Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение

высшего образования

Пермский национальный исследовательский политехнический университет

Электротехнический факультет

Кафедра информационных технологий и автоматизированных систем

**ОТЧЕТ**

о работе по предмету «Информатика в приложении к отрасли»

на тему «TCP dump»

Выполнил студент ИВТ-22-2б:

Мельников Глеб Владимирович

Проверил доцент кафедры ИТАС:

Масич Григорий Федорович

Пермь 2023

СОДЕРЖАНИЕ

[ВВЕДЕНИЕ 3](#_Toc156253863)

[1. Цель работы 4](#_Toc156253864)

[1.2. Задачи работы 5](#_Toc156253865)

[2. ТСP dump 6](#_Toc156253866)

[2.1. Теоретические сведения 6](#_Toc156253867)

[2.2 Пример части сформированной таблицы из «сырца» выбранного TCP-соединения 12](#_Toc156253868)

[2.3 Расчет количества байтов, которые могут быть переданы после момента времени, выделенного TCP-сегмента 13](#_Toc156253869)

[ЗАКЛЮЧЕНИЕ 15](#_Toc156253870)

[3. Список литературы 16](#_Toc156253871)

# ВВЕДЕНИЕ

TCP (Transmission Control Protocol) — это протокол управления передачей данных в сетях. Он является одним из основных протоколов в семействе протоколов TCP/IP. TCP обеспечивает надежную передачу данных между узлами в сети.

Отчет будет полезен для будущих специалистов, работающих в области сетевых технологий и желающих углубить свои знания о протоколе TCP.

# Цель работы

Уяснение предоставляемого протоколом TCP сервиса посредством анализа полей TCP-заголовка в TCP-dump:

- механизм установления и расторжения TCP-соединения;

- способ надежной передачи посредством подтверждений;

- механизм управления потоком посредством скользящего окна.

# 1.2. Задачи работы

- выделить одно TCP-соединение из выданного варианта TCP-dump;

- представить в табличном варианте TCP-соединение;

- разобрать и понять смысл значений полей в TCP-заголовке;

- показать сегмент, подтверждающий правильный прием выделенного TCP-сегмента;

- выполнить расчет количества байтов, которые могут быть переданы

после момента времени выделенного TCP-сегмента.

# 2. ТСP dump

# 2.1. Теоретические сведения

TCP (англ. Transmission Control Protocol — протокол управления передачей) — один из основных протоколов передачи данных интернета. Предназначен для управления передачей данных интернета. Пакеты в TCP называются сегментами.

В стеке протоколов TCP/IP выполняет функции транспортного уровня модели OSI.

Механизм TCP предоставляет поток данных с предварительной установкой соединения, осуществляет повторный запрос данных в случае потери данных и устраняет дублирование при получении двух копий одного пакета, гарантируя тем самым целостность передаваемых данных и уведомление отправителя о результатах передачи.

Реализации TCP обычно встроены в ядра ОС. Существуют реализации TCP, работающие в пространстве пользователя.

Когда осуществляется передача от компьютера к компьютеру через Интернет, TCP работает на верхнем уровне между двумя конечными системами, например, браузером и веб-сервером. TCP осуществляет надёжную передачу потока байтов от одного процесса к другому.

TCP протокольный блок данных (TCP PDU) называется “сегментом”

Сегмент:

* Инкапсулируется в IP-пакет
* Идентифицируется в IP номером 6 в поле “протокол”
* Максимальный размер сегмента (MSS) зависит от максимального размера пакета (L3) или кадра (L2) (фрагментация допускается)

Доставка последовательности сегментов осуществляется в виде байтового потока:

* Под байтовым потоком в TCP понимается то, что один примитив, например, read или write может вызвать посылку адресату последовательности сегментов, которые образуют некоторый блок данных (сообщение)

Прикладные процессы взаимодействуют с TCP модулем через TCP-порты

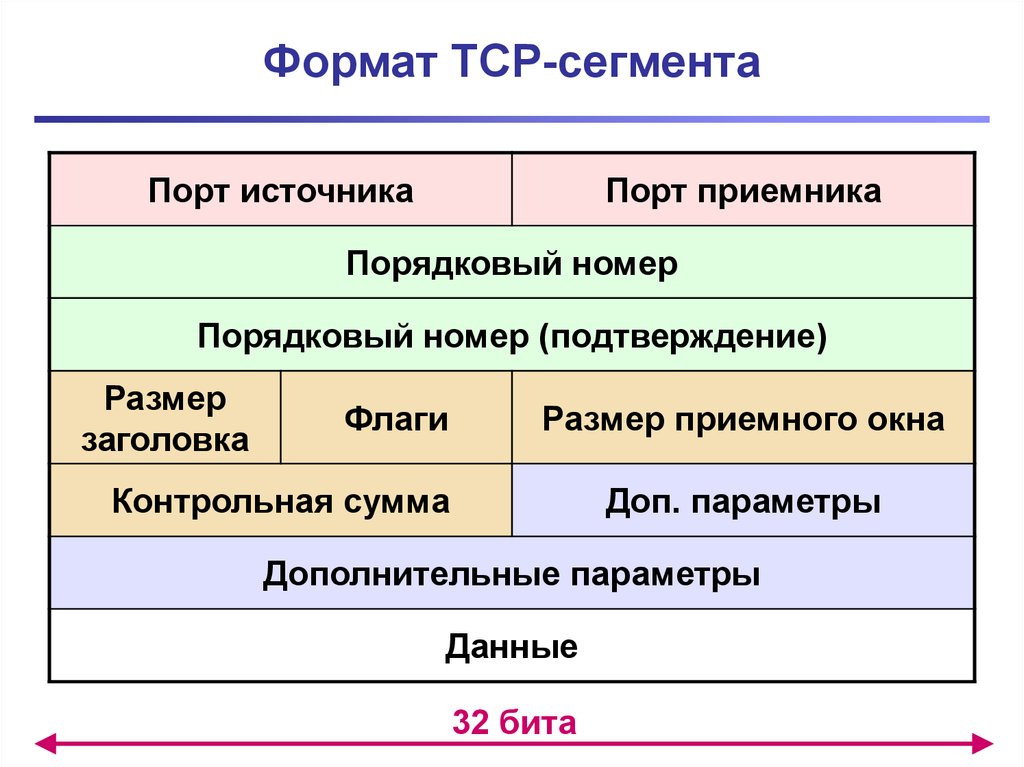


Рисунок 1 – Поля заголовка TCP сегмента

Поля TCP-заголовка:

* Sequence Number (SN) – последовательный номер сегмента
* Acknowledgement Number (AckN ) – подтверждаемый номер сегмента
* Windows Size – размер окна (в байтах, ACK=1)
* Urgent Pointer – указатель срочных данных

Поля TCP-заголовка (флаги):

* SYN - флаг синхронизации
* FIN – флаг окончания (примитив “disconnect request”)
* ACK - флаг подтверждения
* RST – флаг сброса соединения (прерывание соединения)
* URG - флаг важной информации
* PSH – флаг «выталкивание»
* Checksum – контрольная сумма

TCP dump — это утилита, которая позволяет записывать и анализировать сетевой трафик в реальном времени.

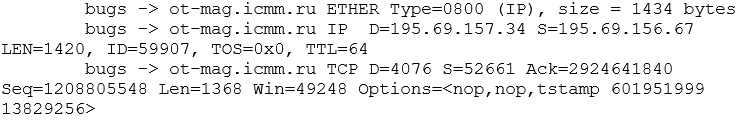
36

Рисунок 2 – пример «сырца» TCP dump

Пояснение:

**D=4076** – номер TCP порта получателя

**S=52661** – номер ТСР порта отправителя

**ACK=2924641840** - номер подтвержденного сегмента, полученного от отправителя

**Seq=1208805548** - номер отправляемого сегмента

**ETHER Type=0800** – тип используемого IP в данном случае IPv4

**D=195.69.157.34** – IP получателя

**S=195.69.156.67** – IP отправителя

**Win=49248** - представляет размер окна, которое используется для управления потоком данных TCP и уведомления другой стороны о доступном пространстве для приема

**Options=<nop,nop,tstamp 601951999 13829256> - это опции TCP-заголовка**

NOP (no operation) — это пустая операция, которая вставляется в опцию временной метки для выравнивания заголовка пакета. Наличие двух NOP означает, что используется опция временной метки с длинной в 8 байт.

tstamp – временная метка (значение содержит опции, которые могут быть использованы при передаче данных. Значения `601951999 **13829256**` представляют собой временную метку и идентификатор сессии)

Фазы работы TCP:

1. Фаза «Установление соединения»

* Выполнение «Трёхкратного рукопожатия»

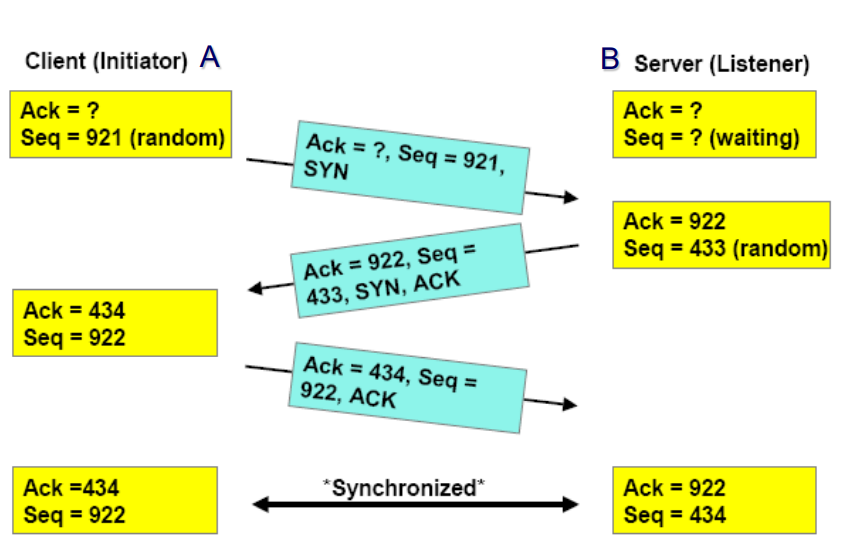


Рисунок 3 – пример принципа «Трёхкратного рукопожатия»

Пояснение:

Чтобы A и B могли общаться, им нужно произвести синхронизацию, для

этого нужно обменяться значениями полей Seq (первоначально случайное

число) и Len (в данном примере Len = 1), тогда для каждого станет известно

поле Ack, которое будет высчитываться как Seq + Len.

Таким образом:

A посылает сегмент B со значениями Seq = 921 (случайное число), Len = 1 и

флагом синхронизации Syn, после получения B отправляет подтверждение

в виде сегмента Ack = 921 + 1 = 922, Seq = 433 (случайное число) и флагом

синхронизации Syn. После чего происходит синхронизация и начинается

фаза «Передачи данных», где A может отправлять новый

сегмент со значениями Ack = 433 + 1 = 434, Seq = 921 + 1 = 922 и т. д.

1. Фаза «Передачи данных» продолжается обмен данными, отправитель передаёт сегменты, а получатель в ответ посылает подтверждение руководствуясь принципом «Скользящее окно».

«Скользящее окно» позволяет быстрее передавать порции данных, посредством подтверждения только последнего сегмента в «окне», таким образом получатель «говорит», что принял текущий сегмент и все предыдущее и теперь ожидает следующий.

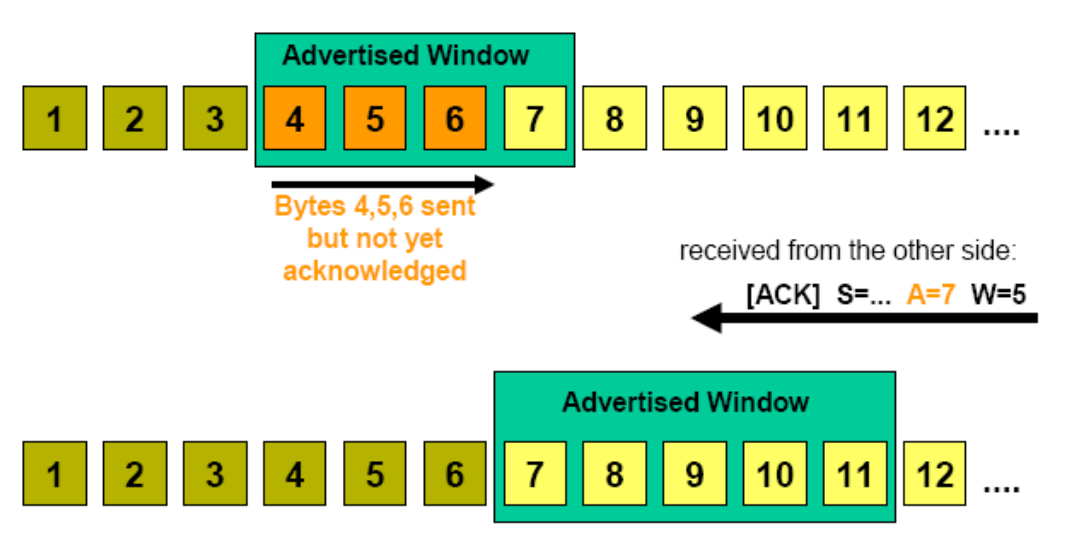


Рисунок 4 – пример «Скользящего окна»

Пояснение:

Изначально было «окно» размером 4, были переданы, но не подтверждены 4-6 сегменты. После чего буфер получателя освободился, и он отправил сообщение, что принял 6 сегмент и все предыдущие и ожидает следующий, то есть 7, так-как Ack = 7 = Seq + Len = 6 + 1, а также может принять новое количество байт Win = 5. После чего размер окна изменился и могут снова передаваться сегменты данных.

1. Фаза «Расторжение соединения»

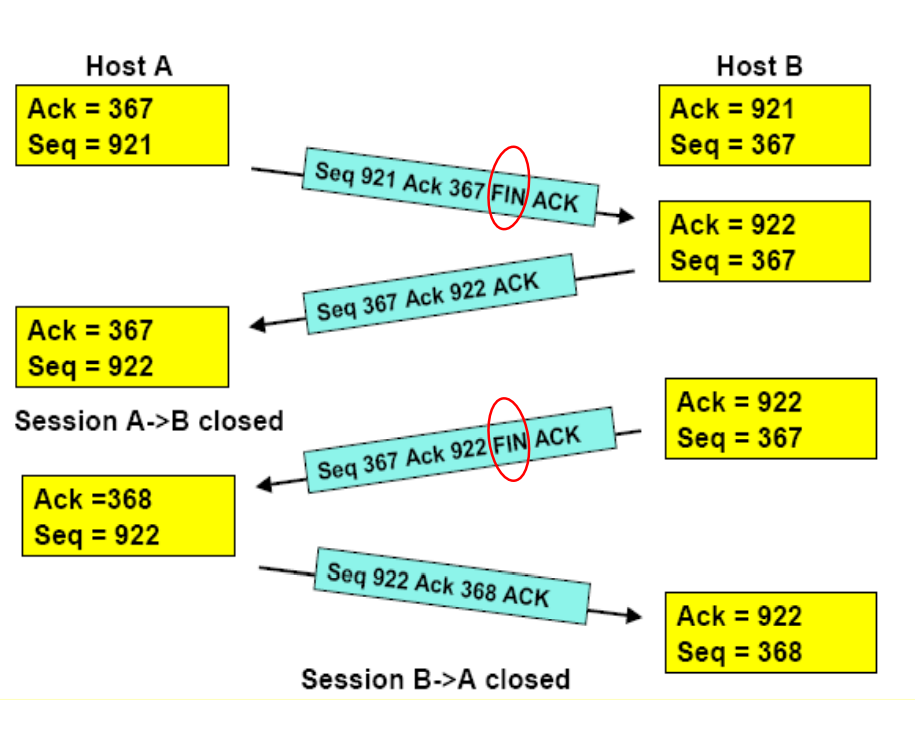


Рисунок 5 – Пример фазы «Расторжения соединения»

Пояснение:

A передаёт сегмент данных B с флагом FIN, который означает закрытие

сессии, в своём случае B отсылает подтверждение A и тоже отправляет

сегмент с флагом Fin, получая подтверждения сессия завещается в обе

стороны.

# 2.2 Пример части сформированной таблицы из «сырца» выбранного TCP-соединения



Таблица 1 - Пример части сформированной таблицы из «сырца» выбранного TCP-соединения

# 

# 2.3 Расчет количества байтов, которые могут быть переданы после момента времени, выделенного TCP-сегмента

1. Для начала нужно найти последний пакет, который отправил ot-mag.icmm.ru, затем ищем последний пакет bugs, который отправлен перед найденным пакетом ot-mag.icmm.ru

2. После чего можно узнать, сколько байт можно передать после подтверждения, по формуле

где флаги с индексами o – это флаги, принадлежащие пакету от ot-mag.icmm.ru, b – принадлежащие bugs

3. Если от bugs ещё отправлялись пакеты до выделенного момента времени, то из полученного значения следует вычесть суму их значений полей Len (ΣSeqbi)

4. Таким образом получаем формулу:

Таблица расчет количества байтов, которые могут быть переданы после выделенного момента времени





Рисунок 2 - Таблица расчет количества байтов, которые могут быть переданы после выделенного момента времени

# ЗАКЛЮЧЕНИЕ

В данном отчете был рассмотрен протокол TCP на примере TCP dump. Были изучены основы протокола TCP, включая его структуру, алгоритмы управления передачей данных и механизмы контроля целостности данных. Изучение протокола TCP и анализ сетевого трафика с помощью TCP dump позволяют специалистам в области сетевых технологий лучше понимать работу протокола TCP и эффективно решать проблемы, связанные с его работой.

# Список литературы

1. [Масич Григорий (masich.ru)](https://www.masich.ru/)
2. [Andrey Sozykin - YouTube](https://www.youtube.com/@AndreySozykin)

Вопросы:

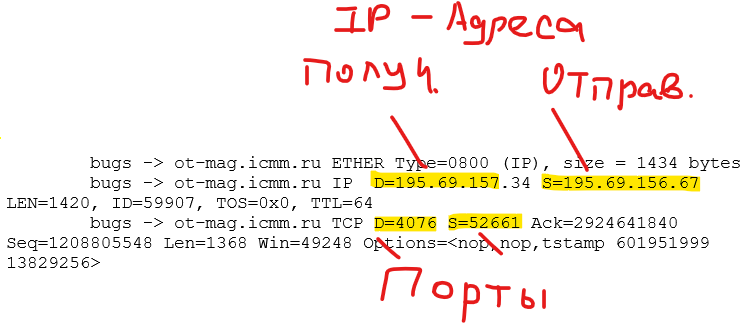
МГФ:

1. Как сформировали исходный сырец?

МГВ:

Требовалось выбрать сегменты из одного TCP-соединения.

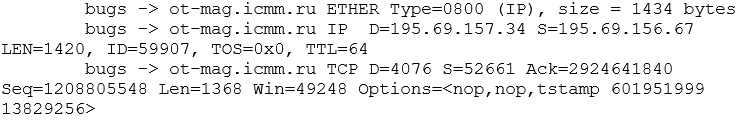
Для формирования TCP-соединения должны быть IP-адреса И TCP-порты получателя и отправителя, если значения полей разные, то это разные соединения



МГФ:

1. Пояснить за поля в сырце

МГВ:



1. ETHER Type=0800 (IP), size = 66 bytes:

• ETHER Type=0800: Это тип Ethernet-кадра, указывающий на использование протокола IP (0800 - идентификатор протокола IPv4).

• size = 1434 bytes: Это размер Ethernet-кадра, равный 1434 байтам.

• IP: Указывает на использование протокола IP.

• D=195.69.157.34 S=195.69.156.67: Поля указывают на IP-адреса, где D - адрес назначения, а S - адрес источника.

• LEN=1420: Это длина (включая заголовок и данные) IP-пакета, равная 1420 байтам.

• ID=59907: Это идентификационный номер IP-пакета.

• TOS=0x0: Это байт обслуживания типа службы (Type of Service), который обычно используется для различных служебных целей (в данном случае, он равен нулю).

• TTL=64: Это время жизни пакета (Time To Live), представляющее количество маршрутизаторов, через которые может пройти пакет, прежде чем быть отброшенным (в данном случае, 64 шагов).

3. TCP D=4076 S=52661 Ack=2924641840 Seq=1208805548 Len= 1368 Win=49248 Options=<nop,nop,tstamp 601951999 13829256>:

• TCP: Указывает на использование протокола TCP.

• D=4076 S=52661: Поля D и S представляют порты получателя и отправителя соответственно.

• Ack=2924641840 Seq=1208805548: Поля Ack и Seq представляют номера подтверждения и последовательности соответственно. Ack - номер подтверждения, Seq - номер последовательности.

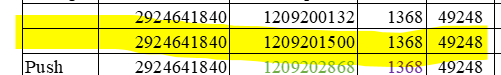
• Len=1368: Это длина полезных данных (в байтах) в TCP-сегменте. В данном случае, длина равна 0.

• Win=49248: Размер окна передачи TCP (TCP Window Size) указывает на количество байтов, которые отправитель может передать

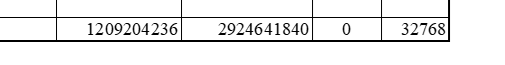
• Options=<nop,nop,tstamp 601951999 13829256>: Это опции TCP-заголовка. В данном случае, указаны опции nop (no operation) и tstamp (timestamp) с указанными временными метками.

МГФ:

1. Найти подтверждение для выделенного сегмента



МГВ:



(Верно)