Home Challenge #1
2020/21

Prof. Cesana Matteo

Shalby Hazem Hesham Yousef (Personal Code: 10596243)

6 April 2021

POLITECNICO
MILANO 1863

1 Questions

1.1 What's the difference between the message with MID: 3978 and the one with MID: 22636?

The main difference between the two messages is that one is reliable (**MID: 3978**) and one is unreliable (**MID: 22636**). The reliability of the first message is ensured by CONFIRMABLE (**CON**) Message (no. 6701) which must be acknowledged through **ACK** Message (no. 6702). The second message is unreliable in fact the exchange is done via a NON-CONFIRMABLE (**NON**) message (no. 6943). The filter used to get all the information is:

```
coap.mid == 3978 || coap.mid == 22636
```

1.2 Does the client receive the response of message No. 6949?

YES. Using `frame.number == 6949` filter we get a CONFIRMABLE message with `MID: 28357` so we should have an ACK message with the same ID as response.
Using the `coap.mid == 28357 && coap.type == 2` filter we get a message as result so the client received the response (`No. 6953`).

1.3 How many replies of type confirmable and result code "Content" are received by the server "localhost"?

There are **8** messages that respect the request. The result is obtained by using the following filter:

```
ip.src == 127.0.0.1 && coap.type == 2 && coap.code == 69
```

1.4 How many messages containing the topic "factory/department*/+" are published by a client with user name: "Jane"? [1]

Zero. Using `mqtt.username == "jane"` filter I got 4 CONNECT messages related to four TCP stream with the following index:

- `112`
- `121`
- `230`
- `354`

Using the previous information and the filter:

```
(tcp.stream == 112 || tcp.stream == 121 || tcp.stream == 230 || tcp.stream == 354
       ) && mqtt.msgtype == 3 && mqtt.topic contains "factory/department"
```

I got no message that respect the request.

[1] * replaces the dep. number, e.g. factory/department1/+, factory/department2/+ and so on.

1.5 How many clients connected to the broker "hivemq" have specified a will message?

10. Using `dns.resp.name contains "hivemq"` filter we got 2 addresses as response:

- `18.185.199.22`;
- `3.120.68.56`.

And using `(ip.addr == 18.185.199.22 || ip.addr == 3.120.68.56) && mqtt.willmsg` we got 10 messages as result.

1.6 How many publishes with QoS 1 don't receive the ACK?

50. Using `mqtt.msgtype == 3 && mqtt.qos == 1` filter we got `124` messages published with `QoS 1`. The reception of messages with `QoS 1` is confirmed by `PUBACK` message, but using `mqtt.msgtype == 4` we got only `74` messages, so there are `124-74= 50` messages that didn't receive any ACK.

1.7 How many last will messages with QoS set to 0 are actually delivered?

ONE. Using `mqtt.msgtype==1 && mqtt.conflag.qos ==0 && mqtt.willmsg` I got 14 connect messages that set the Will Message and only one is actually delivered.

1.8 Are all the messages with QoS > 0 published by the client 4m3DWYzWr40pce6OaBQAfk correctly delivered to the subscribers?

ONE. Using `mqtt.clientid == 4m3DWYzWr40pce6OaBQAfk` filter I got one massage (`no.964`) and this indicates only one connection by the client analyzed. Following the TCP connection and filtering using the filter:

```
tcp.stream eq 67 && mqtt.qos>0 && mqtt.msgtype==3
```

I got 2 messages: `No.1008` and `No.2423`.
The first has `QoS == 1` so it's correctly delivered if and only if a `PUBACK` is received, but using the filter:

```
tcp.stream eq 67 && mqtt.msgtype == 4
```

I got nothing.
The second has `QoS == 2` so it's correctly received if and only if a `PUBREC` is received, and this happens, in fact using the filter:

```
tcp.stream eq 67 && mqtt.msgtype == 5
```

I got one message (No.2425)

1.9 What is the average message length of a connect msg using mqttv5 protocol? Why messages have different size?

The average length is 91 or 32. The message have different length because the length of the options are different (username, password, etc...). For filtering the CONNECT messages that relay on MQTTv5, we use the following filter:

```
mqtt.ver == 5 && mqtt.msgtype == 1
```

I proposed two answers because the question is unclear because it doesn't specify if the average length needed is the one of the entire frame (`91`) or only of the MQTT(`32`).

1.10 Why there aren't any REQ/RESP pings in the pcap?

The request/response mechanism is used to prevent clients with very low messages rates from being disconnected. In the pcap considered there aren't any REQ/RESP because the keepalive timer never expires.

2 Filters Reference

- `coap.type == 2` → COAP message related to an ACK
- `coap.code == 69` → COAP message with result code equals to "Content"
- `mqtt.msgtype == 1` → MQTT connect message
- `mqtt.msgtype == 3` → MQTT publish message
- `mqtt.msgtype == 4` → MQTT publish acknowledge (PUBACK) message
- `mqtt.msgtype == 5` → MQTT publish receive (PUBREC) message