Информационная безопасность АСУ ТП

Лабораторная работа №2. Анализ дампа трафика протокола Modbus.

1. Теория

Целью данной лабораторной работы является изучение протокола Modbus.

Протокол Modbus разработан в 1979 году для соединения первых моделей ПЛК с компьютерами реального времени, и до сих пор является наиболее широко используемым промышленным протоколом в архитектурах АСУ ТП за счет простоты использования. Он обеспечивает эффективный обмен данными между связанными устройствами на основе метода «запрос-ответ». В протоколе Modbus используется три отдельных блока данных (PDU): запрос, ответ и ответ с исключениями.

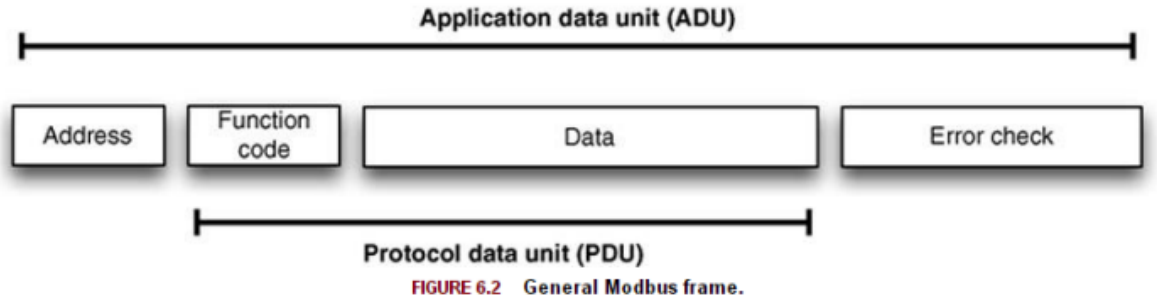

FIGURE 6.2 General Modbus frame.

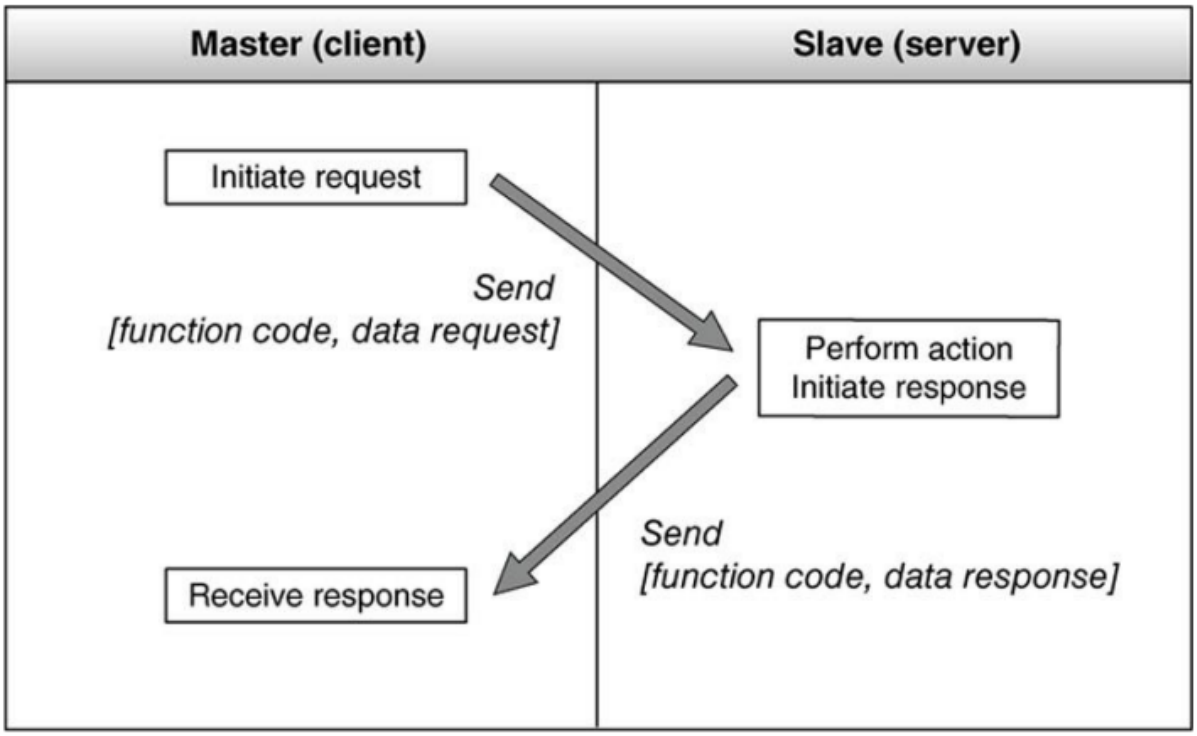

Рисунок 1. — Структура пакета протокола Modbus

При этом, коды функций и запросы данных можно использовать для выполнения широкого диапазона команд, к примеру:

– Чтение значения из одного регистра.
– Запись значения в один регистр.
– Чтение блока значений из группы регистров.
– Запись блока значений в группу регистров.
– Чтение файлов.
– Запись файлов.
– Получение данных диагностики устройства.

Function type			Function name	Function code
Data Access	Bit access	Physical Discrete Inputs	**Read Discrete Inputs**	2
		Internal Bits or Physical Coils	**Read Coils**	1
			Write Single Coil	5
			Write Multiple Coils	15
	16-bit access	Physical Input Registers	**Read Input Registers**	4
		Internal Registers or Physical Output Registers	**Read Holding Registers**	3
			Write Single Register	6
			Write Multiple Registers	16
			Read/Write Multiple Registers	23
			Mask Write Register	22
			Read FIFO Queue	24
	File Record Access		Read File Record	20
			Write File Record	21
Diagnostics			Read Exception Status	7
			Diagnostic	8
			Get Com Event Counter	11
			Get Com Event Log	12
			Report Slave ID	17
			Read Device Identification	43
Other			Encapsulated Interface Transport	43

Рисунок 2. — Типы кодов функций протокола Modbus

2. Задание

1. Используя дамп трафика, определить, какие из устройств являются slave, а какое – master.

2. В дампе трафика присутствует только одна пара запрос-ответ на запись регистров, в то время как остальные – только на чтение. Найти данную пару.

3. Используя карту топологии сети, определить, происходило ли вторжение в сеть на момент записи трафика.

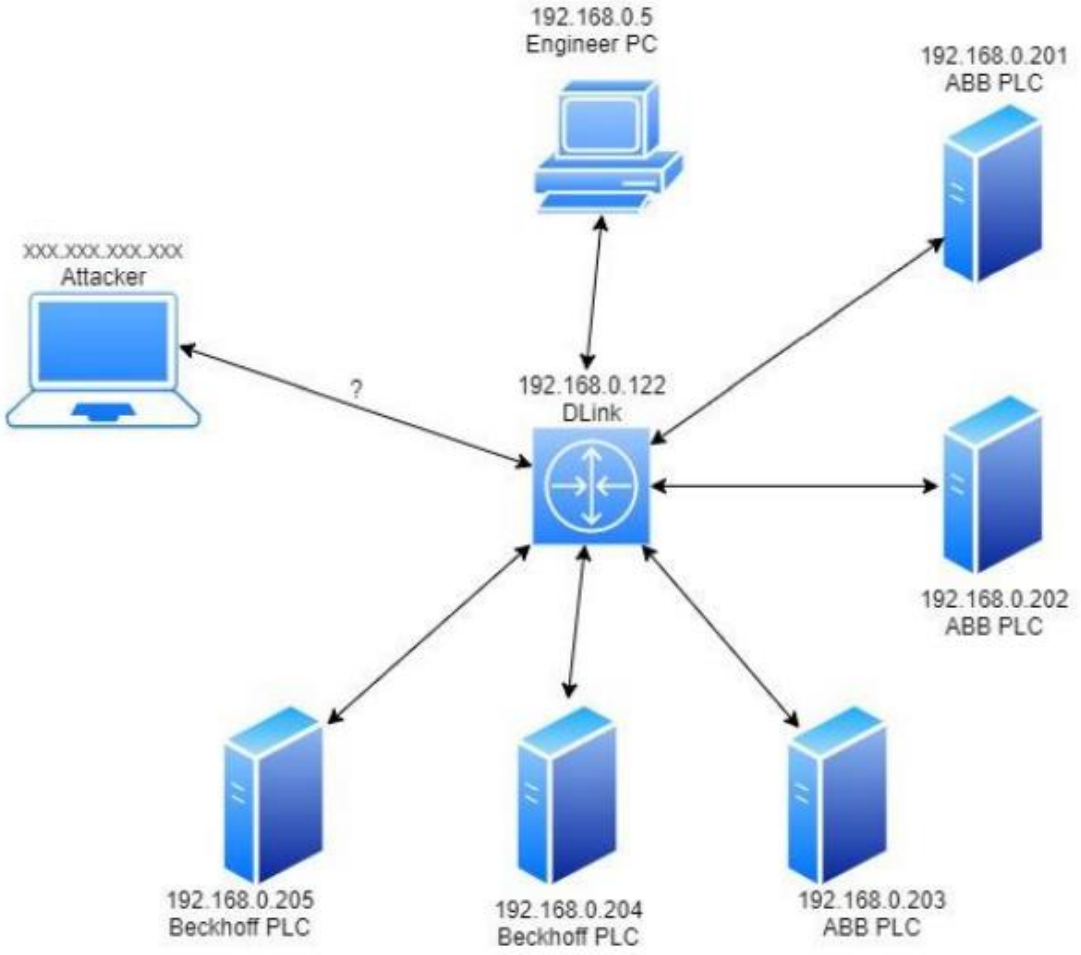

Рисунок 3. — Карта топологии сети

Для защиты лабораторной работы необходимо предоставить отчет, содержащий в себе описание хода выполнения и результатов всех указанных в задании пунктов.