IoT Security and Privacy

Assignment 3 – MQTT

Team:

Kiran Shettar
Tarun Jaykumar Moorjani
Omkar Salunke
Rohan Girase

Requirements:

1. Set up the mosquitto MQTT system. Test the system works with either programs or *mosquitto_sub* and *mosquitto_pub* from *mosquitto*. Document the setup procedure and test results, including all the commands.

Solution: We have installed the Mosquitto Broker and Mosquitto Client on the Raspberry Pi and updated our raspberry pi with following commands:

```
sudo apt-get update
sudo apt-get upgrade
sudo apt-get install mosquitto
sudo apt-get install mosquitto-clients
```

we have IP address set up as below:

IP Address: 129.63.17.135
Loopback address: 127.0.0.1

Post update, all configuration for implementing publisher-subscriber model must be done in */etc/mosquitto/mosquitto.conf*

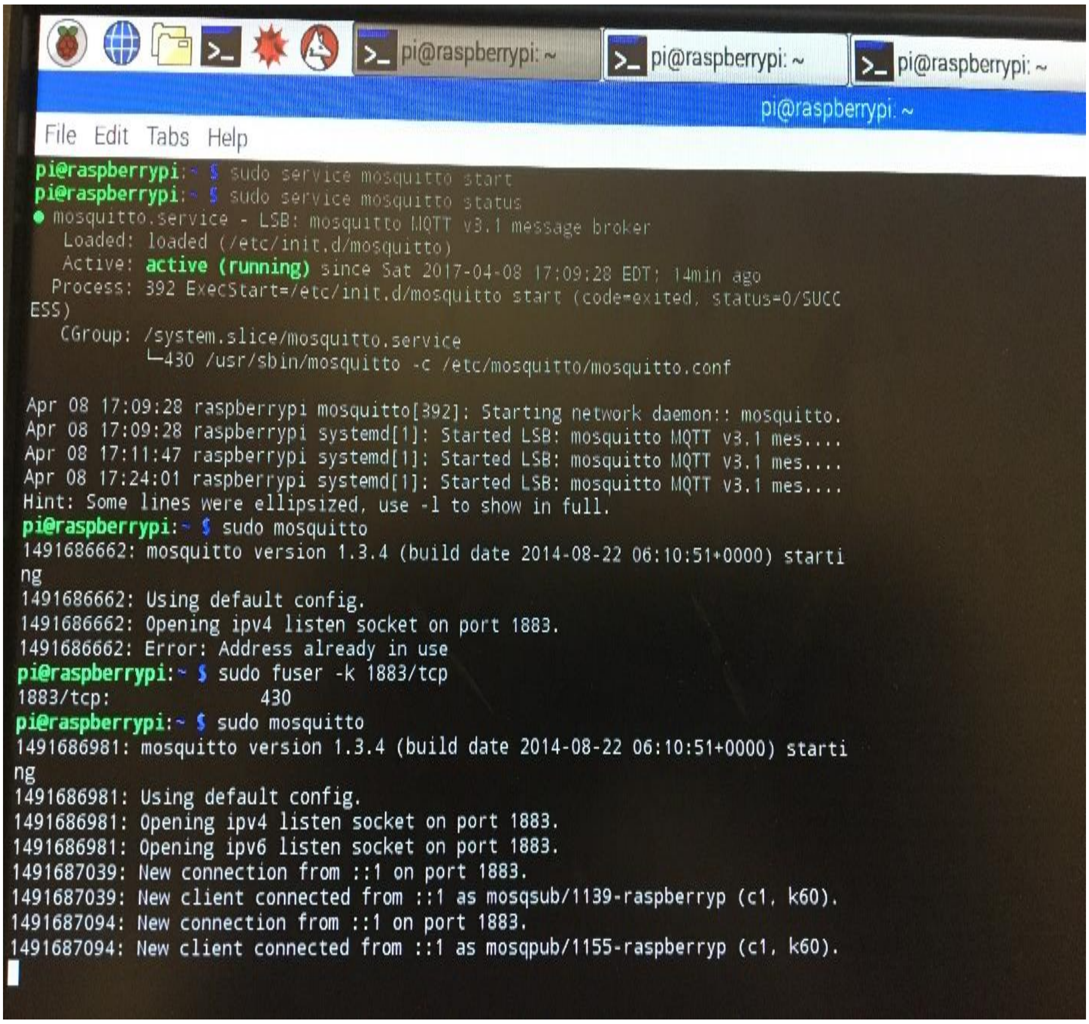
Please refer below changes to be done to configuration file:

```
pid_file /var/run/mosquitto.pid
persistence true
persistence_location /var/lib/mosquitto/
```

Post changes, restart raspberry pi and execute below commands:

```
sudo service mosquitto start
sudo service mosquitto status
```

Post this, we get below output:



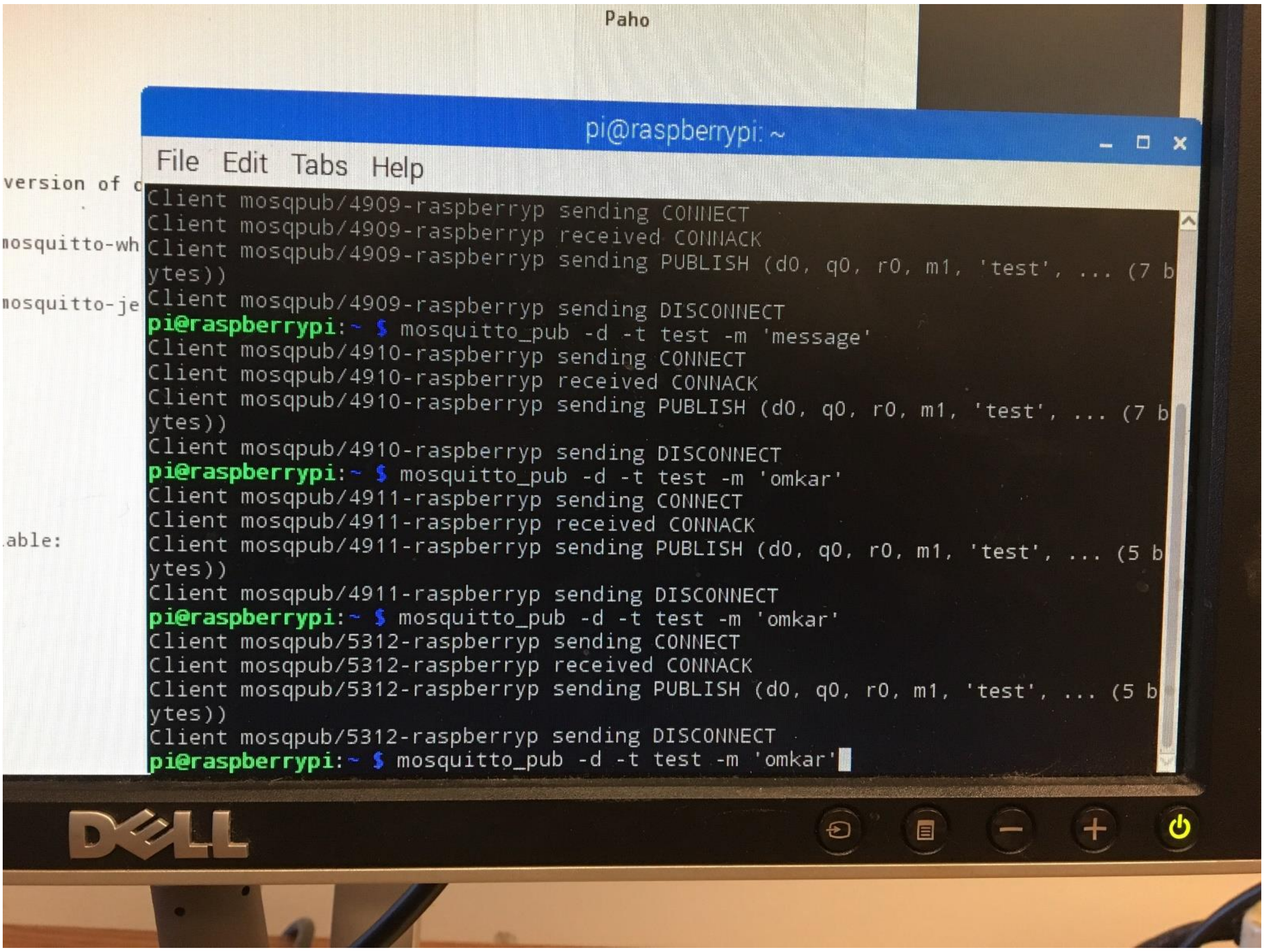
```
pi@raspberrypi:~ $ sudo service mosquitto start
pi@raspberrypi:~ $ sudo service mosquitto status
● mosquitto.service - LSB: mosquitto MQTT v3.1 message broker
   Loaded: loaded (/etc/init.d/mosquitto)
   Active: active (running) since Sat 2017-04-08 17:09:28 EDT; 14min ago
  Process: 392 ExecStart=/etc/init.d/mosquitto start (code=exited, status=0/SUCC
ESS)
   CGroup: /system.slice/mosquitto.service
           └─430 /usr/sbin/mosquitto -c /etc/mosquitto/mosquitto.conf

Apr 08 17:09:28 raspberrypi mosquitto[392]: Starting network daemon:: mosquitto.
Apr 08 17:09:28 raspberrypi systemd[1]: Started LSB: mosquitto MQTT v3.1 mes....
Apr 08 17:11:47 raspberrypi systemd[1]: Started LSB: mosquitto MQTT v3.1 mes....
Apr 08 17:24:01 raspberrypi systemd[1]: Started LSB: mosquitto MQTT v3.1 mes....
Hint: Some lines were ellipsized, use -l to show in full.
pi@raspberrypi:~ $ sudo mosquitto
1491686662: mosquitto version 1.3.4 (build date 2014-08-22 06:10:51+0000) starti
ng
1491686662: Using default config.
1491686662: Opening ipv4 listen socket on port 1883.
1491686662: Error: Address already in use
pi@raspberrypi:~ $ sudo fuser -k 1883/tcp
1883/tcp:              430
pi@raspberrypi:~ $ sudo mosquitto
1491686981: mosquitto version 1.3.4 (build date 2014-08-22 06:10:51+0000) starti
ng
1491686981: Using default config.
1491686981: Opening ipv4 listen socket on port 1883.
1491686981: Opening ipv6 listen socket on port 1883.
1491687039: New connection from ::1 on port 1883.
1491687039: New client connected from ::1 as mosqsub/1139-raspberryp (c1, k60).
1491687094: New connection from ::1 on port 1883.
1491687094: New client connected from ::1 as mosqpub/1155-raspberryp (c1, k60).
```

Once we have setup running, we will setup server on one raspberry pi terminal 1 using below command

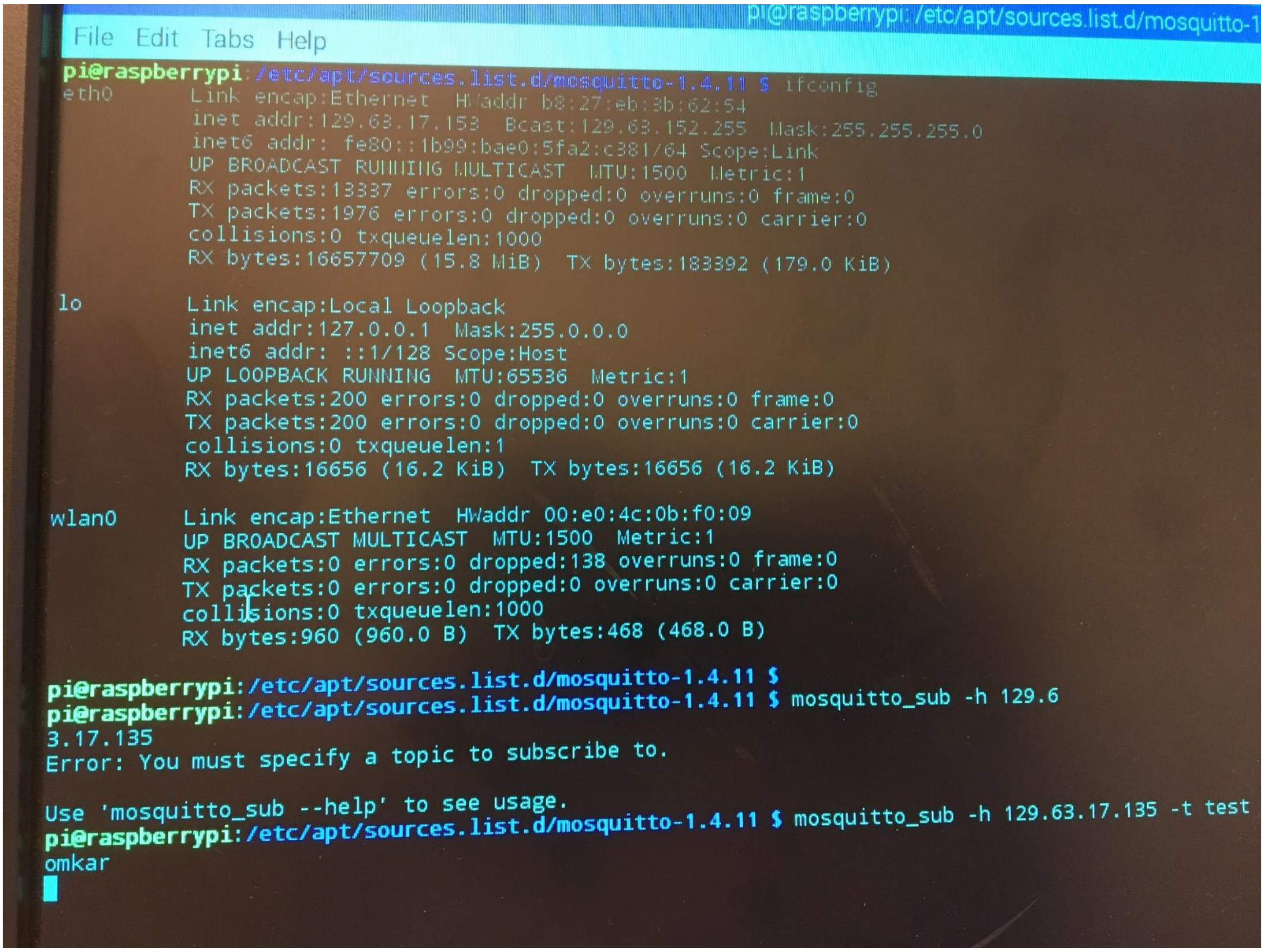
mosquitto_pub -d -t test –m “message”
mosquitto_pub -d -t test –m “omkar”

Once we have setup running, we will setup server on one raspberry pi terminal 2 using below command

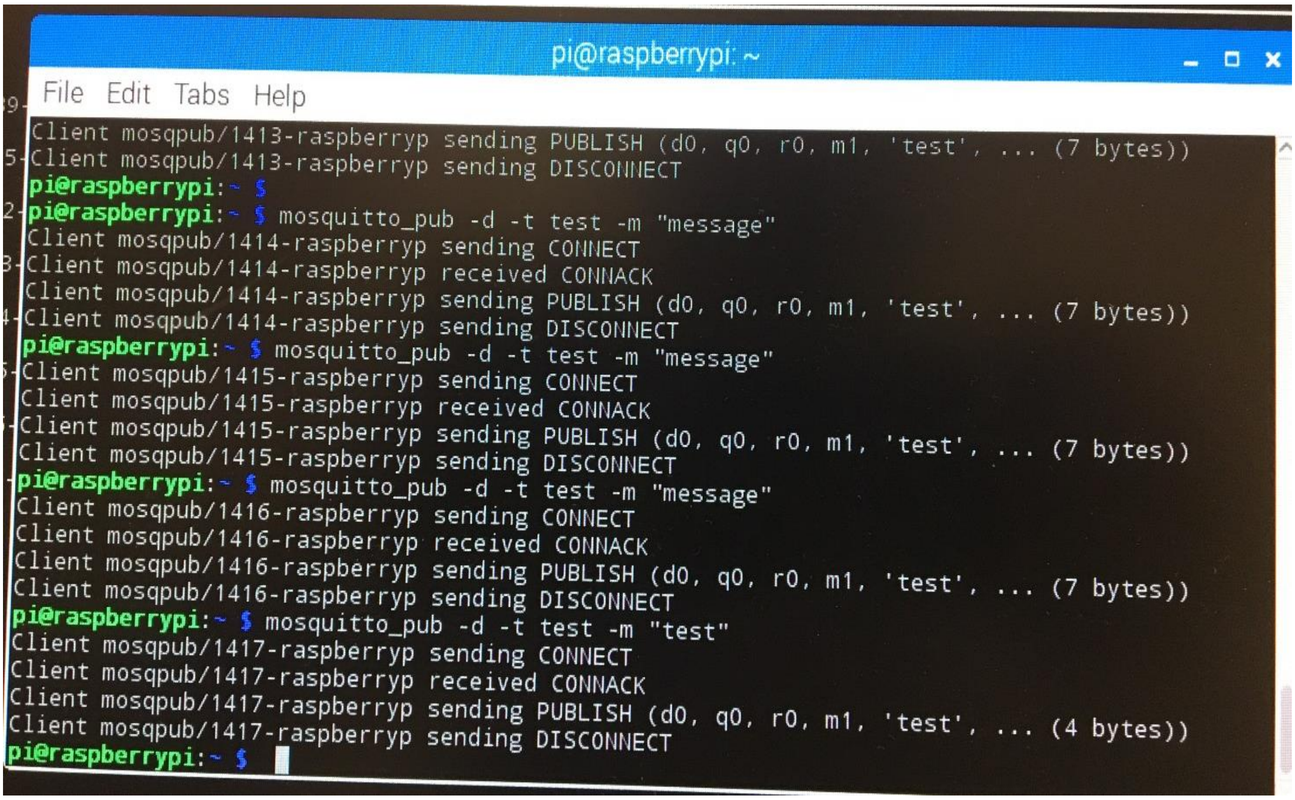
mosquitto_sub -h 129.63.17.135 -t test omkar



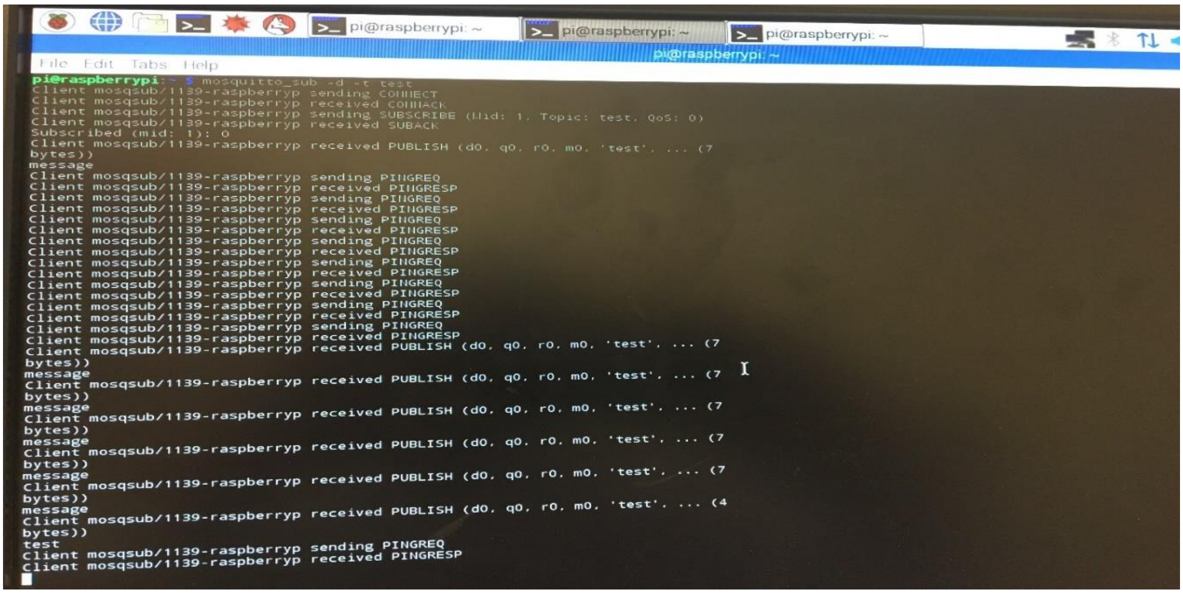
```
Client mosqpub/4909-raspberryp sending CONNECT
Client mosqpub/4909-raspberryp received CONNACK
Client mosqpub/4909-raspberryp sending PUBLISH (d0, q0, r0, m1, 'test', ... (7 b
ytes))
Client mosqpub/4909-raspberryp sending DISCONNECT
pi@raspberrypi:~ $ mosquitto_pub -d -t test -m 'message'
Client mosqpub/4910-raspberryp sending CONNECT
Client mosqpub/4910-raspberryp received CONNACK
Client mosqpub/4910-raspberryp sending PUBLISH (d0, q0, r0, m1, 'test', ... (7 b
ytes))
Client mosqpub/4910-raspberryp sending DISCONNECT
pi@raspberrypi:~ $ mosquitto_pub -d -t test -m 'omkar'
Client mosqpub/4911-raspberryp sending CONNECT
Client mosqpub/4911-raspberryp received CONNACK
Client mosqpub/4911-raspberryp sending PUBLISH (d0, q0, r0, m1, 'test', ... (5 b
ytes))
Client mosqpub/4911-raspberryp sending DISCONNECT
pi@raspberrypi:~ $ mosquitto_pub -d -t test -m 'omkar'
Client mosqpub/5312-raspberryp sending CONNECT
Client mosqpub/5312-raspberryp received CONNACK
Client mosqpub/5312-raspberryp sending PUBLISH (d0, q0, r0, m1, 'test', ... (5 b
ytes))
Client mosqpub/5312-raspberryp sending DISCONNECT
pi@raspberrypi:~ $ mosquitto_pub -d -t test -m 'omkar'
```



```
pi@raspberrypi:/etc/apt/sources.list.d/mosquitto-1.4.11 $ ifconfig
eth0      Link encap:Ethernet  HWaddr b8:27:eb:3b:62:54
          inet addr:129.63.17.153  Bcast:129.63.152.255  Mask:255.255.255.0
          inet6 addr: fe80::1b99:bae0:5fa2:c381/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:13337 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1976 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:16657709 (15.8 MiB)  TX bytes:183392 (179.0 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:200 errors:0 dropped:0 overruns:0 frame:0
          TX packets:200 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:16656 (16.2 KiB)  TX bytes:16656 (16.2 KiB)

wlan0     Link encap:Ethernet  HWaddr 00:e0:4c:0b:f0:09
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:138 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:960 (960.0 B)  TX bytes:468 (468.0 B)

pi@raspberrypi:/etc/apt/sources.list.d/mosquitto-1.4.11 $
pi@raspberrypi:/etc/apt/sources.list.d/mosquitto-1.4.11 $ mosquitto_sub -h 129.6
3.17.135
Error: You must specify a topic to subscribe to.

Use 'mosquitto_sub --help' to see usage.
pi@raspberrypi:/etc/apt/sources.list.d/mosquitto-1.4.11 $ mosquitto_sub -h 129.63.17.135 -t test
omkar
```



```
Client mosqpub/1413-raspberryp sending PUBLISH (d0, q0, r0, m1, 'test', ... (7 bytes))
Client mosqpub/1413-raspberryp sending DISCONNECT
pi@raspberrypi:~ $
pi@raspberrypi:~ $ mosquitto_pub -d -t test -m "message"
Client mosqpub/1414-raspberryp sending CONNECT
Client mosqpub/1414-raspberryp received CONNACK
Client mosqpub/1414-raspberryp sending PUBLISH (d0, q0, r0, m1, 'test', ... (7 bytes))
Client mosqpub/1414-raspberryp sending DISCONNECT
pi@raspberrypi:~ $ mosquitto_pub -d -t test -m "message"
Client mosqpub/1415-raspberryp sending CONNECT
Client mosqpub/1415-raspberryp received CONNACK
Client mosqpub/1415-raspberryp sending PUBLISH (d0, q0, r0, m1, 'test', ... (7 bytes))
Client mosqpub/1415-raspberryp sending DISCONNECT
pi@raspberrypi:~ $ mosquitto_pub -d -t test -m "message"
Client mosqpub/1416-raspberryp sending CONNECT
Client mosqpub/1416-raspberryp received CONNACK
Client mosqpub/1416-raspberryp sending PUBLISH (d0, q0, r0, m1, 'test', ... (7 bytes))
Client mosqpub/1416-raspberryp sending DISCONNECT
pi@raspberrypi:~ $ mosquitto_pub -d -t test -m "test"
Client mosqpub/1417-raspberryp sending CONNECT
Client mosqpub/1417-raspberryp received CONNACK
Client mosqpub/1417-raspberryp sending PUBLISH (d0, q0, r0, m1, 'test', ... (4 bytes))
Client mosqpub/1417-raspberryp sending DISCONNECT
pi@raspberrypi:~ $
```



```
pi@raspberrypi:~ $ mosquitto_sub -d -t test
Client mosqsub/1139-raspberryp sending CONNECT
Client mosqsub/1139-raspberryp received CONNACK
Client mosqsub/1139-raspberryp sending SUBSCRIBE (Mid: 1, Topic: test, QoS: 0)
Client mosqsub/1139-raspberryp received SUBACK
Subscribed (mid: 1): 0
Client mosqsub/1139-raspberryp received PUBLISH (d0, q0, r0, m0, 'test', ... (7
bytes))
message
Client mosqsub/1139-raspberryp sending PINGREQ
Client mosqsub/1139-raspberryp received PINGRESP
Client mosqsub/1139-raspberryp sending PINGREQ
Client mosqsub/1139-raspberryp received PINGRESP
Client mosqsub/1139-raspberryp sending PINGREQ
Client mosqsub/1139-raspberryp received PINGRESP
Client mosqsub/1139-raspberryp sending PINGREQ
Client mosqsub/1139-raspberryp received PINGRESP
Client mosqsub/1139-raspberryp sending PINGREQ
Client mosqsub/1139-raspberryp received PINGRESP
Client mosqsub/1139-raspberryp sending PINGREQ
Client mosqsub/1139-raspberryp received PINGRESP
Client mosqsub/1139-raspberryp sending PINGREQ
Client mosqsub/1139-raspberryp received PINGRESP
Client mosqsub/1139-raspberryp sending PINGREQ
Client mosqsub/1139-raspberryp received PINGRESP
Client mosqsub/1139-raspberryp received PUBLISH (d0, q0, r0, m0, 'test', ... (7
bytes))
message
Client mosqsub/1139-raspberryp received PUBLISH (d0, q0, r0, m0, 'test', ... (7
bytes))
message
Client mosqsub/1139-raspberryp received PUBLISH (d0, q0, r0, m0, 'test', ... (7
bytes))
message
Client mosqsub/1139-raspberryp received PUBLISH (d0, q0, r0, m0, 'test', ... (7
bytes))
message
Client mosqsub/1139-raspberryp received PUBLISH (d0, q0, r0, m0, 'test', ... (7
bytes))
message
Client mosqsub/1139-raspberryp received PUBLISH (d0, q0, r0, m0, 'test', ... (4
bytes))
test
Client mosqsub/1139-raspberryp sending PINGREQ
Client mosqsub/1139-raspberryp received PINGRESP
```

2. **Set up the mosquitto broker with SSL/TLS transport security. Please refer to [6][7][8]. Test the setup. Document the setup procedure and test results, including all the commands.**

Solution:

We will be using successful client server model created in first question. Initially, we will update some libraries

sudo apt-get update
sudo apt-get install pkg-config cmake openssl libc-ares-dev libssl-dev python-mosquitto

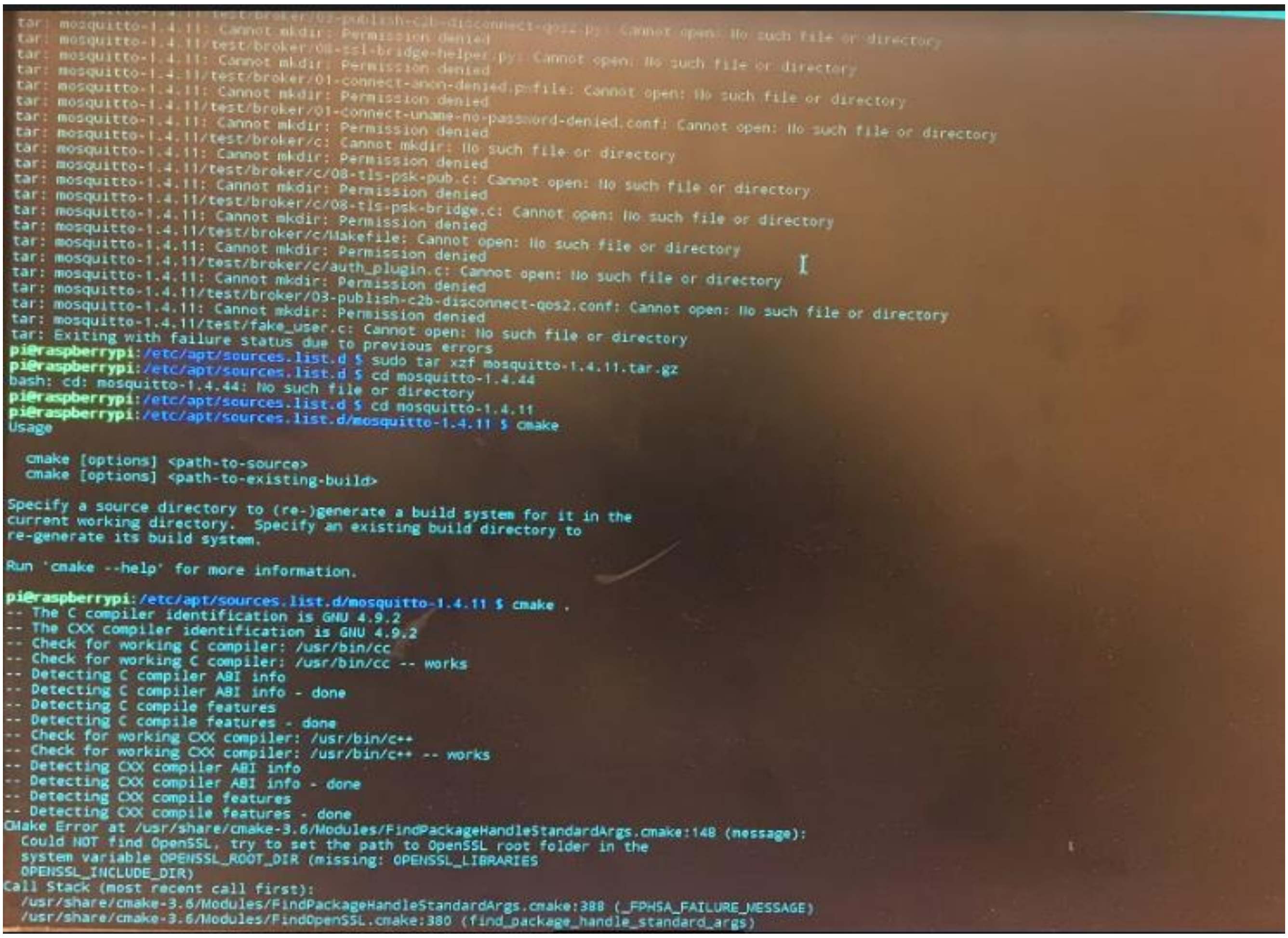
sudo wget http://mosquitto.org/files/source/mosquitto-1.4.11.tar.gz
sudo tar xzf mosquitto-1.4.11.tar.gz
cd mosquitto-1.4.11
sudo cmake .
make install

A. **To use the new repository you should first import the repository package signing key**:
sudo wget http://repo.mosquitto.org/debian/mosquitto-repo.gpg.key
sudo apt-key add mosquitto-repo.gpg.key

Then make the repository available to apt:
sudo cd /etc/apt/sources.list.d/

B. **Then one of the following, depending on which version of debian you are using:**
sudo wget http://repo.mosquitto.org/debian/mosquitto-wheezy.list
sudo wget http://repo.mosquitto.org/debian/mosquitto-jessie.list

Then update apt information:
sudo apt-get update
And discover what mosquitto packages are available:
sudo apt-cache search mosquitto
Or just install:
sudo apt-get install mosquitto

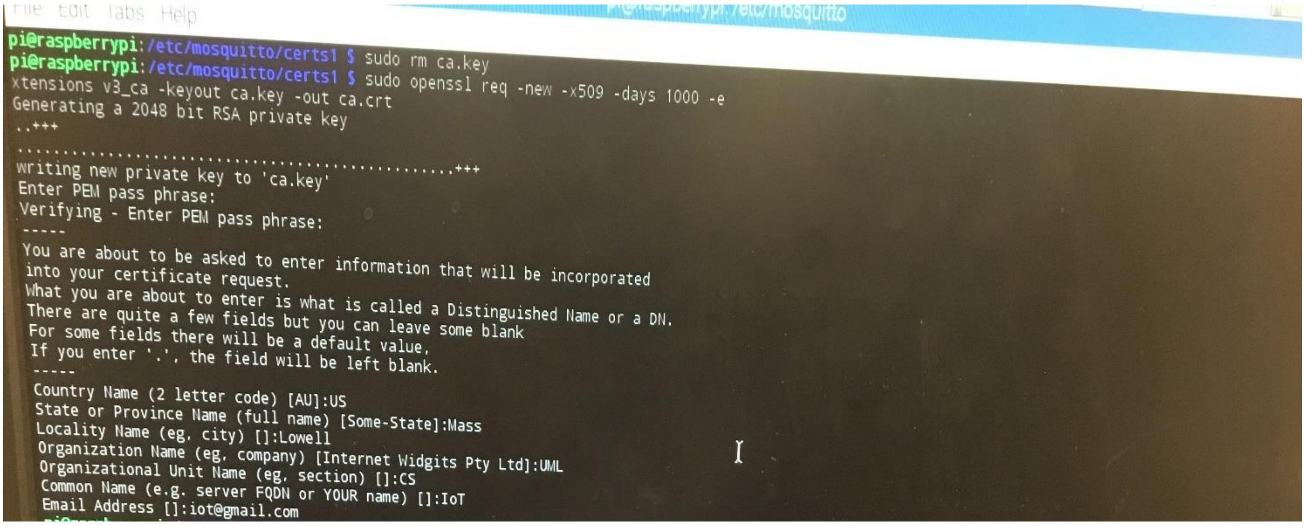


```
tar: mosquitto-1.4.11/test/broker/02-publish-c2b-disconnect-qos2.py: Cannot open: No such file or directory
tar: mosquitto-1.4.11: Cannot mkdir: Permission denied
tar: mosquitto-1.4.11/test/broker/08-ssl-bridge-helper.py: Cannot open: No such file or directory
tar: mosquitto-1.4.11: Cannot mkdir: Permission denied
tar: mosquitto-1.4.11/test/broker/01-connect-anon-denied.pwfile: Cannot open: No such file or directory
tar: mosquitto-1.4.11: Cannot mkdir: Permission denied
tar: mosquitto-1.4.11/test/broker/01-connect-uname-no-password-denied.conf: Cannot open: No such file or directory
tar: mosquitto-1.4.11: Cannot mkdir: Permission denied
tar: mosquitto-1.4.11/test/broker/c: Cannot mkdir: No such file or directory
tar: mosquitto-1.4.11: Cannot mkdir: Permission denied
tar: mosquitto-1.4.11/test/broker/c/08-tls-psk-pub.c: Cannot open: No such file or directory
tar: mosquitto-1.4.11: Cannot mkdir: Permission denied
tar: mosquitto-1.4.11/test/broker/c/08-tls-psk-bridge.c: Cannot open: No such file or directory
tar: mosquitto-1.4.11: Cannot mkdir: Permission denied
tar: mosquitto-1.4.11/test/broker/c/Makefile: Cannot open: No such file or directory
tar: mosquitto-1.4.11: Cannot mkdir: Permission denied
tar: mosquitto-1.4.11/test/broker/c/auth_plugin.c: Cannot open: No such file or directory
tar: mosquitto-1.4.11: Cannot mkdir: Permission denied
tar: mosquitto-1.4.11/test/broker/03-publish-c2b-disconnect-qos2.conf: Cannot open: No such file or directory
tar: mosquitto-1.4.11: Cannot mkdir: Permission denied
tar: mosquitto-1.4.11/test/fake_user.c: Cannot open: No such file or directory
tar: Exiting with failure status due to previous errors
pi@raspberrypi:/etc/apt/sources.list.d $ sudo tar xzf mosquitto-1.4.11.tar.gz
pi@raspberrypi:/etc/apt/sources.list.d $ cd mosquitto-1.4.44
bash: cd: mosquitto-1.4.44: No such file or directory
pi@raspberrypi:/etc/apt/sources.list.d $ cd mosquitto-1.4.11
pi@raspberrypi:/etc/apt/sources.list.d/mosquitto-1.4.11 $ cmake
Usage

  cmake [options] <path-to-source>
  cmake [options] <path-to-existing-build>

Specify a source directory to (re-)generate a build system for it in the
current working directory.  Specify an existing build directory to
re-generate its build system.

Run 'cmake --help' for more information.

pi@raspberrypi:/etc/apt/sources.list.d/mosquitto-1.4.11 $ cmake .
-- The C compiler identification is GNU 4.9.2
-- The CXX compiler identification is GNU 4.9.2
-- Check for working C compiler: /usr/bin/cc
-- Check for working C compiler: /usr/bin/cc -- works
-- Detecting C compiler ABI info
-- Detecting C compiler ABI info - done
-- Detecting C compile features
-- Detecting C compile features - done
-- Check for working CXX compiler: /usr/bin/c++
-- Check for working CXX compiler: /usr/bin/c++ -- works
-- Detecting CXX compiler ABI info
-- Detecting CXX compiler ABI info - done
-- Detecting CXX compile features
-- Detecting CXX compile features - done
CMake Error at /usr/share/cmake-3.6/Modules/FindPackageHandleStandardArgs.cmake:148 (message):
  Could NOT find OpenSSL, try to set the path to OpenSSL root folder in the
  system variable OPENSSL_ROOT_DIR (missing: OPENSSL_LIBRARIES
  OPENSSL_INCLUDE_DIR)
Call Stack (most recent call first):
  /usr/share/cmake-3.6/Modules/FindPackageHandleStandardArgs.cmake:388 (_FPHSA_FAILURE_MESSAGE)
  /usr/share/cmake-3.6/Modules/FindOpenSSL.cmake:380 (find_package_handle_standard_args)
```

D. Next step is to Setup a CA (certificate authority) this will create a certificate authority certificate and key. Then the server certificate and key by creating the following files server.key, server.csr, server.crt and then send the CSR to the CA by creating these set of files ca.crt ca.key ca.srl. The commands to create the certificates are as below.

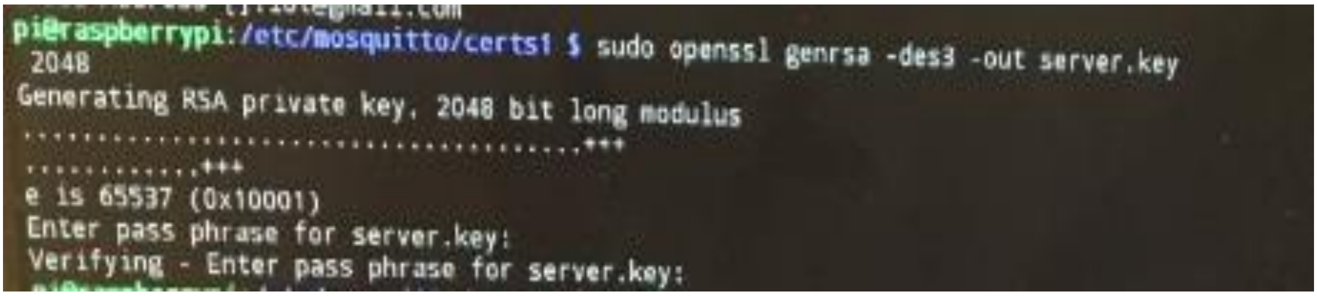
OpenSSL commands to create the certificates are:

- *Sudo openssl req -new -x509 -days 1000 -extensions v3_ca -keyout ca.key -out ca.crt*



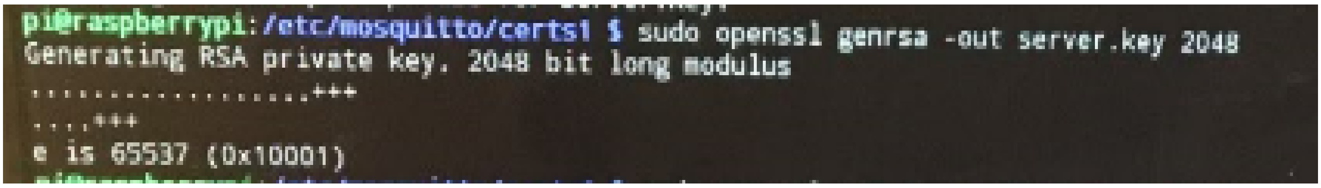
```
pi@raspberrypi:/etc/mosquitto/certs1 $ sudo rm ca.key
pi@raspberrypi:/etc/mosquitto/certs1 $ sudo openssl req -new -x509 -days 1000 -e
xtensions v3_ca -keyout ca.key -out ca.crt
Generating a 2048 bit RSA private key
..+++
..............................................+++
writing new private key to 'ca.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:Mass
Locality Name (eg, city) []:Lowell
Organization Name (eg, company) [Internet Widgits Pty Ltd]:UML
Organizational Unit Name (eg, section) []:CS
Common Name (e.g. server FQDN or YOUR name) []:IoT
Email Address []:iot@gmail.com
```

- *Sudo openssl genrsa -des3 -out server.key 2048*



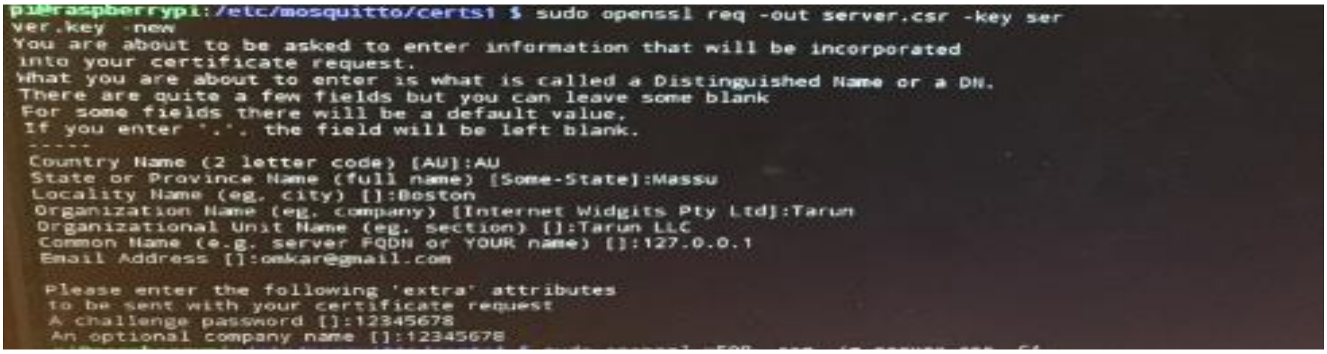
```
pi@raspberrypi:/etc/mosquitto/certs1 $ sudo openssl genrsa -des3 -out server.key
 2048
Generating RSA private key, 2048 bit long modulus
........................................+++
............+++
e is 65537 (0x10001)
Enter pass phrase for server.key:
Verifying - Enter pass phrase for server.key:
```

- *Sudo openssl genrsa -out server.key 2048*



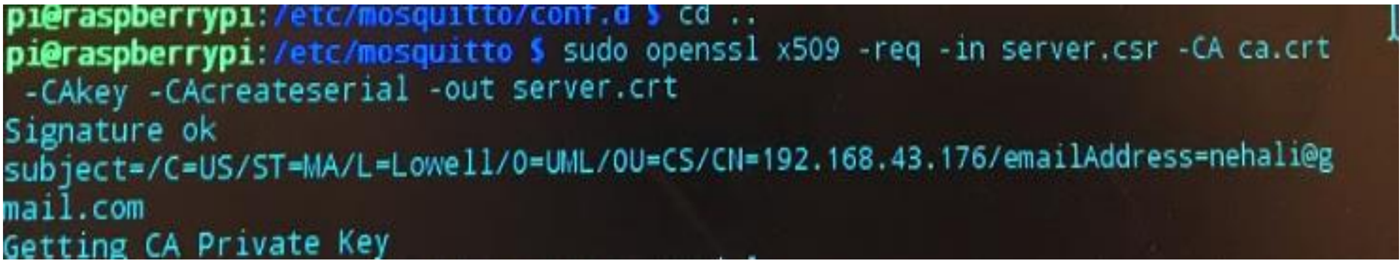
```
pi@raspberrypi:/etc/mosquitto/certs1 $ sudo openssl genrsa -out server.key 2048
Generating RSA private key, 2048 bit long modulus
..................+++
....+++
e is 65537 (0x10001)
```

- *Sudo openssl req -out server.csr -key server.key –new*



```
pi@raspberrypi:/etc/mosquitto/certs1 $ sudo openssl req -out server.csr -key ser
ver.key -new
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:AU
State or Province Name (full name) [Some-State]:Massu
Locality Name (eg, city) []:Boston
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Tarun
Organizational Unit Name (eg, section) []:Tarun LLC
Common Name (e.g. server FQDN or YOUR name) []:127.0.0.1
Email Address []:omkar@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:12345678
An optional company name []:12345678
```

- *Sudo openssl x509 -req -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt*



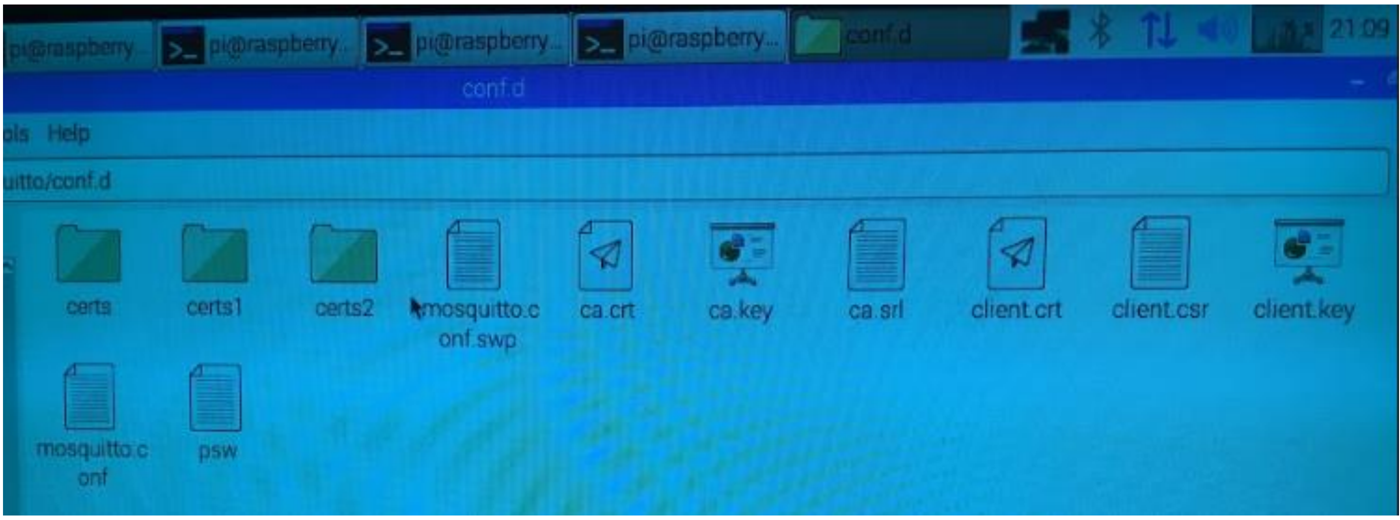
```
pi@raspberrypi:/etc/mosquitto/conf.d $ cd ..
pi@raspberrypi:/etc/mosquitto $ sudo openssl x509 -req -in server.csr -CA ca.crt
 -CAkey -CAcreateserial -out server.crt
Signature ok
subject=/C=US/ST=MA/L=Lowell/O=UML/OU=CS/CN=192.168.43.176/emailAddress=nehali@g
mail.com
Getting CA Private Key
```

3. **Set up the certificate based authentication between each client and the broker while using the mosquitto broker with SSL/TLS transport security. Test the setup. Document the setup procedure and test results, including all the commands. (3 points)**

Solution:

We have setup SSL for our client server in question 2. We will be using same configuration for message transportation

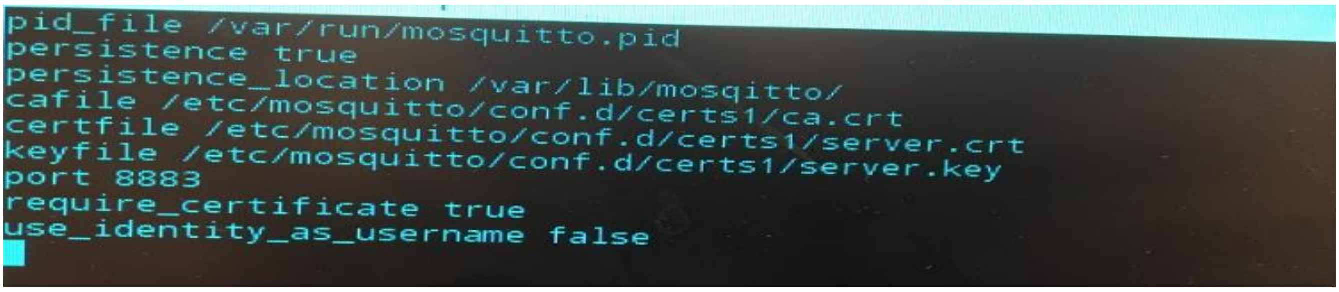
Client and server certificate created



We need to move all certificates to following locations for each machine i.e. server and client

/etc/mosquitto/conf.d/certs

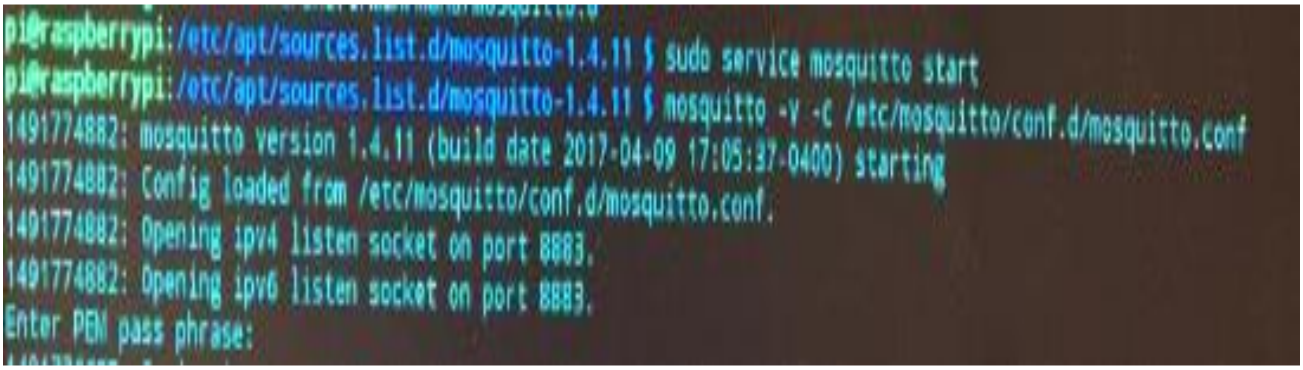
All these changes need to be reflected in */etc/mosquitto/conf.d/mosquitto.conf*



```
pid_file /var/run/mosquitto.pid
persistence true
persistence_location /var/lib/mosqitto/
cafile /etc/mosquitto/conf.d/certs1/ca.crt
certfile /etc/mosquitto/conf.d/certs1/server.crt
keyfile /etc/mosquitto/conf.d/certs1/server.key
port 8883
require_certificate true
use_identity_as_username false
```

Once these changes are made we need to start the service as below on 8883 port:

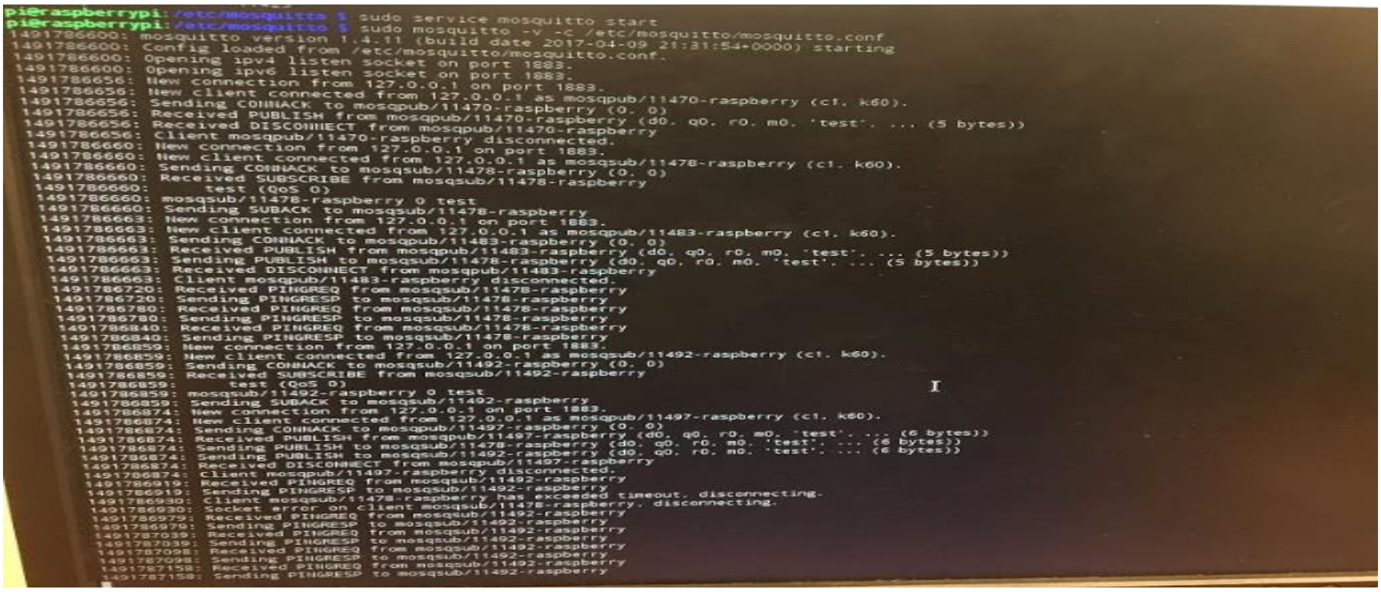
sudo service mosquitto start
sudo mosquittto –v –c /etc/mosquitto/conf.d/mosquitto.conf



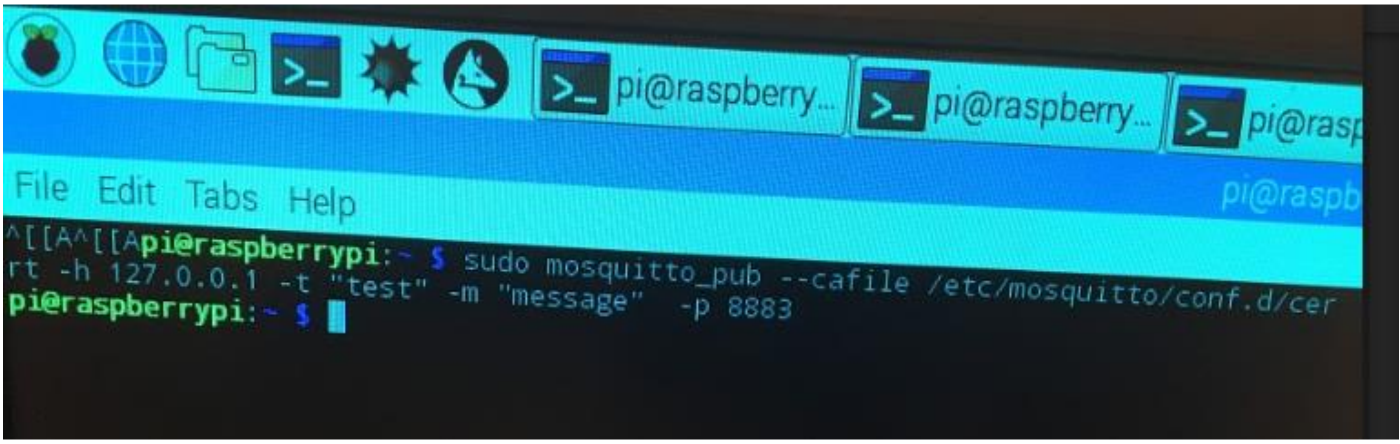
```
pi@raspberrypi:/etc/apt/sources.list.d/mosquitto-1.4.11 $ sudo service mosquitto start
pi@raspberrypi:/etc/apt/sources.list.d/mosquitto-1.4.11 $ mosquitto -v -c /etc/mosquitto/conf.d/mosquitto.conf
1491774882: mosquitto version 1.4.11 (build date 2017-04-09 17:05:37-0400) starting
1491774882: Config loaded from /etc/mosquitto/conf.d/mosquitto.conf.
1491774882: Opening ipv4 listen socket on port 8883.
1491774882: Opening ipv6 listen socket on port 8883.
Enter PEM pass phrase:
```

Command for server setup:

mosquitto_pub –cafile /etc/mosquitto.conf.d/certs1/ca.crt –h 127.0.0.1 –t “test” -m message –p 8883



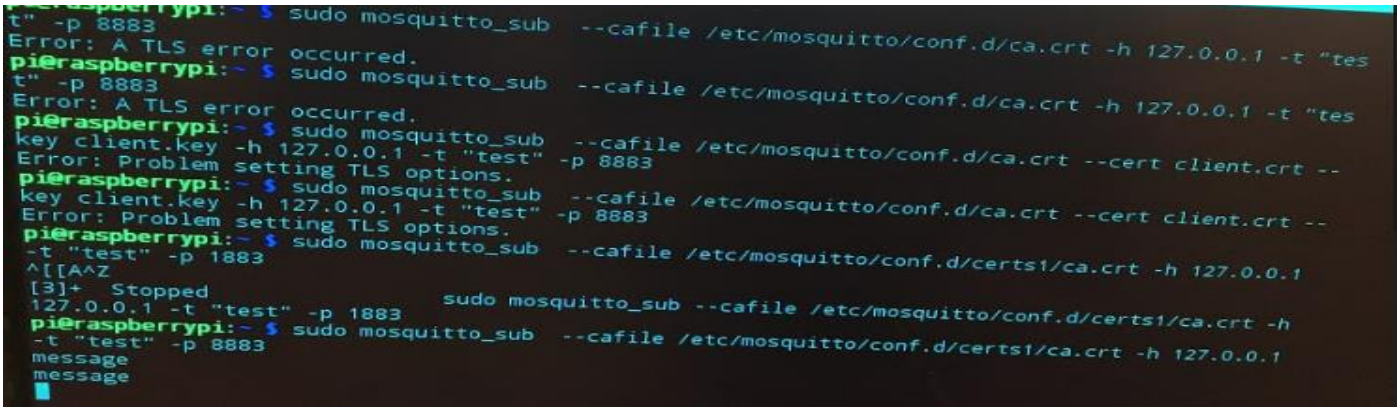
```
pi@raspberrypi:/etc/mosquitto $ sudo service mosquitto start
pi@raspberrypi:/etc/mosquitto $ sudo mosquitto -v -c /etc/mosquitto/mosquitto.conf
1491786600: mosquitto version 1.4.11 (build date 2017-04-09 21:31:54+0000) starting
1491786600: Config loaded from /etc/mosquitto/mosquitto.conf.
1491786600: Opening ipv4 listen socket on port 1883.
1491786600: Opening ipv6 listen socket on port 1883.
1491786656: New connection from 127.0.0.1 on port 1883.
1491786656: New client connected from 127.0.0.1 as mosqpub/11470-raspberry (c1, k60).
1491786656: Sending CONNACK to mosqpub/11470-raspberry (0, 0)
1491786656: Received PUBLISH from mosqpub/11470-raspberry (d0, q0, r0, m0, 'test', ... (5 bytes))
1491786656: Received DISCONNECT from mosqpub/11470-raspberry
1491786656: Client mosqpub/11470-raspberry disconnected.
1491786660: New connection from 127.0.0.1 on port 1883.
1491786660: New client connected from 127.0.0.1 as mosqsub/11478-raspberry (c1, k60).
1491786660: Sending CONNACK to mosqsub/11478-raspberry (0, 0)
1491786660: Received SUBSCRIBE from mosqsub/11478-raspberry
1491786660:     test (QoS 0)
1491786660: mosqsub/11478-raspberry 0 test
1491786660: Sending SUBACK to mosqsub/11478-raspberry
1491786663: New connection from 127.0.0.1 on port 1883.
1491786663: New client connected from 127.0.0.1 as mosqpub/11483-raspberry (c1, k60).
1491786663: Sending CONNACK to mosqpub/11483-raspberry (0, 0)
1491786663: Received PUBLISH from mosqpub/11483-raspberry (d0, q0, r0, m0, 'test', ... (5 bytes))
1491786663: Sending PUBLISH to mosqsub/11478-raspberry (d0, q0, r0, m0, 'test', ... (5 bytes))
1491786663: Received DISCONNECT from mosqpub/11483-raspberry
1491786663: Client mosqpub/11483-raspberry disconnected.
1491786720: Received PINGREQ from mosqsub/11478-raspberry
1491786720: Sending PINGRESP to mosqsub/11478-raspberry
1491786780: Received PINGREQ from mosqsub/11478-raspberry
1491786780: Sending PINGRESP to mosqsub/11478-raspberry
1491786840: Received PINGREQ from mosqsub/11478-raspberry
1491786840: Sending PINGRESP to mosqsub/11478-raspberry
1491786859: New connection from 127.0.0.1 on port 1883.
1491786859: New client connected from 127.0.0.1 as mosqsub/11492-raspberry (c1, k60).
1491786859: Sending CONNACK to mosqsub/11492-raspberry (0, 0)
1491786859: Received SUBSCRIBE from mosqsub/11492-raspberry
1491786859:     test (QoS 0)
1491786859: mosqsub/11492-raspberry 0 test
1491786859: Sending SUBACK to mosqsub/11492-raspberry
1491786874: New connection from 127.0.0.1 on port 1883.
1491786874: New client connected from 127.0.0.1 as mosqpub/11497-raspberry (c1, k60).
1491786874: Sending CONNACK to mosqpub/11497-raspberry (0, 0)
1491786874: Received PUBLISH from mosqpub/11497-raspberry (d0, q0, r0, m0, 'test', ... (6 bytes))
1491786874: Sending PUBLISH to mosqsub/11478-raspberry (d0, q0, r0, m0, 'test', ... (6 bytes))
1491786874: Sending PUBLISH to mosqsub/11492-raspberry (d0, q0, r0, m0, 'test', ... (6 bytes))
1491786874: Received DISCONNECT from mosqpub/11497-raspberry
1491786874: Client mosqpub/11497-raspberry disconnected.
1491786919: Received PINGREQ from mosqsub/11492-raspberry
1491786919: Sending PINGRESP to mosqsub/11492-raspberry
1491786930: Client mosqsub/11478-raspberry has exceeded timeout, disconnecting.
1491786930: Socket error on client mosqsub/11478-raspberry, disconnecting.
1491786979: Received PINGREQ from mosqsub/11492-raspberry
1491786979: Sending PINGRESP to mosqsub/11492-raspberry
1491787039: Received PINGREQ from mosqsub/11492-raspberry
1491787039: Sending PINGRESP to mosqsub/11492-raspberry
1491787098: Received PINGREQ from mosqsub/11492-raspberry
1491787098: Sending PINGRESP to mosqsub/11492-raspberry
1491787158: Received PINGREQ from mosqsub/11492-raspberry
1491787158: Sending PINGRESP to mosqsub/11492-raspberry
```



```
^[[A^[[Api@raspberrypi:~ $ sudo mosquitto_pub --cafile /etc/mosquitto/conf.d/cer
rt -h 127.0.0.1 -t "test" -m "message"  -p 8883
pi@raspberrypi:~ $
```

This will setup server on this terminal, for client we need to open new terminal and execute following command:

mosquitto_sub –cafile /etc/mosquitto.conf.d/certs1/ca.crt –h 127.0.0.1 –t “test” –p 8883



```
pi@raspberrypi:~ $ sudo mosquitto_sub  --cafile /etc/mosquitto/conf.d/ca.crt -h 127.0.0.1 -t "tes
t" -p 8883
Error: A TLS error occurred.
pi@raspberrypi:~ $ sudo mosquitto_sub  --cafile /etc/mosquitto/conf.d/ca.crt -h 127.0.0.1 -t "tes
t" -p 8883
Error: A TLS error occurred.
pi@raspberrypi:~ $ sudo mosquitto_sub  --cafile /etc/mosquitto/conf.d/ca.crt --cert client.crt --
key client.key -h 127.0.0.1 -t "test" -p 8883
Error: Problem setting TLS options.
pi@raspberrypi:~ $ sudo mosquitto_sub  --cafile /etc/mosquitto/conf.d/ca.crt --cert client.crt --
key client.key -h 127.0.0.1 -t "test" -p 8883
Error: Problem setting TLS options.
pi@raspberrypi:~ $ sudo mosquitto_sub  --cafile /etc/mosquitto/conf.d/certs1/ca.crt -h 127.0.0.1
-t "test" -p 1883
^[[A^Z
[3]+  Stopped                 sudo mosquitto_sub --cafile /etc/mosquitto/conf.d/certs1/ca.crt -h
127.0.0.1 -t "test" -p 1883
pi@raspberrypi:~ $ sudo mosquitto_sub  --cafile /etc/mosquitto/conf.d/certs1/ca.crt -h 127.0.0.1
-t "test" -p 8883
message
message
```

Hence, we have successfully implemented client server model on two separate terminal using SSL/TSL.

References

[1] Mosquitto, An Open Source MQTT v3.1/v3.1.1 Broker, Documentation, 2016

[2] Python Software Foundation, paho-mqtt 1.2, 2016

[3] mosquitto.conf — the configuration file for mosquitto, 2016

[4] James Lewis, MQTT Introduction and Tutorial Part One - Message Brokers and why your IoT device should use them, February 17, 2016.

[5] James Lewis, MQTT Tutorial for Raspberry Pi, Arduino, and ESP8266 - Send MQTT messages between 3 different platforms, February 24, 2016

[6] Primal Cortex, MQTT Mosquitto broker with SSL/TLS transport security, March 31, 2016

[7] J. Dunmire, SSL/TLS Client Certs to Secure MQTT, 2016

[8] HuyITF, Configure SSL/TLS for MQTT broker mosquitto, Jun 2, 2016