eman ta zabal zazu

Universidad del País Vasco
Euskal Herriko Unibertsitatea

VITORIA-GASTEIZKO INGENIARITZA ESKOLA
ESCUELA DE INGENIERÍA DE VITORIA-GASTEIZ

GRADO EN INGENIERÍA ELECTRÓNICA INDUSTRIAL Y AUTOMÁTICA

TRABAJO DE FIN DE GRADO

DESARROLLO DE UN CLIENTE MQTT PARA COMUNICACIONES SEGURAS EN SISTEMAS EMBEBIDOS

Alumno: Jorge Botana Mtz. de Ibarreta

Director: José Miguel Gil-García Leiva

Curso: 2021 - 2022

Contenido

Contexto

MQTT es un protocolo de mensajería con las siguientes ventajas:

- Es ligero y sencillo, pero completo.
- Se considera apto para redes de baja calidad.
- Consume poca energía.

Es ideal para el IoT, donde se usan muchos sistemas embebidos.

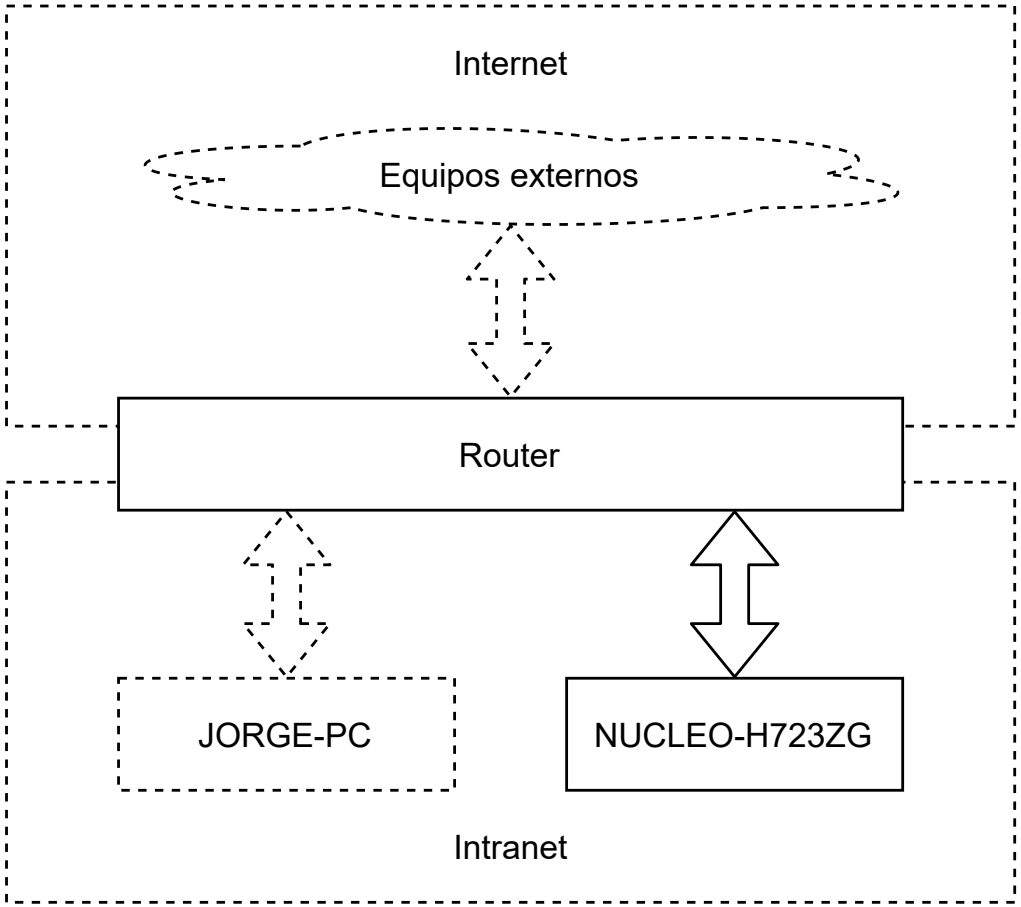
Objetivos

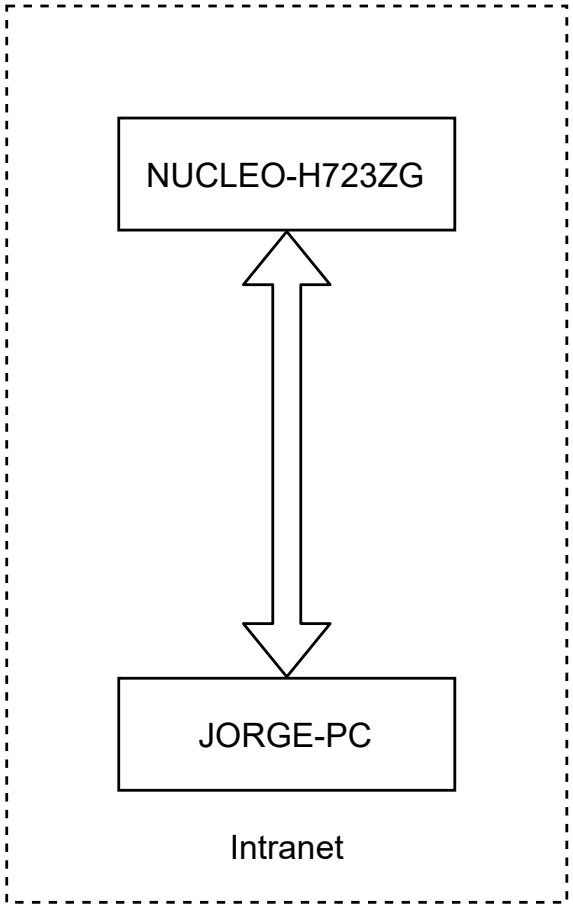
- Desarrollar un cliente MQTT.
- Añadir TLS con autenticación del servidor y del cliente.
- Crear una aplicación para un sistema embebido.
- Comparar tiempos de RD/WR de paquetes con/sin TLS.

Tareas

- Crear redes de comunicaciones con varios dispositivos.
- Desarrollar clientes para diversos protocolos.
- Configurar servidores en red local.
- Capturar y analizar el tráfico de red.
- Construir infraestructuras de certificados.
- Programar, configurar, ejecutar y depurar la aplicación.

Redes de dispositivos

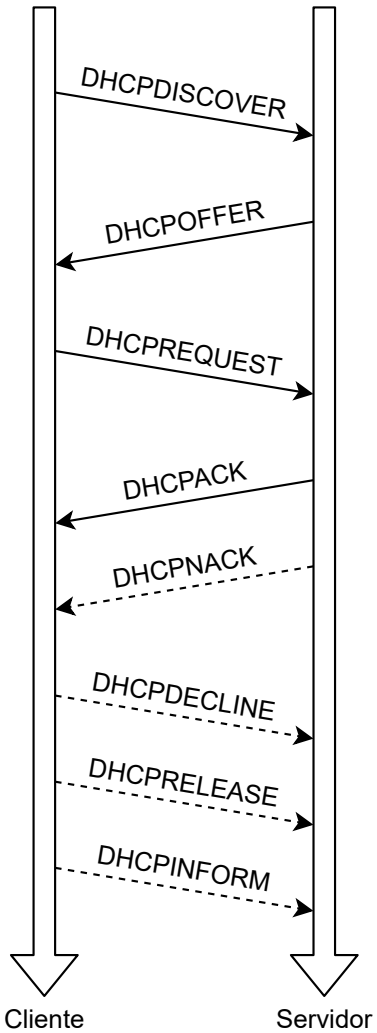


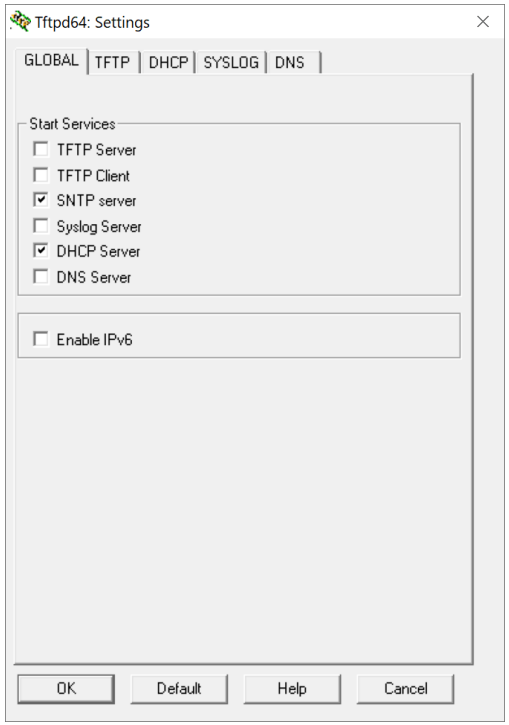


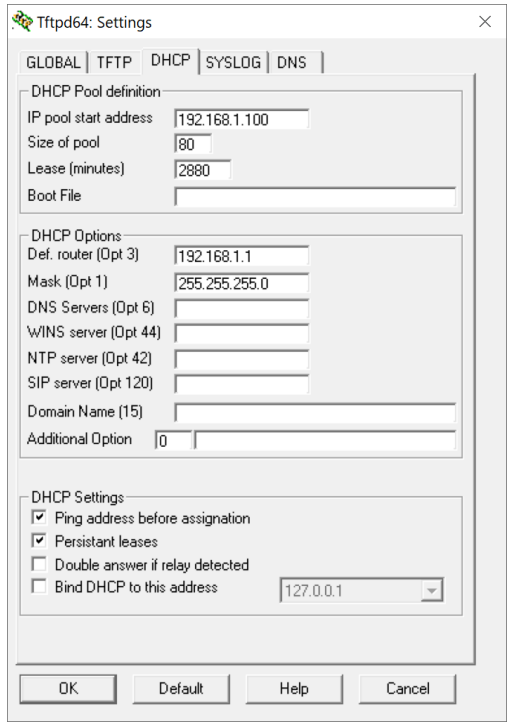
DHCP

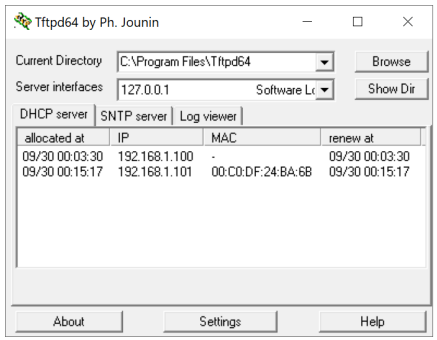
- Dynamic Host Configuration Protocol
- Configuración de red (IP address, netmask, gateway)
- Transporte UDP
- Puertos 68 (cliente) y 67 (servidor)
- IETF RFC 2131

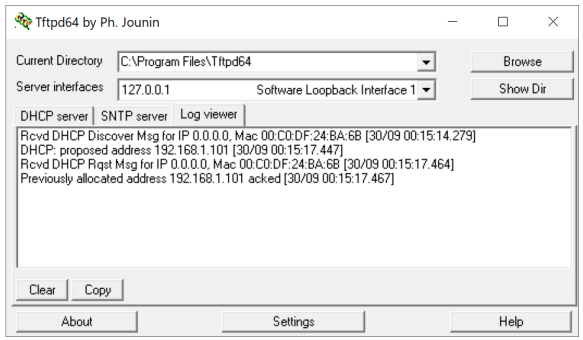
DHCP


DHCPDISCOVER
DHCPOFFER
DHCPREQUEST
DHCPACK
DHCPNACK
DHCPDECLINE
DHCPRELEASE
DHCPINFORM
Cliente
Servidor


Tftpd64: Settings
GLOBAL TFTP DHCP SYSLOG DNS
Start Services
TFTP Server
TFTP Client
SNTP server
Syslog Server
DHCP Server
DNS Server
Enable IPv6
OK Default Help Cancel

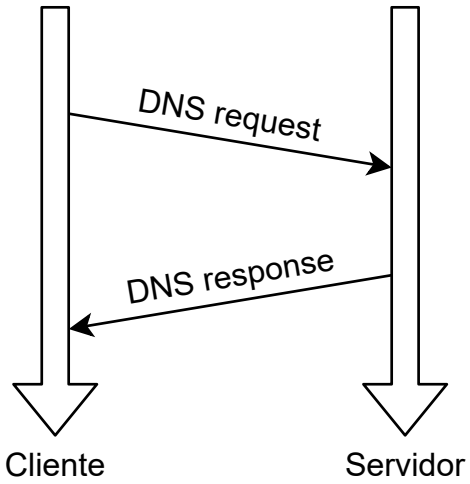

Tftpd64: Settings
GLOBAL TFTP DHCP SYSLOG DNS
DHCP Pool definition
IP pool start address 192.168.1.100
Size of pool 80
Lease (minutes) 2880
Boot File
DHCP Options
Def. router (Opt 3) 192.168.1.1
Mask (Opt 1) 255.255.255.0
DNS Servers (Opt 6)
WINS server (Opt 44)
NTP server (Opt 42)
SIP server (Opt 120)
Domain Name (15)
Additional Option 0
DHCP Settings
Ping address before assignation
Persistant leases
Double answer if relay detected
Bind DHCP to this address 127.0.0.1
OK Default Help Cancel


Tftpd64 by Ph. Jounin
Current Directory C:\Program Files\Tftpd64 Browse
Server interfaces 127.0.0.1 Show Dir
DHCP server SNTP server Log viewer
allocated at IP MAC renew at
09/30 00:03:30 192.168.1.100 - 09/30 00:03:30
09/30 00:15:17 192.168.1.101 00:C0:DF:24:BA:6B 09/30 00:15:17
About Settings Help

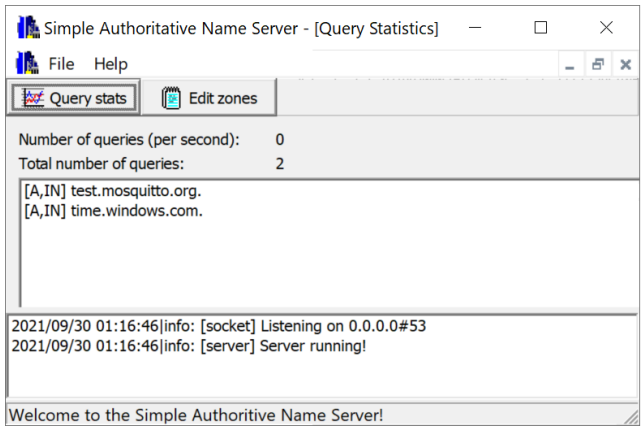

Tftpd64 by Ph. Jounin
Current Directory C:\Program Files\Tftpd64 Browse
Server interfaces 127.0.0.1 Software Loopback Interface 1 Show Dir
DHCP server SNTP server Log viewer
Rcvd DHCP Discover Msg for IP 0.0.0.0, Mac 00:C0:DF:24:BA:6B [30/09 00:15:14.279]
DHCP: proposed address 192.168.1.101 [30/09 00:15:17.447]
Rcvd DHCP Rqst Msg for IP 0.0.0.0, Mac 00:C0:DF:24:BA:6B [30/09 00:15:17.464]
Previously allocated address 192.168.1.101 acked [30/09 00:15:17.467]
Clear Copy
About Settings Help

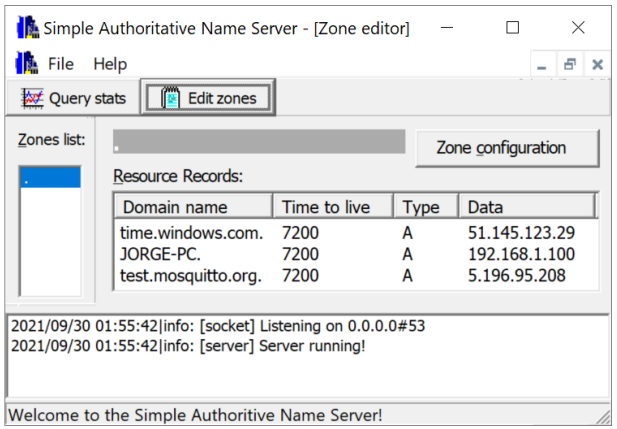
DNS

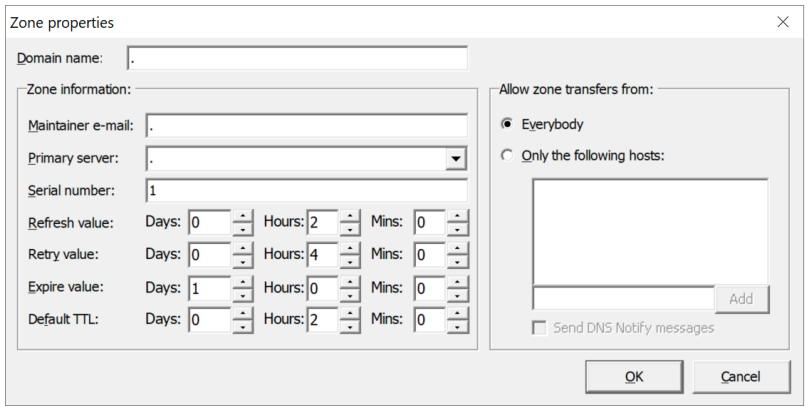
- Domain Name System
- Resolución de hostnames
- Transporte UDP (normalmente)
- Puerto 53 (servidor)
- IETF RFC 1034, 1035

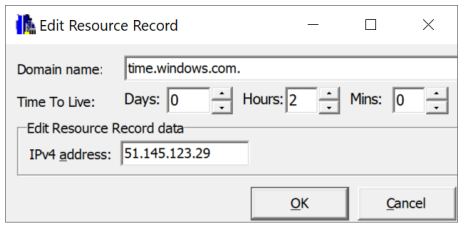


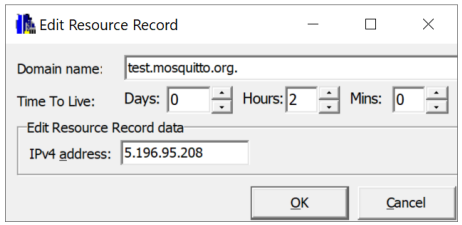
DNS

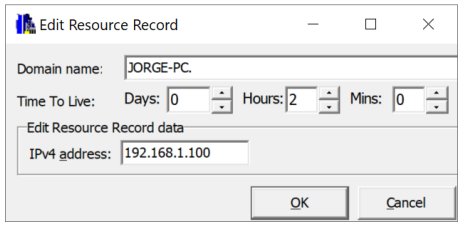

Simple Authoritative Name Server - [Query Statistics]
File Help
Query stats
Edit zones
Number of queries (per second): 0
Total number of queries: 2
[A,IN] test.mosquitto.org.
[A,IN] time.windows.com.
2021/09/30 01:16:46|info: [socket] Listening on 0.0.0.0#53
2021/09/30 01:16:46|info: [server] Server running!
Welcome to the Simple Authoritive Name Server!


Simple Authoritative Name Server - [Zone editor]
File Help
Query stats
Edit zones
Zones list:
Zone configuration
Resource Records:
Domain name | Time to live | Type | Data
time.windows.com. 7200 A 51.145.123.29
JORGE-PC. 7200 A 192.168.1.100
test.mosquitto.org. 7200 A 5.196.95.208
2021/09/30 01:55:42|info: [socket] Listening on 0.0.0.0#53
2021/09/30 01:55:42|info: [server] Server running!
Welcome to the Simple Authoritive Name Server!


Zone properties
Domain name: .
Zone information:
Maintainer e-mail: .
Primary server: .
Serial number: 1
Refresh value: Days: 0 Hours: 2 Mins: 0
Retry value: Days: 0 Hours: 4 Mins: 0
Expire value: Days: 1 Hours: 0 Mins: 0
Default TTL: Days: 0 Hours: 2 Mins: 0
Allow zone transfers from:
Everybody
Only the following hosts:
Add
Send DNS Notify messages
OK
Cancel

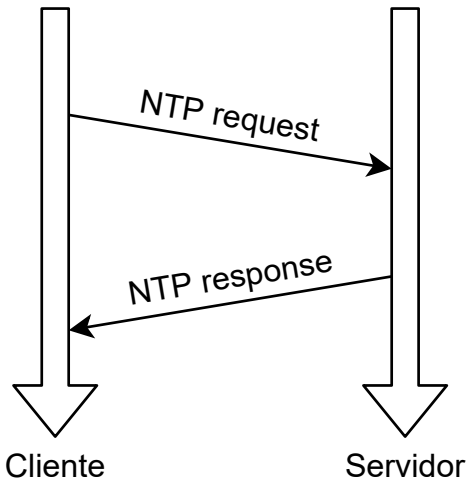

Edit Resource Record
Domain name: time.windows.com.
Time To Live: Days: 0 Hours: 2 Mins: 0
Edit Resource Record data
IPv4 address: 51.145.123.29
OK
Cancel


Edit Resource Record
Domain name: test.mosquitto.org.
Time To Live: Days: 0 Hours: 2 Mins: 0
Edit Resource Record data
IPv4 address: 5.196.95.208
OK
Cancel


Edit Resource Record
Domain name: JORGE-PC.
Time To Live: Days: 0 Hours: 2 Mins: 0
Edit Resource Record data
IPv4 address: 192.168.1.100
OK
Cancel

NTP

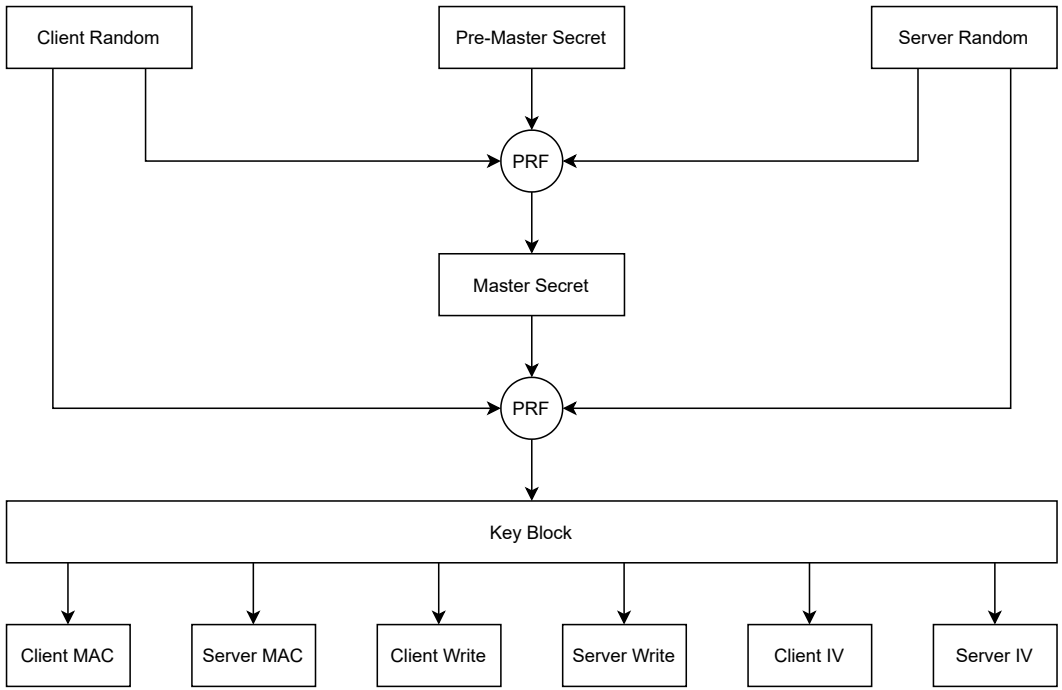
- Network Time Protocol
- Fecha y hora
- Transporte UDP (normalmente)
- Puerto 123 (servidor)
- IETF RFC 5905



TLS

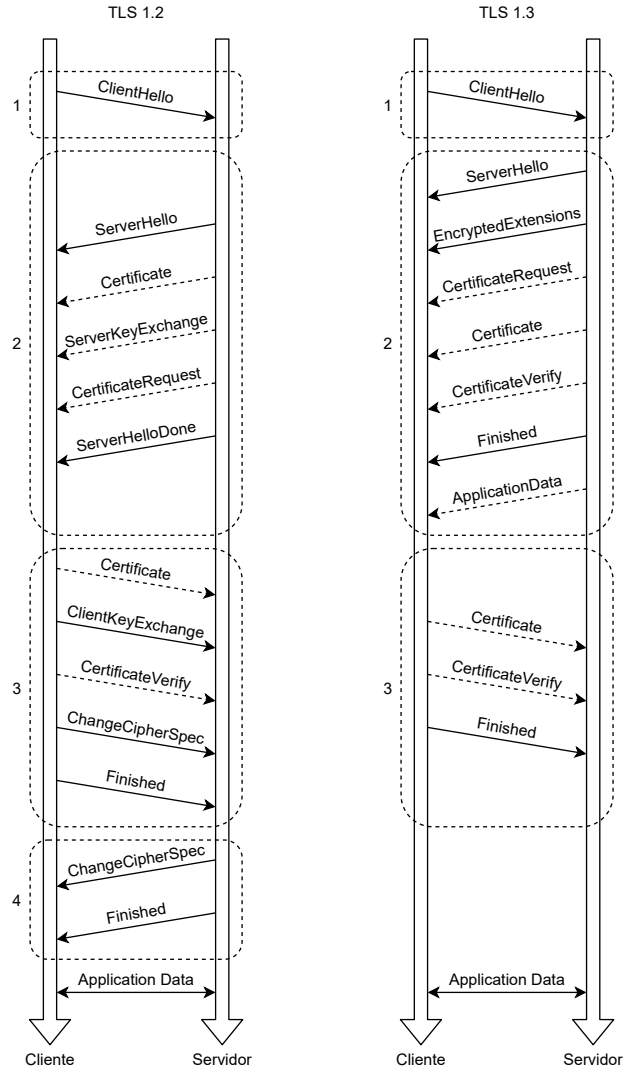
- Transport Layer Security
- Seguridad (confidencialidad, autenticación e integridad)
- Transporte TCP
- Puerto determinado por el protocolo asegurado
- IETF RFC 5246 (TLS 1.2) e IETF RFC 8446 (TLS 1.3)
- Uso de certificados digitales (normalmente)
- Handshake TLS
- Comunicación sobre el protocolo asegurado

TLS



Ejemplo de suite de cifrado

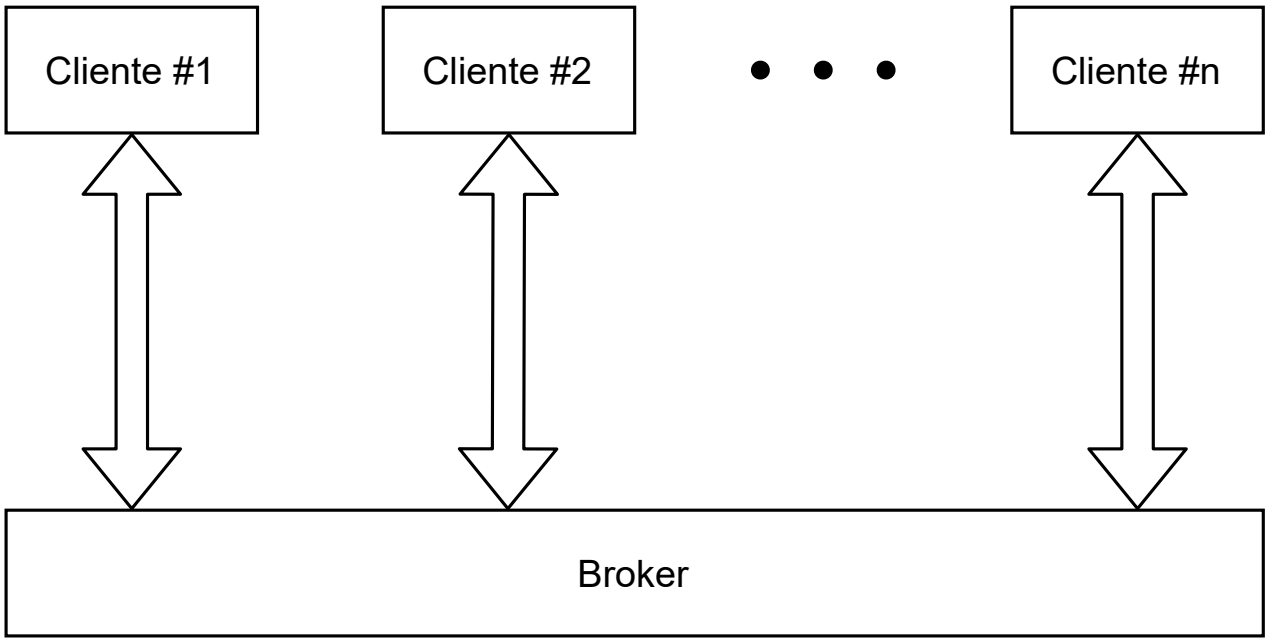
`TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384`



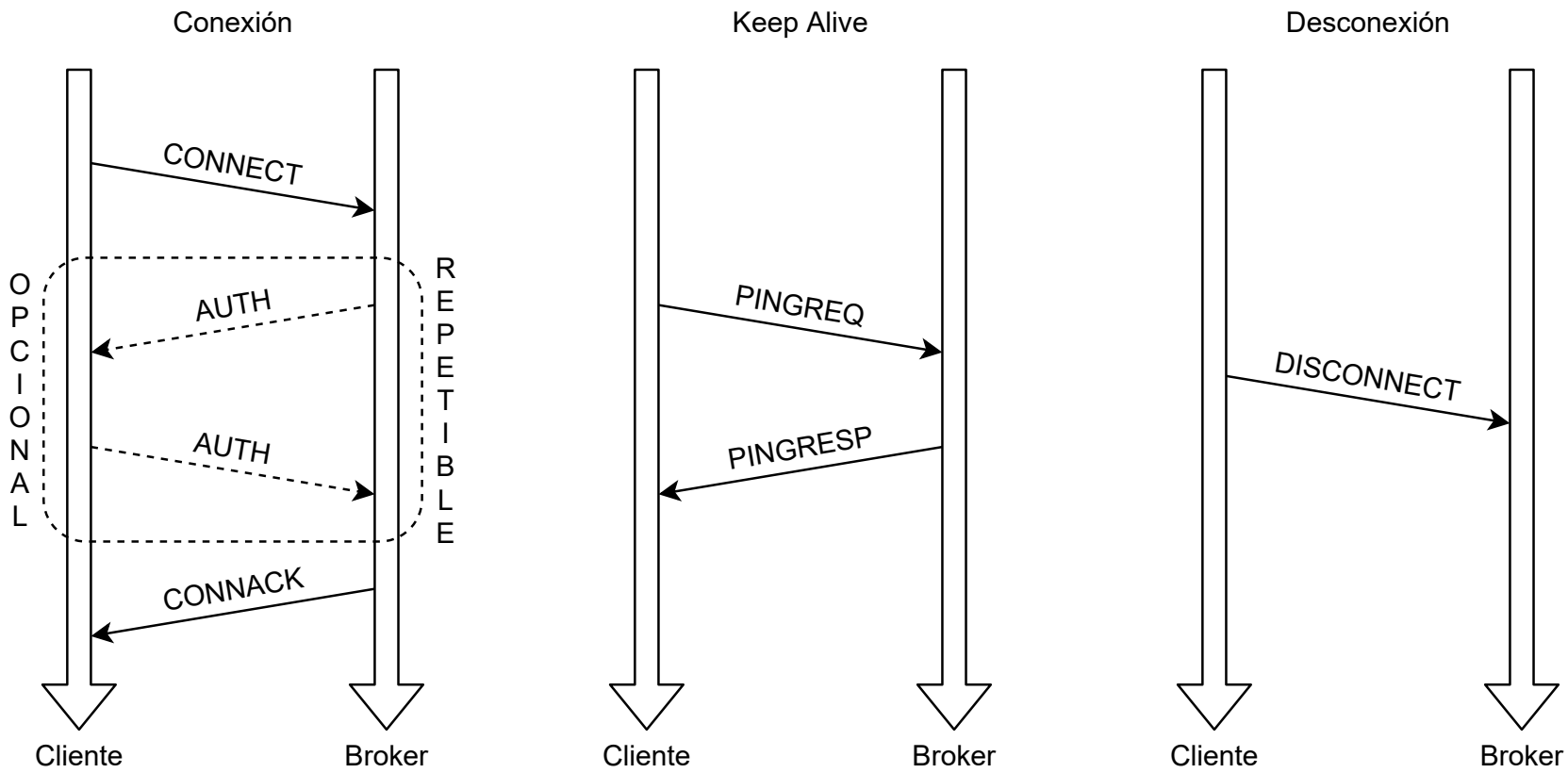
MQTT

- Message Queuing Telemetry Transport
- Mensajería
- Transporte TCP
- Puertos 1883 (servidor, inseguro) y 8883 (servidor, TLS)
- Estándar de OASIS

MQTT

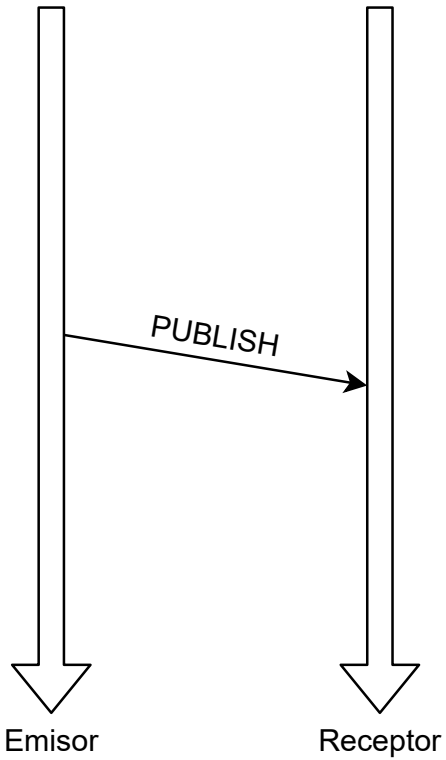


MQTT


Conexión
CONNECT
OPCIONAL
AUTH
AUTH
REPETIBLE
CONNACK
Cliente
Broker
Keep Alive
PINGREQ
PINGRESP
Cliente
Broker
Desconexión
DISCONNECT
Cliente
Broker

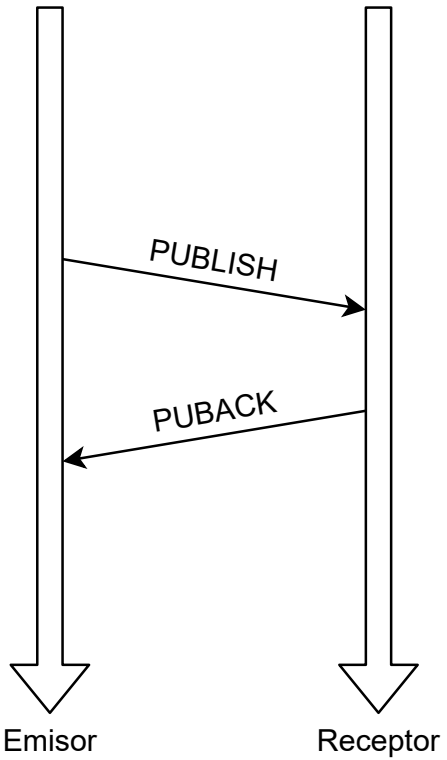
MQTT

Publicación (QoS 0)



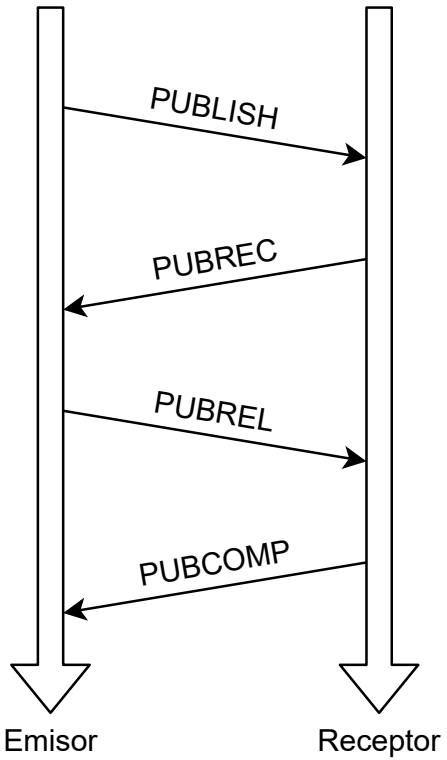
≤ 1

Publicación (QoS 1)



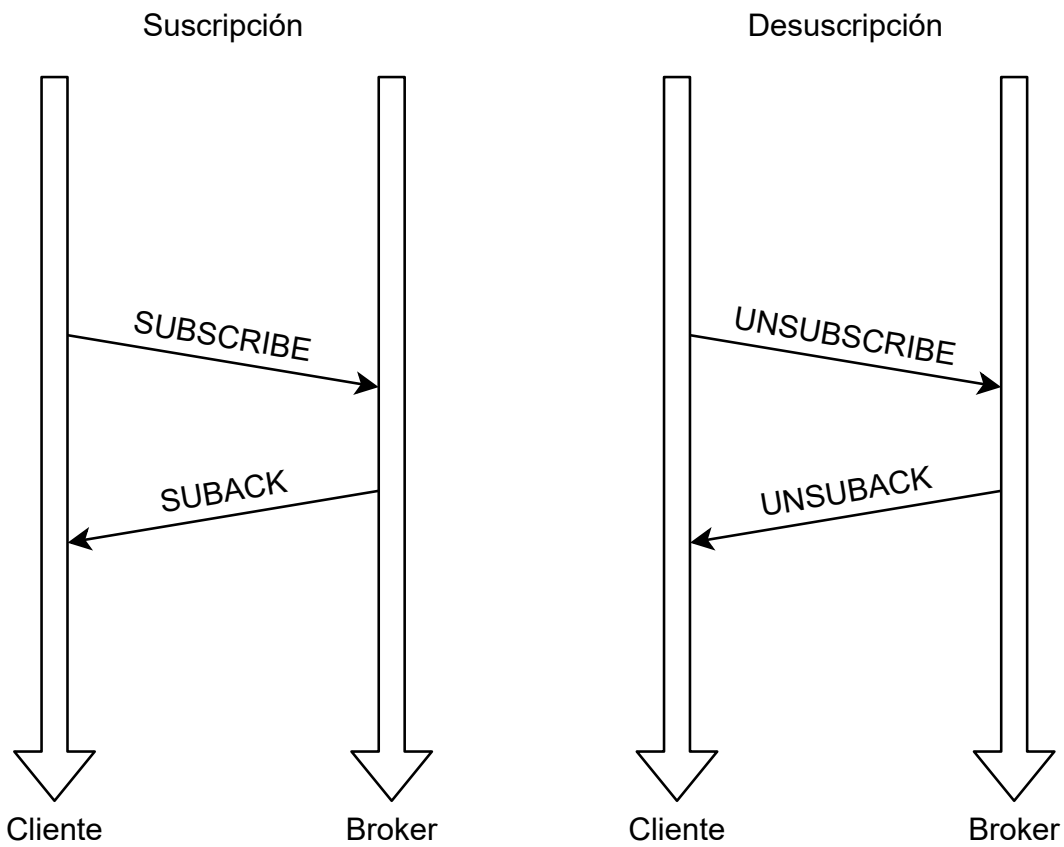
≥ 1

Publicación (QoS 2)

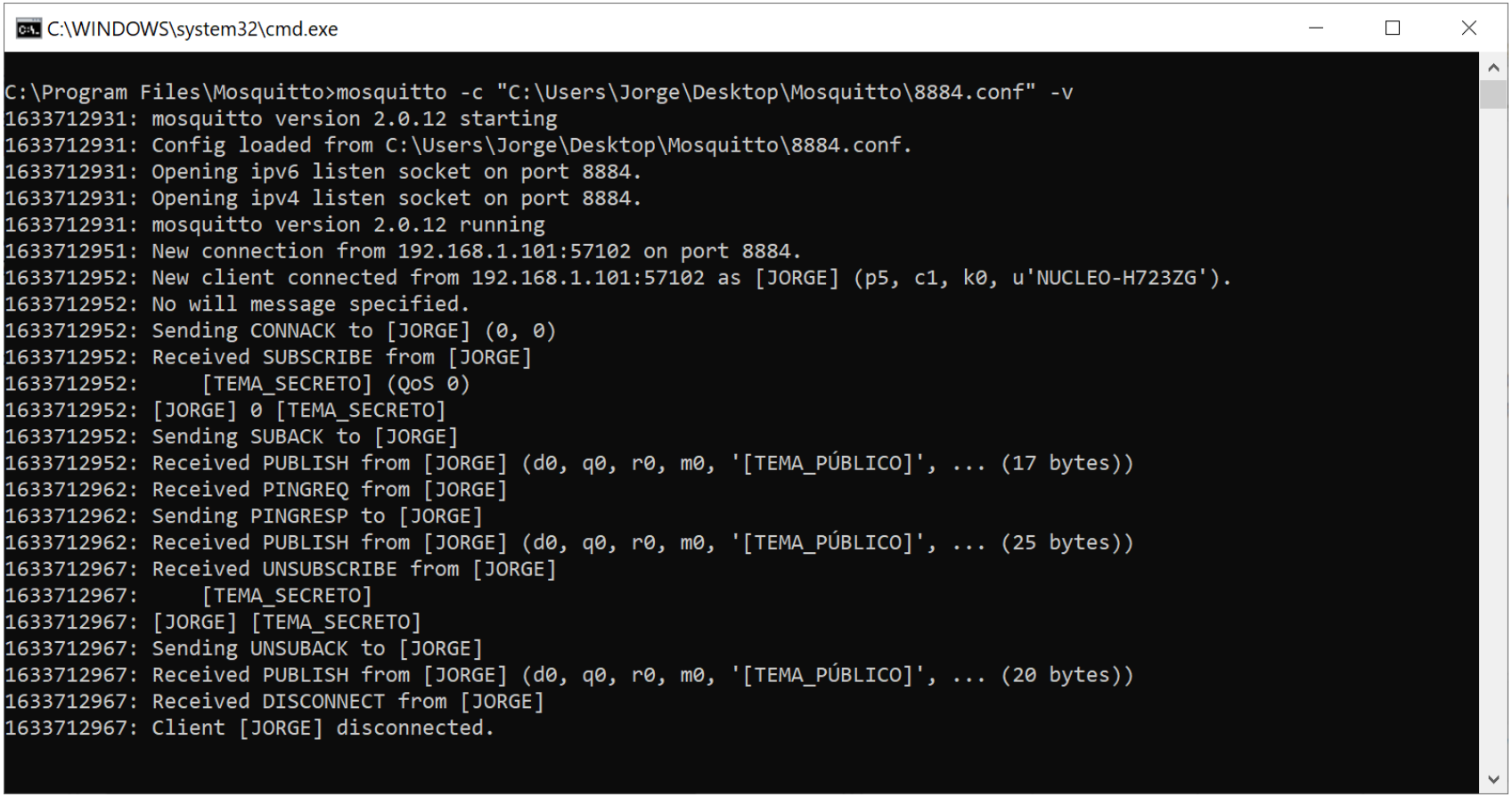


$= 1$

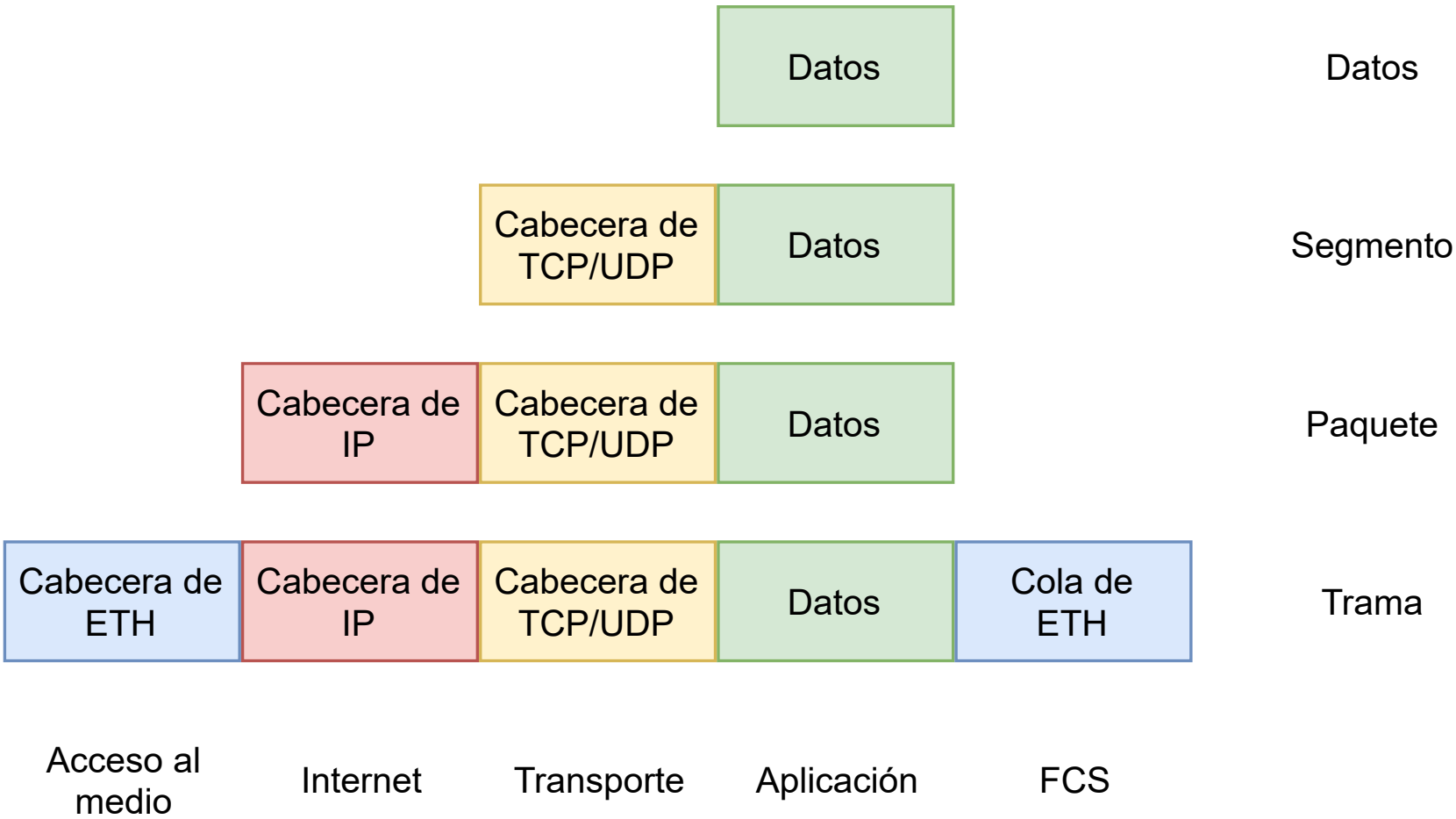
MQTT


Suscripción
SUBSCRIBE
SUBACK
Cliente
Broker
Desuscripción
UNSUBSCRIBE
UNSUBACK
Cliente
Broker

MQTT


C:\WINDOWS\system32\cmd.exe
C:\Program Files\Mosquitto>mosquitto -c "C:\Users\Jorge\Desktop\Mosquitto\8884.conf" -v
1633712931: mosquitto version 2.0.12 starting
1633712931: Config loaded from C:\Users\Jorge\Desktop\Mosquitto\8884.conf.
1633712931: Opening ipv6 listen socket on port 8884.
1633712931: Opening ipv4 listen socket on port 8884.
1633712931: mosquitto version 2.0.12 running
1633712951: New connection from 192.168.1.101:57102 on port 8884.
1633712952: New client connected from 192.168.1.101:57102 as [JORGE] (p5, c1, k0, u'NUCLEO-H723ZG').
1633712952: No will message specified.
1633712952: Sending CONNACK to [JORGE] (0, 0)
1633712952: Received SUBSCRIBE from [JORGE]
1633712952: [TEMA_SECRETO] (QoS 0)
1633712952: [JORGE] 0 [TEMA_SECRETO]
1633712952: Sending SUBACK to [JORGE]
1633712952: Received PUBLISH from [JORGE] (d0, q0, r0, m0, '[TEMA_PÚBLICO]', ... (17 bytes))
1633712962: Received PINGREQ from [JORGE]
1633712962: Sending PINGRESP to [JORGE]
1633712962: Received PUBLISH from [JORGE] (d0, q0, r0, m0, '[TEMA_PÚBLICO]', ... (25 bytes))
1633712967: Received UNSUBSCRIBE from [JORGE]
1633712967: [TEMA_SECRETO]
1633712967: [JORGE] [TEMA_SECRETO]
1633712967: Sending UNSUBACK to [JORGE]
1633712967: Received PUBLISH from [JORGE] (d0, q0, r0, m0, '[TEMA_PÚBLICO]', ... (20 bytes))
1633712967: Received DISCONNECT from [JORGE]
1633712967: Client [JORGE] disconnected.

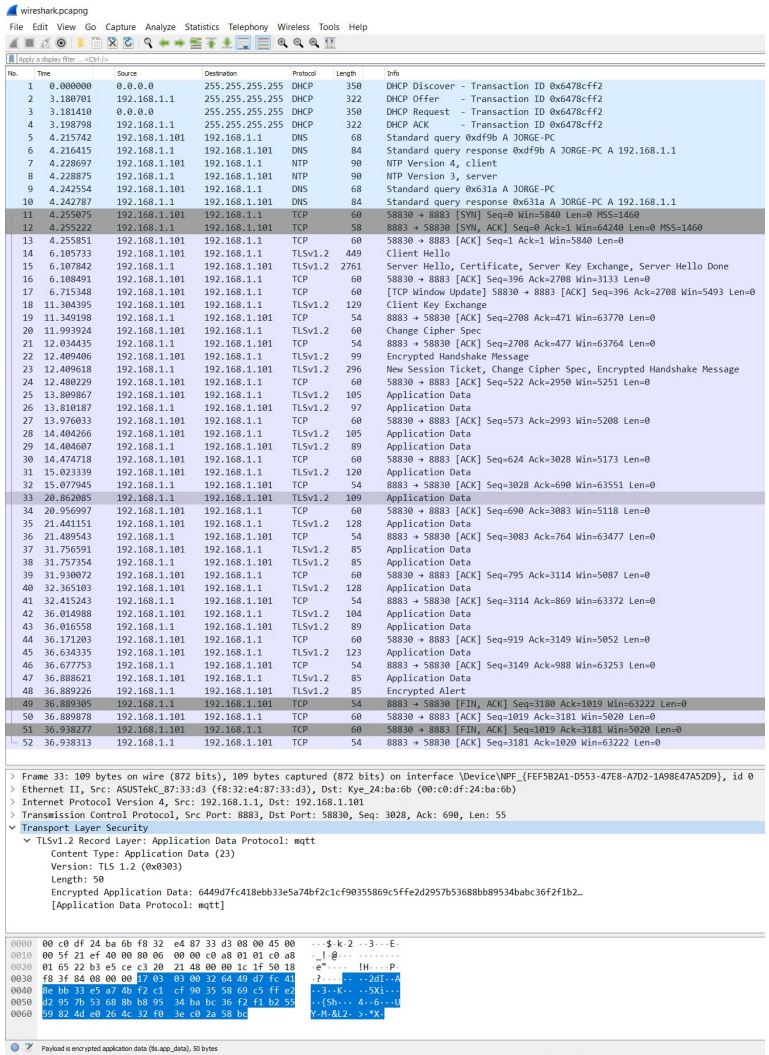
Análisis de protocolos



Análisis de protocolos

Sesión encriptada (TLS 1.2)

¿Qué contienen los datos de la trama 33?



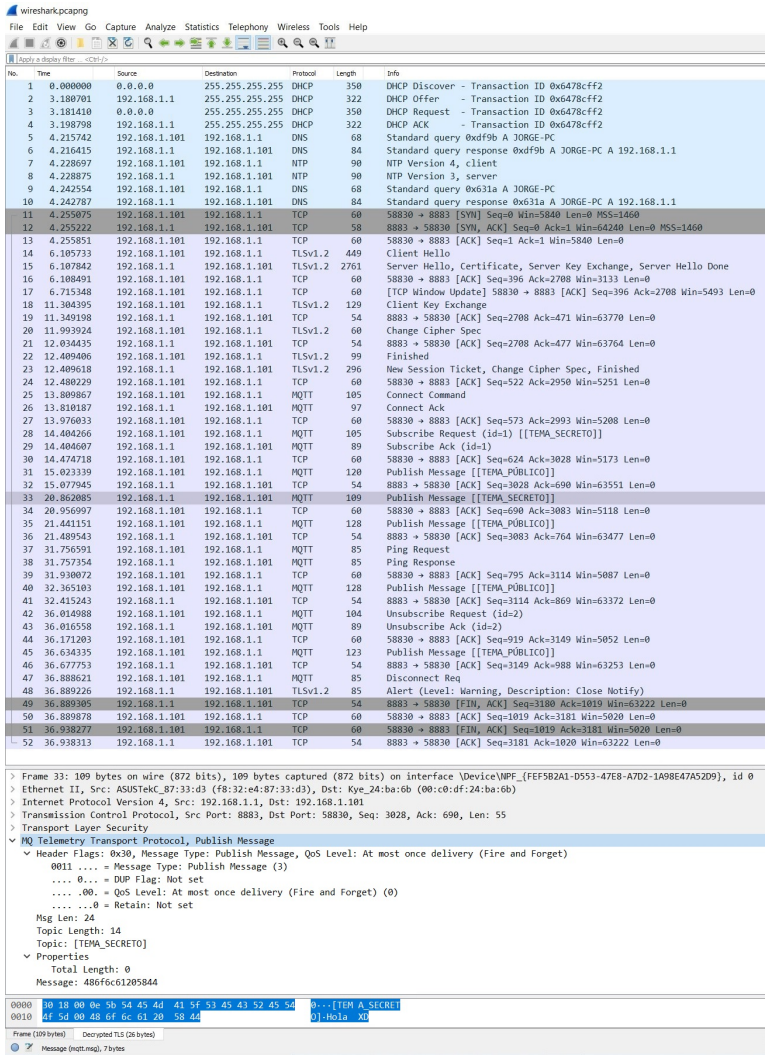
Análisis de protocolos

Sesión desencriptada

Datos de la trama 33

Paquete PUBLISH

```
Tema    : [TEMA_SECRETO]
Mensaje : Hola XD
```

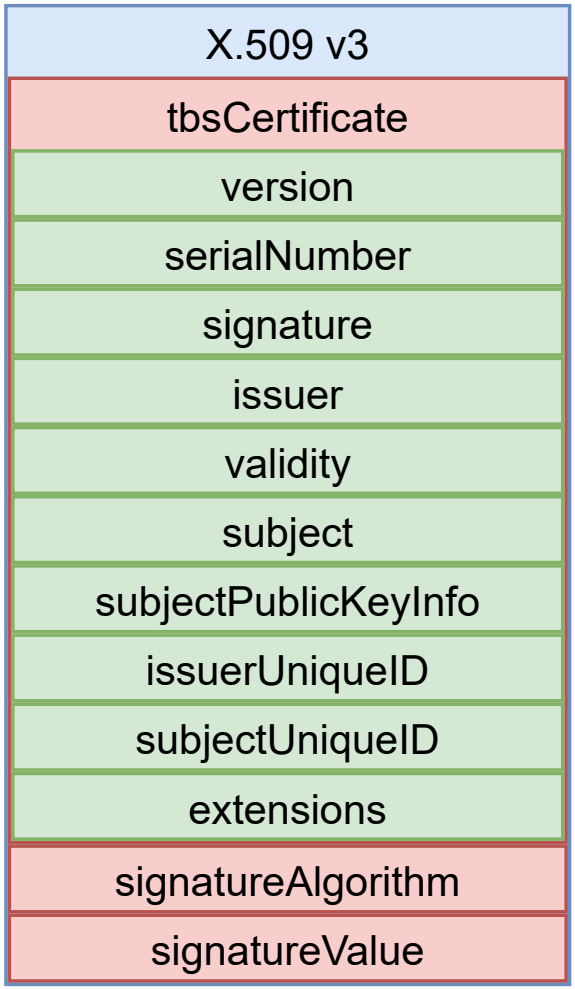


Certificados X.509

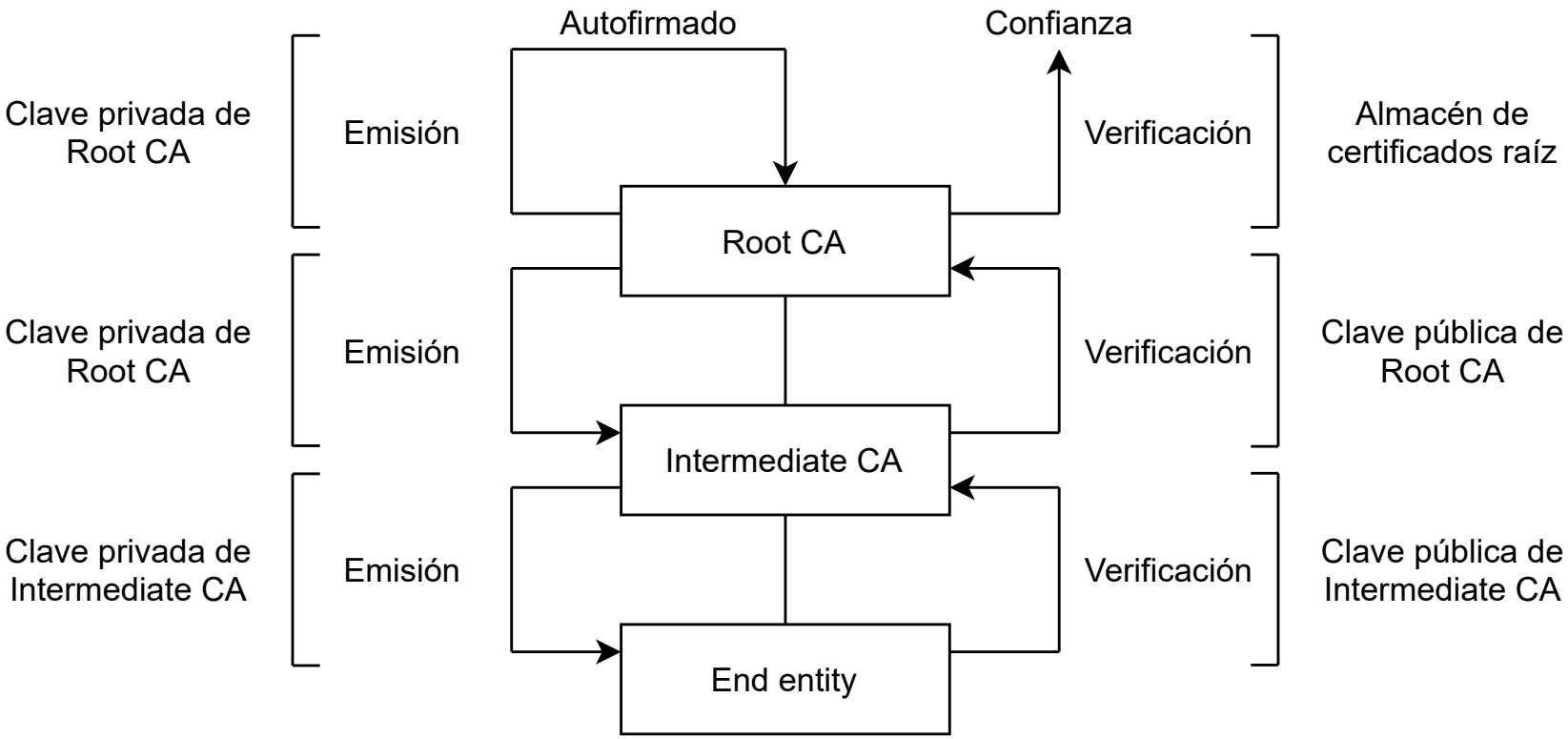
- Firma de documentos
- Cifrado de mensajes
- Autenticación de usuarios

- Par de claves (KEY)
- Solicitud de firma del certificado (CSR)
- Certificado X.509 (CRT)
- Lista de revocación (CRL)

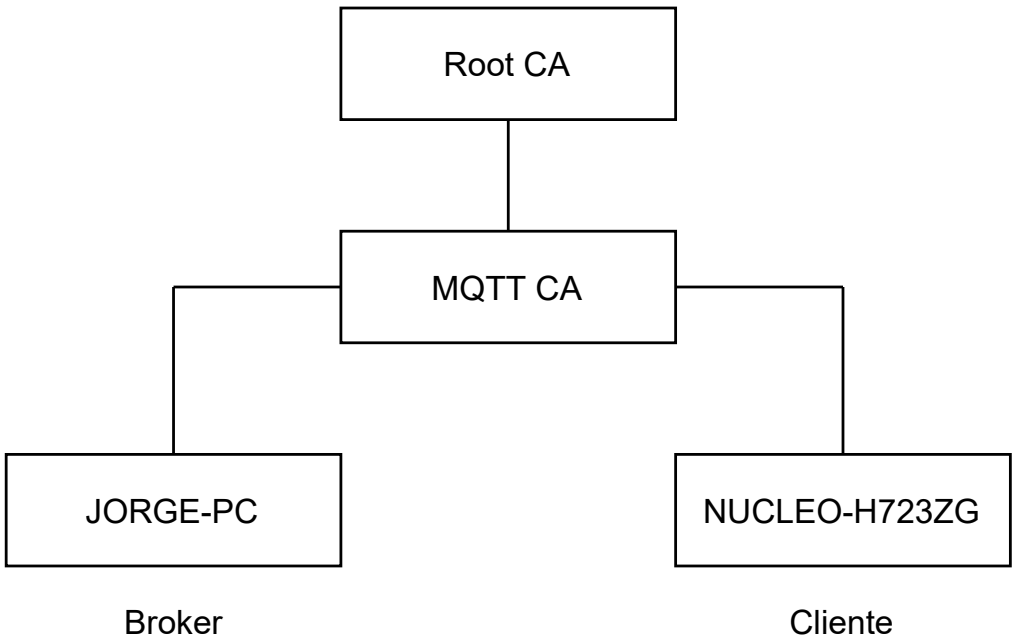
- DER (binario) o PEM (ASCII)



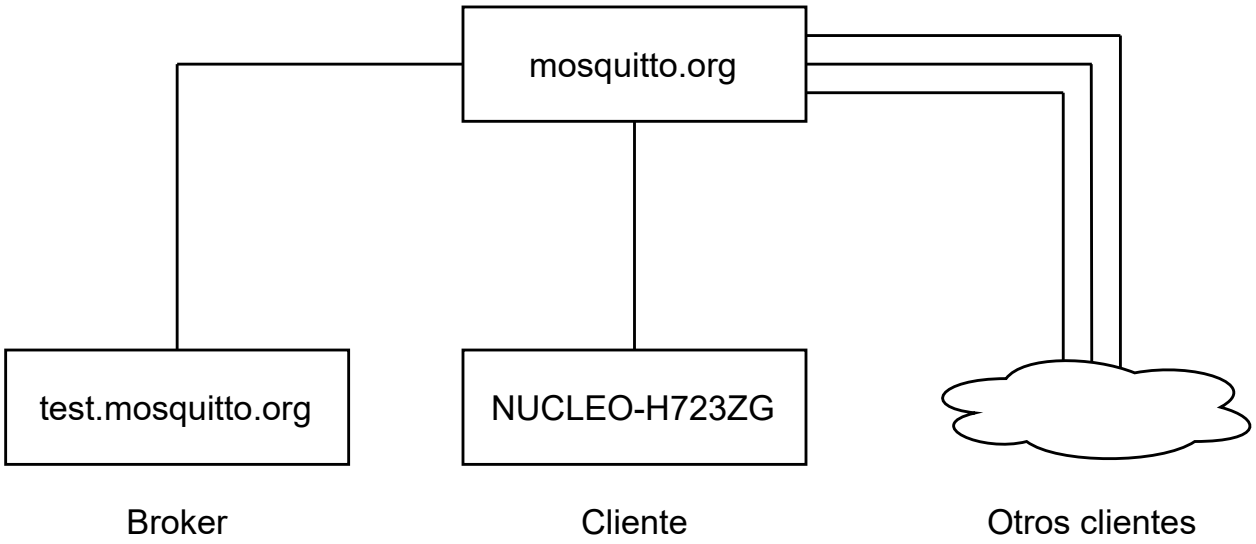
Cadenas de confianza



Intranet



Internet


mosquitto.org
test.mosquitto.org
NUCLEO-H723ZG
Broker
Cliente
Otros clientes

Modo normal

- DHCP → DNS → NTP → DNS → TLS → MQTT
- Se suscribe al tema secreto.
- Realiza publicaciones en el tema público.
- Enciende/apaga LEDs al recibir determinados comandos.
- Notifica de eventos (p.e. "`[LED 1 ENCENDIDO]`").
- Publica periódicamente la fecha y hora.
- Finaliza el programa pulsando un botón.

Modo de pruebas

- Habilitarlo en el fichero de configuración de la aplicación.
- DHCP $\rightarrow$ DNS $\rightarrow$ NTP $\rightarrow$ DNS $\rightarrow$ TLS $\rightarrow$ MQTT
- Tener pulsado el botón.
- Se suscribe al tema secreto.
- Realiza publicaciones periódicas en el tema secreto.
- Tema publicaciones = Tema suscrito $\rightarrow$ Enviado = Recibido
- Mide los tiempos de escritura y lectura de paquetes MQTT.
- Repite un número de ciclos.
- Calcula y muestra los tiempos de cada ciclo y los promedios.
- Finaliza el programa.

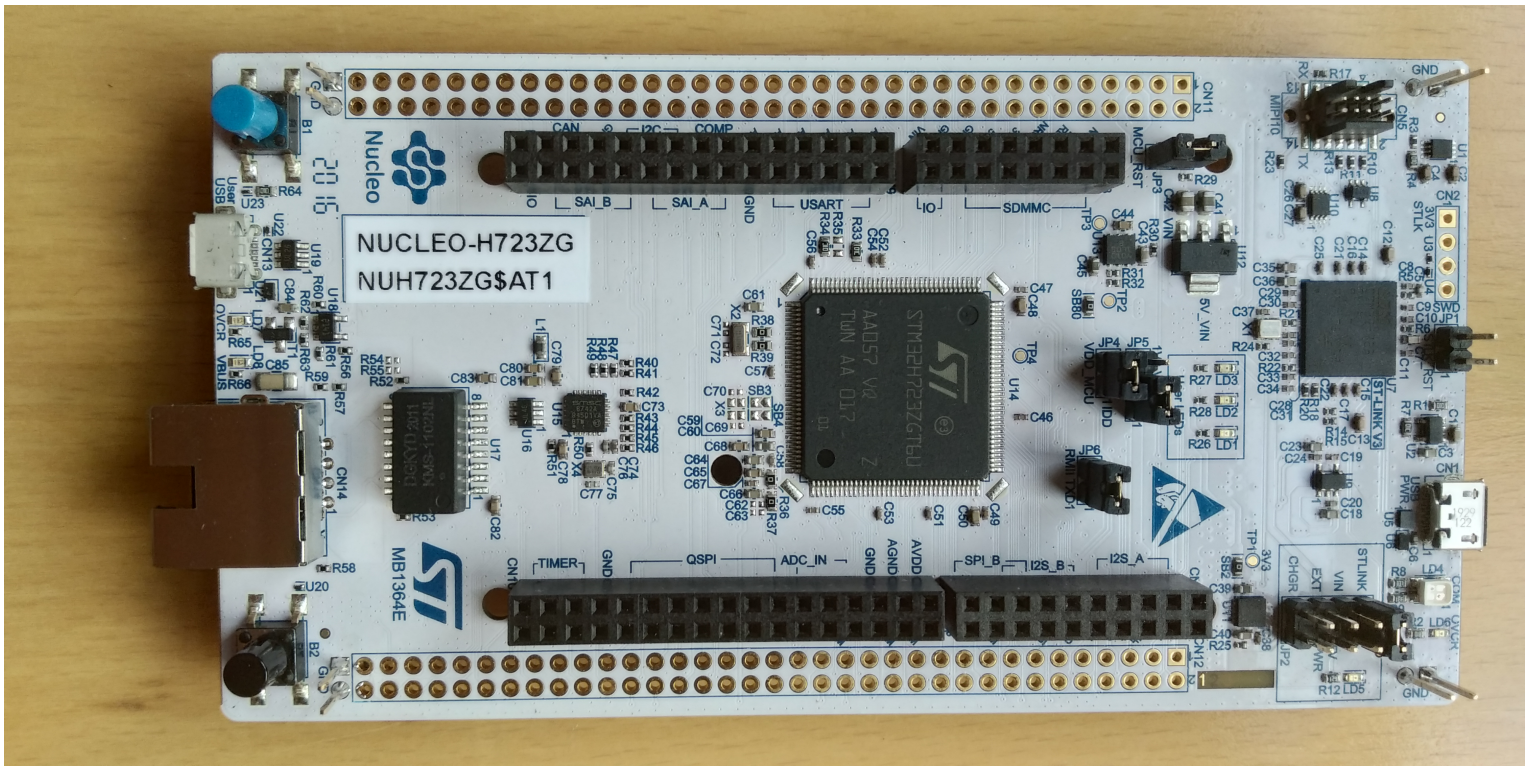
Configuración

- Nombre de la plataforma
- Depuración por la UART
- Intentos del cliente DHCP y configuración de red estática
- Servidor DNS
- Servidor NTP y zona horaria GMT
- Uso de TLS, autenticación del cliente y depuración de TLS
- Broker MQTT, ID, Keep Alive, tema público y tema secreto
- Modo de pruebas, bytes por mensaje MQTT y ciclos totales

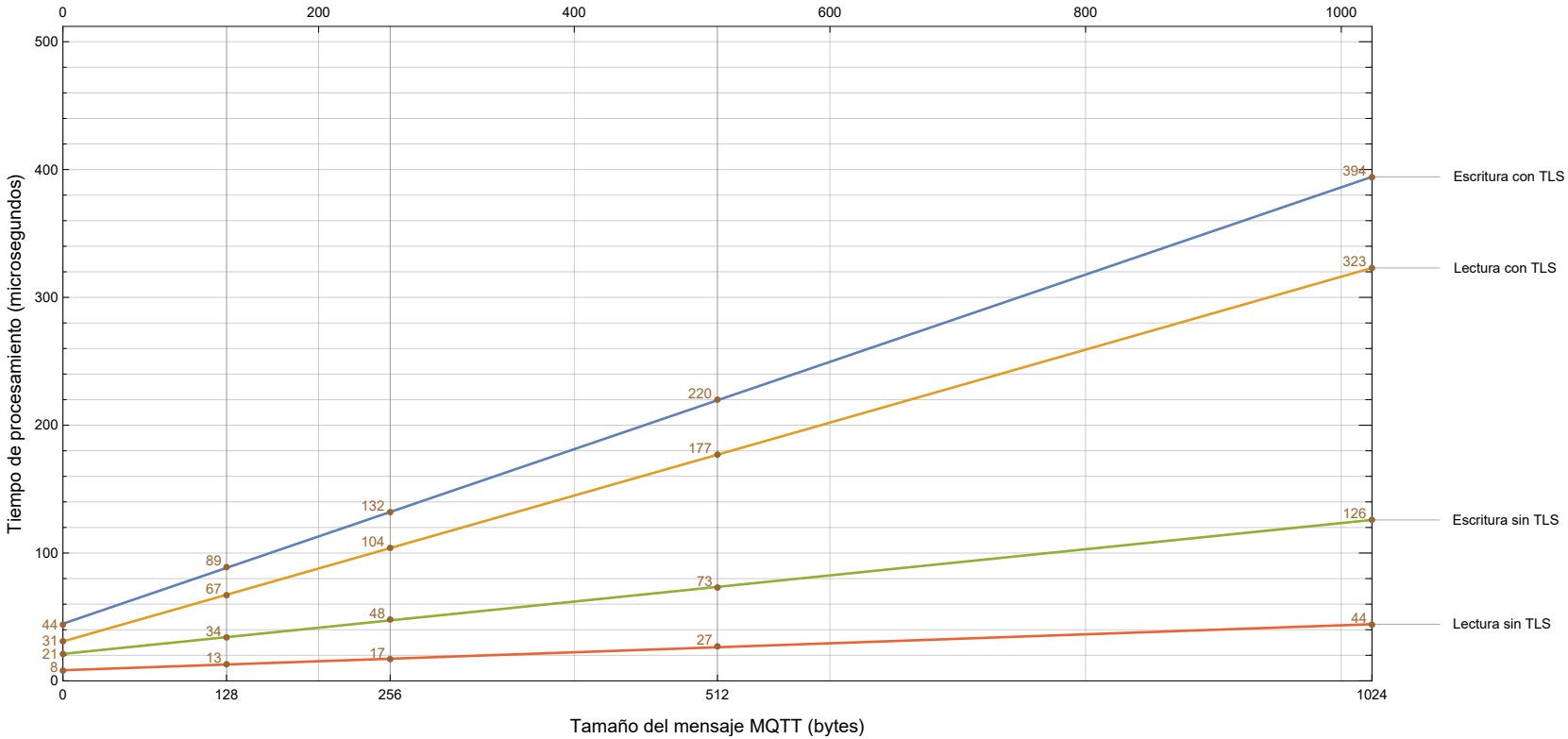
Configuración

- Certificado raíz de confianza
- Certificado del cliente
- Par de claves del cliente

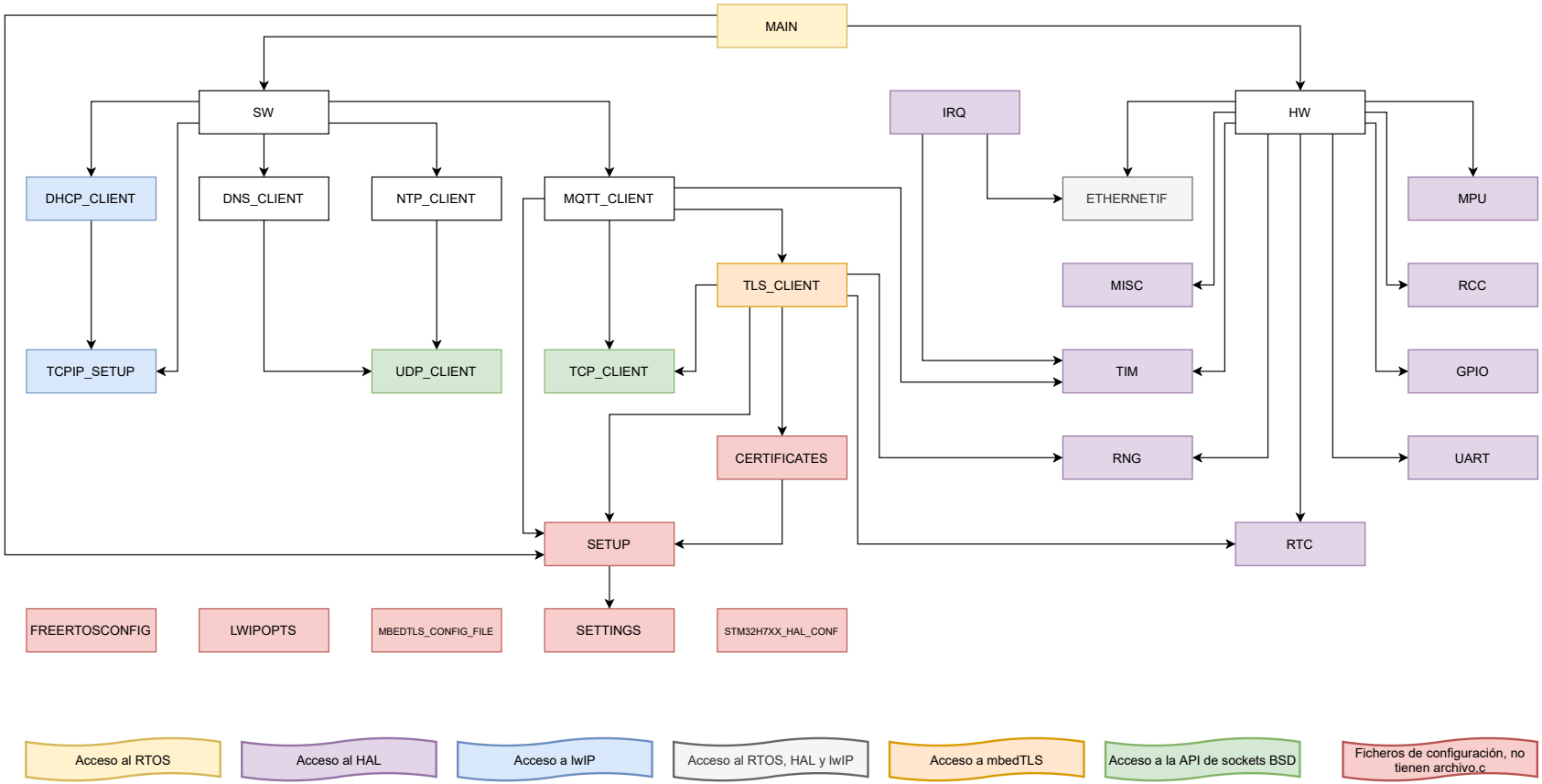
Sistema embebido



Rendimiento



Mapa de dependencias



Código fuente

- Lenguaje C (todo)
- API de sockets BSD (clientes portables)
- Licencia MIT (aplicación) y también otras (librerías)
- Estilo de programación propio (aplicación)

Librerías

- CMSIS (Core + RTOS2)
- FreeRTOS
- lwIP
- mbedTLS
- STM32H7 (drivers HAL + BSP)

Desarrollo

- STM32CubeIDE
- GNU Compiler Collection

Portabilidad

Demostraciones

- NUCLEO-H723ZG (usando el modo normal)
- DISCO-F769NI (usando el modo de pruebas)

Conclusiones

- Clientes sencillos y fáciles de usar, ideales para fines didácticos
- µCs en los que es viable usar TLS, pese a su gran sobrecarga
- Material útil sobre TCP/IP, PKI y STM32

Trabajo futuro

- Desarrollar un cliente DHCP con la API de sockets BSD.
- Mejorar el cliente DNS.
- Actualizar el cliente TLS a la versión 1.3 del protocolo.
- Añadir al cliente MQTT los QoS 1 y 2.
- Estudiar el uso de otros stacks de TCP/IP y de TLS.
- Crear un port para PC.