
4. Что такое мониторинг сервера и брандмауэра?
5. Что вы знаете о мониторинге коммутатора?
6. Принцип работы коммутатора в локальной сети?
7. Как правильно установить Wireshark?
8. Может ли Wireshark захватывать трафик с нескольких интерфейсов одновременно? Если да, то как это сделать?
9. Что такое колоризация списка пакетов?
10. Как настроить правила колоризации пакетов?
11. Как сменить конфигурацию захвата пакетов?
12. Как в Wireshark можно сохранять данные?

3. РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

1. Пятибратов, Л. Гудыно, А. Кириченко Вычислительные системы, сети и телекоммуникации. М.:Кнорус, 2013
2. Олифер Н.А., Олифер В.Г. «Компьютерные сети. Принципы, технологии, протоколы. Учебник для вузов»- Ст-П.: Ст-П Пресс, 2010
3. Кузьменко Н.Г. Компьютерные сети и сетевые технологии. СПб.: Наука и Техника, 2013.-368с.
4. Щербо В.К. Стандарты вычислительных сетей. Взаимосвязи сетей. Справочник -М.:КУДИЦ-ОБРАЗ, 2000
5. Лабораторные работы по Cisco. // www. easy-network.ru

Содержание