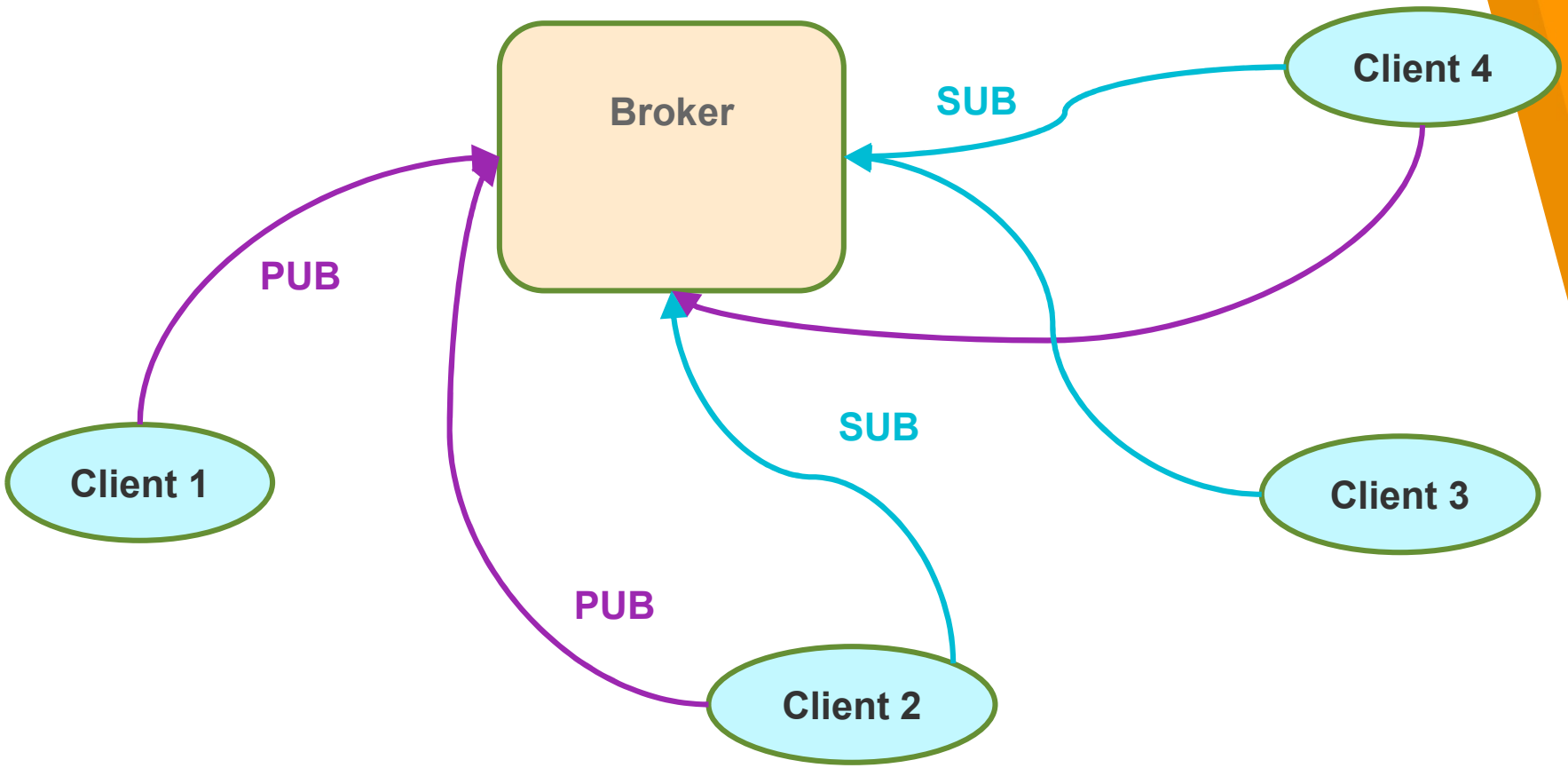
La sécurité du protocole MQTT

CIEL 1

MQTT : modèle client/broker



MQTT : QoS

- QoS 0 message envoyé 1 fois sans confirmation
  - Quand on accepte la perte de messages
- QoS 1 : au moins 1 livraison
  - Le broker envoie le message
  - Puis renvoie si pas d'ACK
  - Le client peut recevoir le message en double
- QoS 2 : exactement une livraison
  - Le broker envoie le message
  - S'assure de la réception en un exemplaire

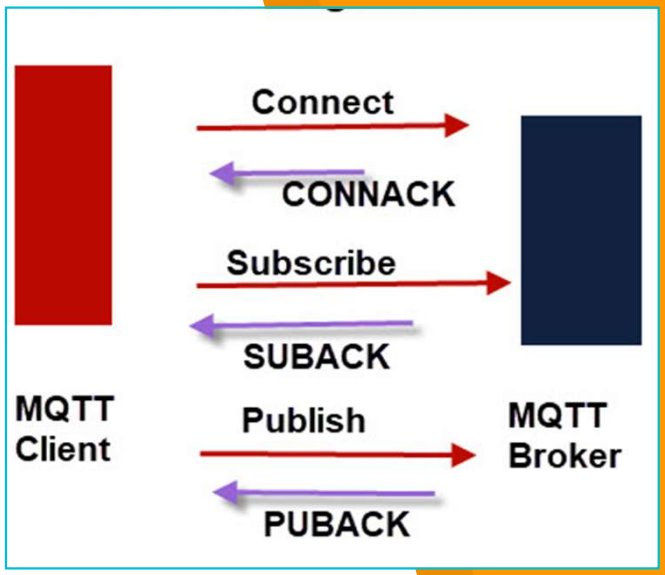
Sécurité : la triade CIA

- **Confidentiality** : la donnée n'est accessible qu'aux personnes autorisées.
- **Integrity** : les données ne doivent pas être altérées de façon fortuite, illicite ou malveillante.
- **Availability (Disponibilité)** : la donnée doit être disponible au moment voulu

MQTT : Connexion

Un client **doit** être connecté au broker

- Pour subscribe
- Pour publish
- Le client publie un message keep-alive
  - À intervalles réguliers
  - Dit au broker qu'il est connecté



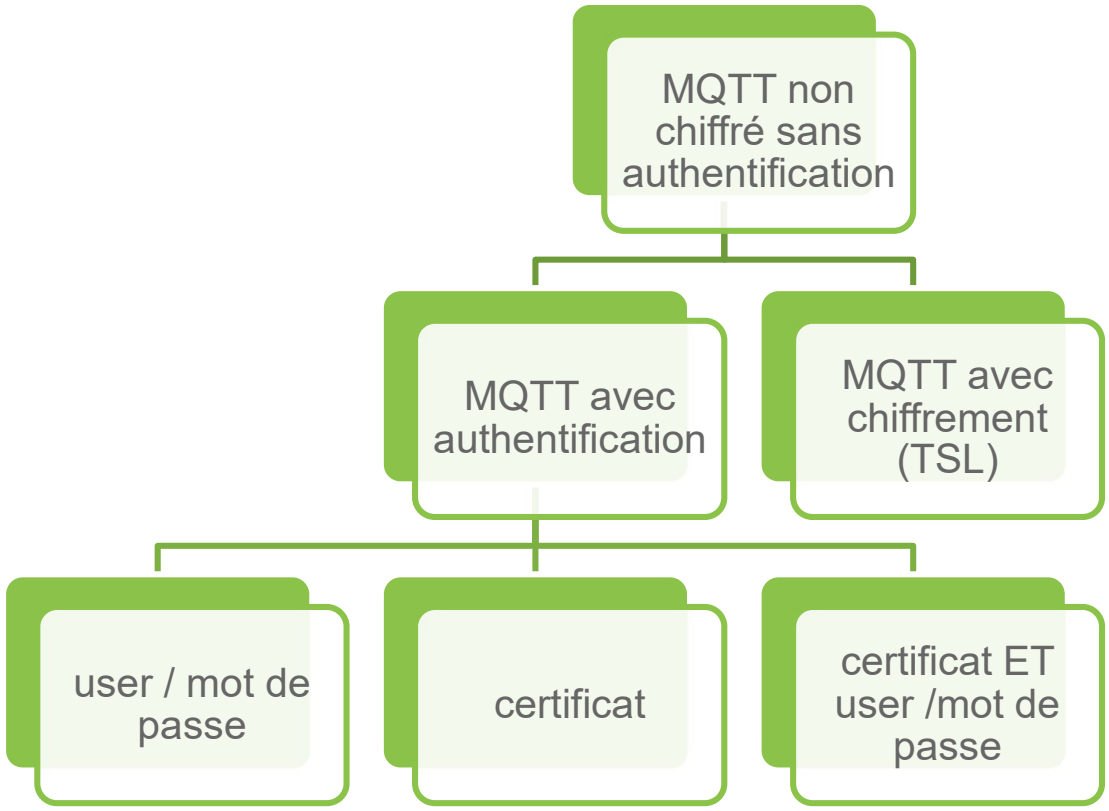
MQTT : Types de messages (1)

- CONNECT — La demande du client de se connecter au courtier
- CONNACK — Acquittement de la connexion
- SUBSCRIBE — Paquet du client pour s'abonner aux sujets
- SUBACK — Accusé de réception du paquet d'abonnement
- UNSUBSCRIBE — Paquet du client pour se désinscrire des sujets

MQTT : Types de messages (2)

- PUBLIER — Publie un message dans un sujet
- PUBACK — Accusé de réception de la publication avec QoS niveau 1
- PUBREC — Accusé de réception de la publication avec QoS niveau 2 (2ème paquet)
- PUBREL — Réponse au PUBREC. (3ème paquet lors de l'utilisation de QoS niveau 2)
- PUBCOMP — Réponse à PUBREL (4ème et dernier paquet lors de l'utilisation de QoS lvl 2)

MQTT : niveaux de sécurité



MQTT : sans authentification / sans chiffrement

- `$ mosquitto_pub -h hostname -t test -m  " hello"`

- Avantages
  - Facile et rapide à mettre en œuvre
  - à réserver aux architectures de développement
- Inconvénients
  - Aucune sécurisation

MQTT : avec authentification + SSL

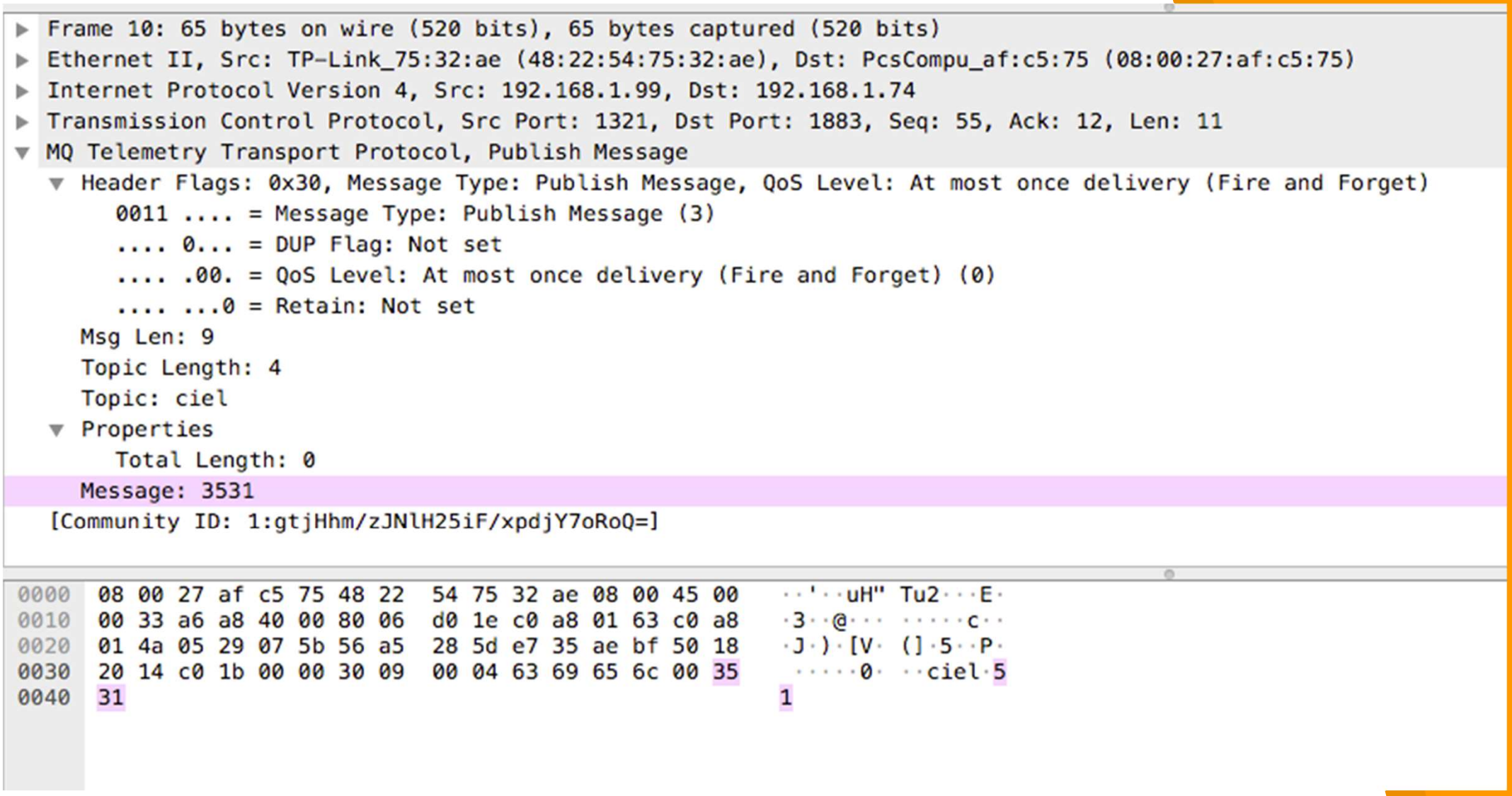
- `$ mosquitto_pub -h hostname -p 8883 --capath /etc/ssl/certs/ -u ciel -P motDePasse -t test -m " hello"`

- Avantages
  - Communication sécurisé (authentification + chiffrement)
- Inconvénients
  - Plus complexe à mettre en oeuvre

No.	Time	Source	Destination	Protocol	Length	Info
4	0.002860	192.168.1.99	192.168.1.74	MQTT	108	Connect Command
6	0.003062	192.168.1.74	192.168.1.99	MQTT	65	Connect Ack
10	8.416012	192.168.1.99	192.168.1.74	MQTT	65	Publish Message [ciel]

```
▶ Frame 4: 108 bytes on wire (864 bits), 108 bytes captured (864 bits)
▶ Ethernet II, Src: TP-Link_75:32:ae (48:22:54:75:32:ae), Dst: PcsCompu_af:c5:75 (08:00:27:af:c5:75)
▶ Internet Protocol Version 4, Src: 192.168.1.99, Dst: 192.168.1.74
▶ Transmission Control Protocol, Src Port: 1321, Dst Port: 1883, Seq: 1, Ack: 1, Len: 54
▼ MQ Telemetry Transport Protocol, Connect Command
  ▶ Header Flags: 0x10, Message Type: Connect Command
    Msg Len: 52
    Protocol Name Length: 4
    Protocol Name: MQTT
    Version: MQTT v5.0 (5)
  ▶ Connect Flags: 0xc2, User Name Flag, Password Flag, QoS Level: At most once delivery (Fire and Forget), Clean Session Flag
    Keep Alive: 60
  ▶ Properties
    Client ID Length: 15
    Client ID: mqttx_badclient
    User Name Length: 7
    User Name: mystere
    Password Length: 8
    Password: GreatJ0b
  [Community ID: 1:gtjHhm/zJNlH25iF/xpdjY7oRoQ=]
```

```
0000  08 00 27 af c5 75 48 22  54 75 32 ae 08 00 45 00   ··'··uH" Tu2···E·
0010  00 5e a6 a6 40 00 80 06  cf f5 c0 a8 01 63 c0 a8   ·^··@··· ·····c··
0020  01 4a 05 29 07 5b 56 a5  28 27 e7 35 ae b4 50 18   ·J·)·[V· ('·5··P·
0030  20 14 0d 38 00 00 10 34  00 04 4d 51 54 54 05 c2    ··8···4 ··MQTT··
0040  00 3c 05 11 00 00 00 00  00 0f 6d 71 74 74 78 5f   ·<····· ··mqttx_
0050  62 61 64 63 6c 69 65 6e  74 00 07 6d 79 73 74 65   badclien t··myste
0060  72 65 00 08 47 72 65 61  74 4a 30 62               re··Grea tJ0b
```


Frame 10: 65 bytes on wire (520 bits), 65 bytes captured (520 bits)
Ethernet II, Src: TP-Link_75:32:ae (48:22:54:75:32:ae), Dst: PcsCompu_af:c5:75 (08:00:27:af:c5:75)
Internet Protocol Version 4, Src: 192.168.1.99, Dst: 192.168.1.74
Transmission Control Protocol, Src Port: 1321, Dst Port: 1883, Seq: 55, Ack: 12, Len: 11
MQ Telemetry Transport Protocol, Publish Message
Header Flags: 0x30, Message Type: Publish Message, QoS Level: At most once delivery (Fire and Forget)
0011 .... = Message Type: Publish Message (3)
.... 0... = DUP Flag: Not set
.... .00. = QoS Level: At most once delivery (Fire and Forget) (0)
....0 = Retain: Not set
Msg Len: 9
Topic Length: 4
Topic: ciel
Properties
Total Length: 0
Message: 3531
[Community ID: 1:gtjHhm/zJNlH25iF/xpdjY7oRoQ=]
0000 08 00 27 af c5 75 48 22 54 75 32 ae 08 00 45 00
0010 00 33 a6 a8 40 00 80 06 d0 1e c0 a8 01 63 c0 a8
0020 01 4a 05 29 07 5b 56 a5 28 5d e7 35 ae bf 50 18
0030 20 14 c0 1b 00 00 30 09 00 04 63 69 65 6c 00 35
0040 31
1