Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский ядерный университет «МИФИ»

Институт интеллектуальных кибернетических систем

Кафедра №42 «Криптология и кибербезопасность»

Отчёт о БДЗ по теме

«Добавление модуля анализа промышленного протокола IEC104

в ПО Suricata»

по дисциплине «ИБ АСУ ТП»

Выполнили студенты группы Б17-505:

Зоричев В.В.

Рудик М.В.

Савченко А.М.

Худоярова А.М.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Москва – 2020

Оглавление

[**1** **Описание промышленного протокола IEC 104** 4](#_Toc54712817)

[**2** **Клиент – сервер для промышленного протокола IEC – 104** 8](#_Toc54712818)

1. **Описание промышленного протокола IEC 104**

Стандарт IEC 60870–5-104 (IEC 104): «Доступ к сети для IEC 60870-5-101 с использованием стандартных транспортных профилей» опубликован Международной электротехнической комиссией (IEC) в наборе стандартов IEC 60870-5.

IEC 60870–5 обеспечивает профиль связи для отправки базовых сообщений телеуправления (диспетчерское управление и сбор данных) между двумя системами через постоянно подключенные каналы передачи данных между этими системами. Стандарт IEC 104 определен для передачи сообщений телеуправления IEC 60870–5-101 (IEC 101) через TCP с использованием порта 2404. То есть IEC 104 инкапсулирует сообщения телеуправления IEC 101 в блок данных APDU (Application Protocol Data Unit), который передается как часть полезной нагрузки TCP (рис.1).

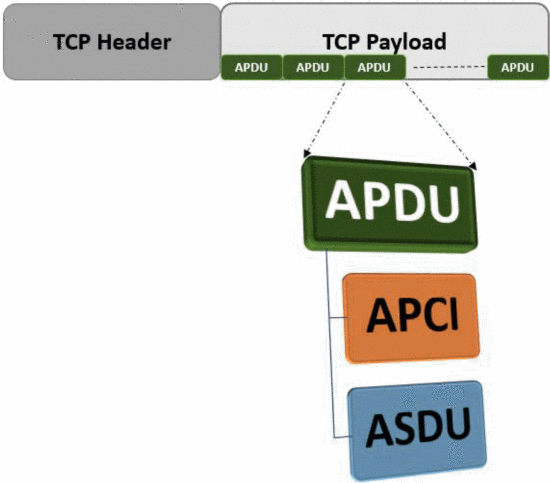


Рисунок 1 – APDU как полезная нагрузка TCP.

Поля APDU состоят из двух частей (рис. 2):

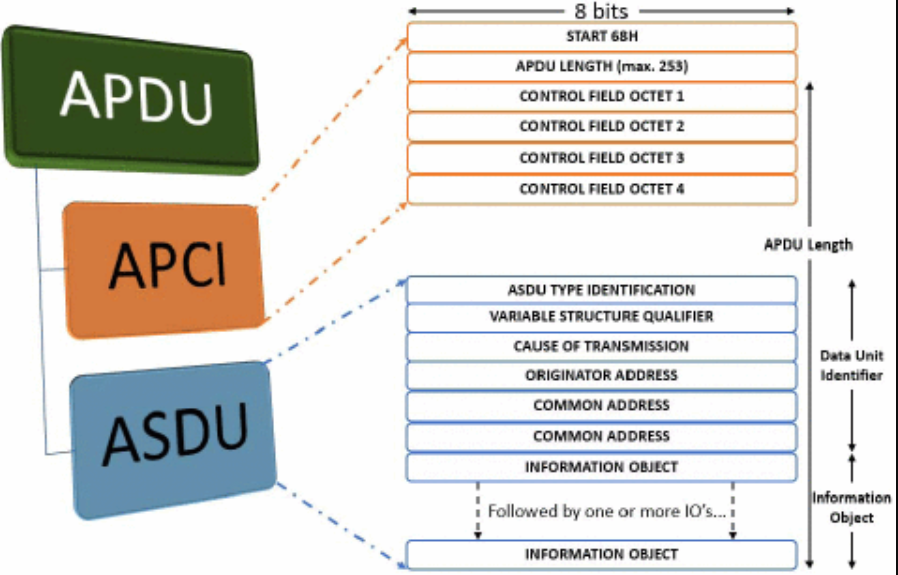


Рисунок 2 – Структура ADPU

1. APCI (Application Protocol Control Information) - информация управления, которая функционирует как заголовок;
2. ASDU (Application Protocol Data Unit) - блок данных, который содержит данные прикладного уровня IEC 101 то есть сообщения телеуправления.

APCI - это 6-октетный заголовок, который включает в себя начальный октет (68H), за которым следуют 1-октетное поле, определяющее длину APDU (4 октета полей управления и длина ASDU) и 4-октетные поля управления. Два младших бита первого октета поля управления определяют тип сообщения телеуправления, которое может иметь формат:

1. I (00b) – передает информацию датчиков и управления, и за APCI всегда следует ASDU;
2. S-формат (01b) – используется для отправки подтверждений порядкового номера;
3. U-формат (11b) – используется для отправки сообщений поддержания активности соединения.

ASDU – это структура данных переменной длины, которая состоит из идентификатора блока данных фиксированной длины DUI (Data Unit Identifier) и информационного объекта переменной длины IO (Information Object). ASDU состоит из следующих полей (рис. 3):

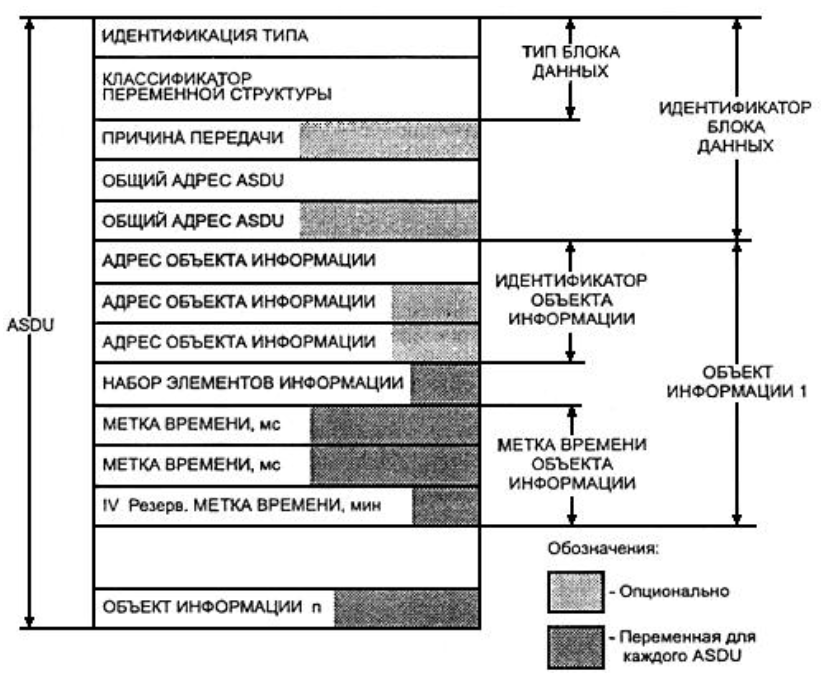


Рисунок 3 – Структура ASDU

1. Идентификатор типа ASDU – определяет структуру, тип и формат следующего(их) за ним объекта(ов) информации (IO). IO с временной меткой или без нее отличаются различными значениями идентификатора типа. При приеме ASDU со значениями идентификатора типа, не входящими в заранее определенный перечень, посылается отрицательная квитанция;
2. Классификатор переменной структуры;
3. Причина передачи (рис. 4) – направляет ASDU определенной прикладной задаче для обработки. Бит P/N показывает, какое (положительное или отрицательное) подтверждение активации требуется для первичной прикладной функции. В случае, когда бит P/N не используется, он равен нулю;

Рисунок 4 – Поле причины передачи ASDU

1. Общий адрес ASDU – связан со всеми объектами в данном ASDU. Глобальный адрес (65535) – это широковещательный адрес, обращенный ко всем станциям данной системы. В ответ на переданные в направлении управления ASDU с широковещательным адресом, в направлении контроля должны передаваться ASDU, содержащие специально определенный общий адрес;
2. Адрес объектов информации – используется как адрес получателя в направлении управления и как адрес источника в направлении контроля;
3. Элементы информации;
4. Метка времени.

IEC 104 также определяет следующие таймеры:

* T0 – тайм-аут этого времени вызовет запрос SYN;
* T1 – тайм-аут этого таймера вызовет активный запрос закрытия для установленного соединения. Кроме того, событие тайм-аута T1 на управляющей станции может автоматически инициировать новое резервное соединение и автоматическое переключение соединения;
* T2 – истечение этого таймера заставит приемник отправить S-формат с принятым порядковым номером (сообщение ACK), который является подтверждением на уровне приложения для получения определенного количества APDU;
* T3 – истечение этого таймера указывает, что не было получено сообщений IEC 104 с другой стороны для данного открытого TCP-соединения. Прием любого типа сообщения, I-формата, S-формата или U-формата сбрасывает этот таймер.

1. **Клиент – сервер для промышленного протокола IEC – 104**

За основу был взят симулятор IEC-104 трафика <https://github.com/RocyLuo/IEC104TCP>. Однако он не является полностью рабочим, поскольку написан для Python2, а также содержит ошибку в коде.

Поэтому данная реализация была модифицирована:

* интерпретирована под Python3,
* устранена ошибка (в библиотеке scapy, файл fields.py на локальном компьютере необходимо заменить 167-ю строку на return copy.copy(x), ошибка именно в стандартной библиотеке)
* выполнено корректное завершние соединения между клиентом и сервером
* исправлены названия файлов, чтобы они соответствовали своей реальной функциональности (то есть сервер в изначальном симуляторе на самом деле должен быть клиентом, а клиент сервером).

**Запуск.**

Перед запуском проверьте наличие библиотеки scapy. (Для ее установки: python3 -m pip install scapy). И запустите пример.

python3 EchoIEC104Client.py

python3 example.py

Данные для теста описаны в iec104\_tcp\_packets.py и представляют собой APDU (APCI и ASDU).

**Формирование трафика.**

После запуска example.py формируется передача данных по IEC-104.

**Содержание дампа.**

При запуске формируются блоки данных на прикладном уровне (ASDU) с идентификаторами типа 45,46,47,48,58,59,60,61,62,50,101,103, и управляющая информация прикладного уровня (APCI: с форматами поля управления "s", "i","u"):

* 45(C\_SC\_NA\_1) - однопозиционная команда
* 46(C\_DC\_NA\_1) - двухпозиционная команда
* 47(C\_RC\_NA\_1) - команда пошагового регулирования
* 48(C\_SE\_NA\_1) - команда уставки, нормализованное значение
* 50(C\_SE\_NC\_1) - команда уставки, короткий формат плавающей запятой
* 58(C\_SC\_TA\_1) - однопозиционная команда с меткой времени СР56Время2а
* 59(C\_DC\_TA\_1) - двухпозиционная команда с меткой времени СР56Время2а
* 60(C\_RC\_TA\_1) – команда пошагового регулирования с меткой времени СР56Время2а
* 61(C\_SE\_TA\_1) – команда уставки, нормализованное значение с меткой времени СР56Время2а
* 62(C\_SE\_TB\_1) – команда уставки, масштабированное значение с меткой времени СР56Время2а
* 101(C\_CI\_NA\_1) - команда опроса счетчиков
* 103(C\_CS\_NA\_1) - команда синхронизации часов

Результирующий дамп находится в result.pcanpg. На рисунке 1 представлен общий сформированный дамп, на рисунке 2 представлен пакет, с типом ASDU №45, то есть это однопозиционная обычная команда, что так же видно на скриншоте в расшифровке команды.

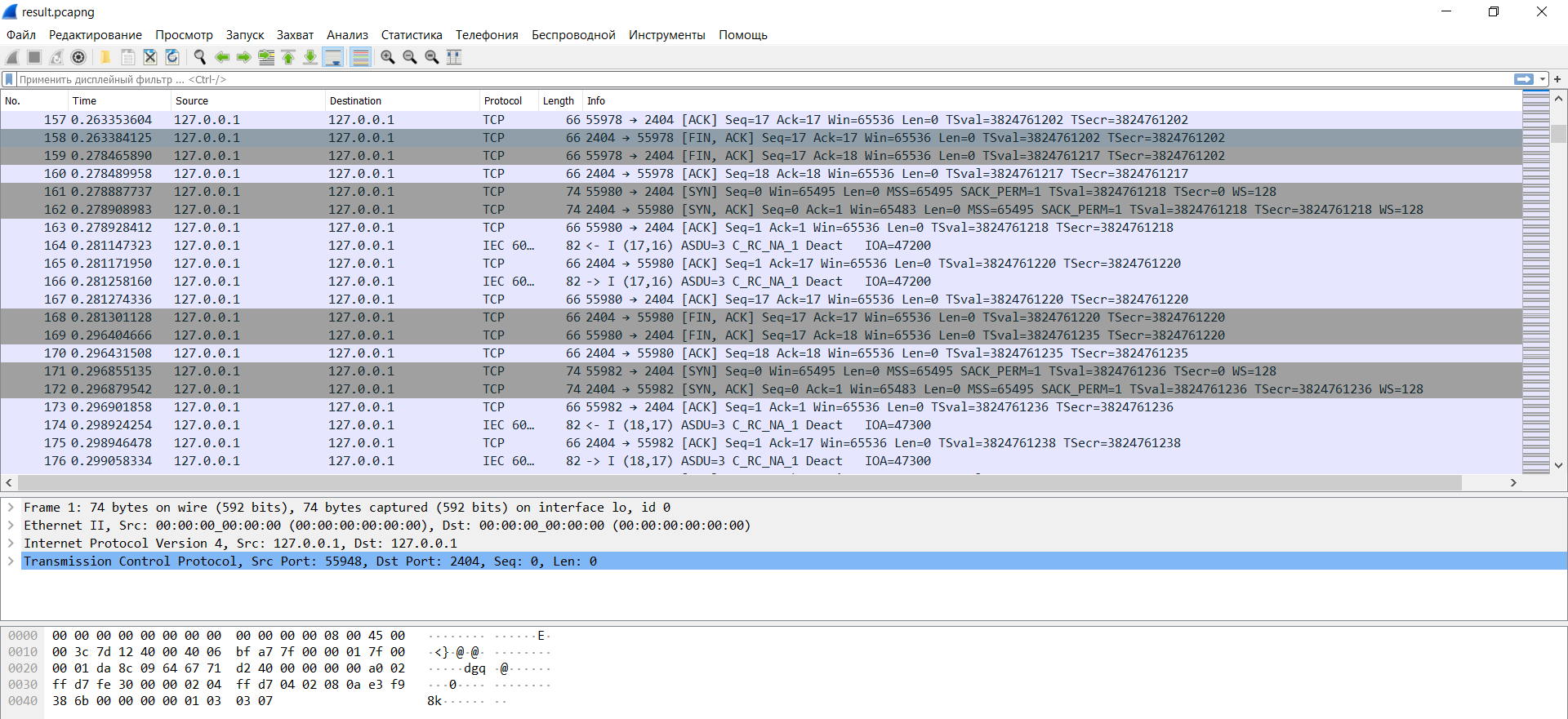


Рисунок 1 — общий сформированный дамп трафика при передаче данных по IEC-104.

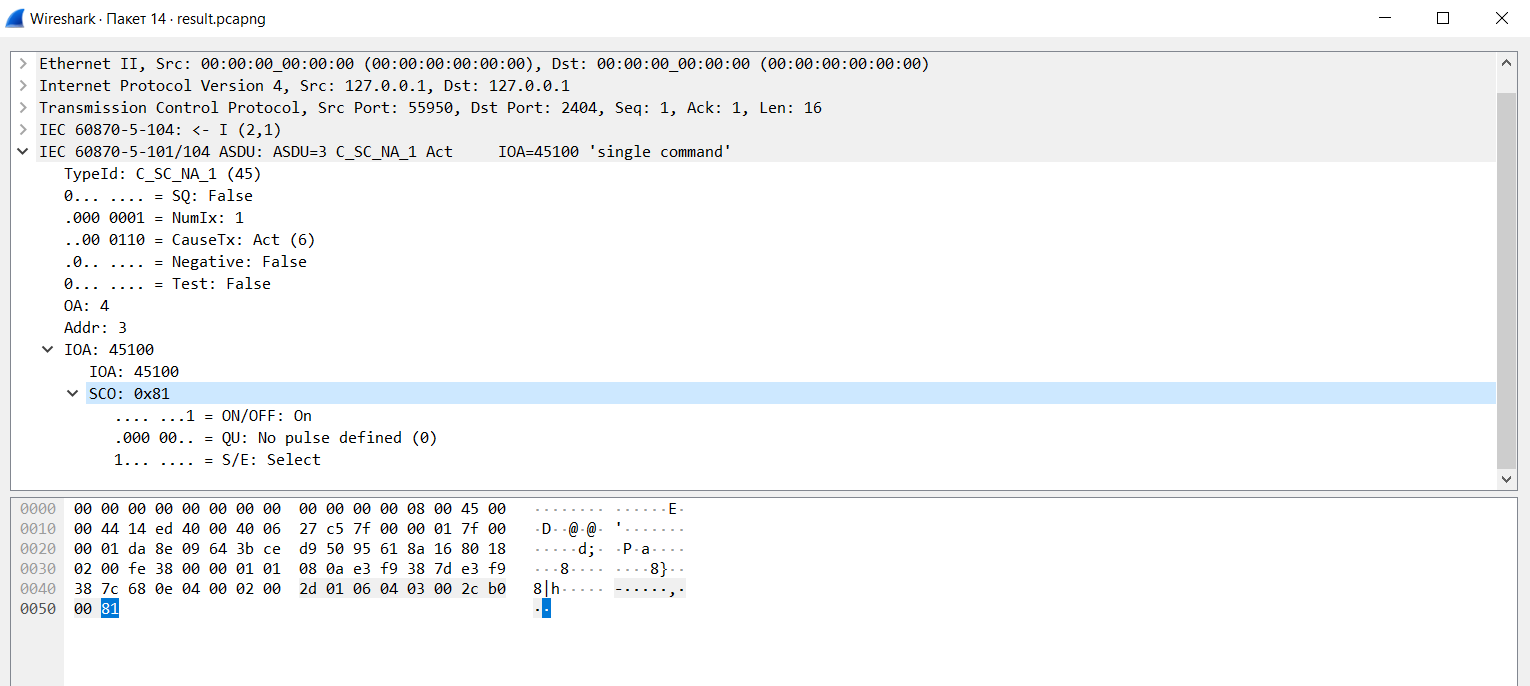


Рисунок 2 — блок данных ASDU с типом №45.