## TCP Server

### Description

This use case is to demonstrate creating TCP server socket and TCP data communication over the created socket.

### Prerequisites

1. Access Point configured with WPA/WPA2 personal security.
2. Hercules tool to create TCP client in Windows laptop.

### AT Command Sequence

|  |  |
| --- | --- |
| **AT Command** | **Description** |
| *at* | Check communication state |
| *at+wscan* | Get list of available APs from the vicinity |
| *at+wcon* | Connect to a desired AP from the received scan results |
| *at+wstatus* | Get IP address of Talaria TWO to verify the connection(L2+L3) is successful |
| *at+socsrv* | Start TCP server |
| *at+socsend* | Send data |

Table 14: TCP Server - AT Commands

### Procedure

**Step 1**: Execute the following commands on Talaria TWO:

|  |
| --- |
| at  at+wscan  at+wcon=InnoPhase,Inno@9070  at+wstatus=0  at+socsrv=0,0,0,9000 |

Text

Description automatically generated

Figure 46: TCP Server – Serial log

**Step 2**: Connect your laptop to the same access point “InnoPhase” to which the Talaria TWO is connected.

Graphical user interface, text

Description automatically generated

Figure 47: Connecting to AP

**Step 3**: Start TCP client using Hercules and connect to Talaria TWO TCP server.

Graphical user interface, text, application, email

Description automatically generated

Figure 48: Starting TCP client

**Step 4**: Log for data communication between application endpoints.

**Note**: Send data from Talaria TWO using command at+socsend=1,ASCII,5,Hello.

Graphical user interface, text, application, chat or text message

Description automatically generated

Figure 49: Log for data communication between application endpoints – Tera Term

Graphical user interface, text, application, chat or text message

Description automatically generated

Figure 50: Log for data communication between application endpoints - Hercules

## TCP Client

### Description

This use case is to demonstrate creating TCP client socket and TCP data communication over the created socket.

### Prerequisites

1. Access Point configured with WPA/WPA2 personal security.
2. Any network tool (Hercules tool in this example) to be used to create TCP server in Windows/Linux laptop.

### AT Command Sequence

|  |  |
| --- | --- |
| **AT Command** | **Description** |
| *at* | Check communication state |
| *at+wscan* | Get list of available APs from the vicinity |
| *at+wcon* | Connect to a desired AP from the received scan results |
| *at+wstatus* | Get IP address of Talaria TWO to verify the connection(L2+L3) is successful |
| *at+soccli* | Create TCP client socket |
| *at+socsend* | Send data |

Table 15: TCP Client - AT Commands

### Procedure

**Step 1**: Connect your laptop to the same access point “InnoPhase” to which the Talaria TWO is connected.

Graphical user interface, text

Description automatically generated

Figure 51: Connecting to AP

**Step 2**: Using Hercules tool create TCP server socket.

Graphical user interface, application

Description automatically generated

Figure 52: Creating TCP server socket

**Step 3**: Get IP address of the server/laptop using the command ipconfig.

Text

Description automatically generated

Figure 53: Getting the IP address

**Step 4**: Execute the following commands on Talaria TWO:

|  |
| --- |
| at  at+wscan  at+wcon=InnoPhase,Inno@9070  at+wstatus=0  at+soccli=0,0,0,8000,192.168.1.5  at+socsend=0,ASCII,12,Hello Server |

**Step 5**: Data communication between the application endpoints.

Graphical user interface, text

Description automatically generated

Figure 54: Data communication – Tera Term

Graphical user interface, text

Description automatically generated

Figure 55: Data communication - Hercules

## UDP Server

### Description

This use case is to demonstrate creating UDP server socket and UDP data communication over the created socket.

### Prerequisites

1. Access Point configured with WPA/WPA2 personal security.
2. Hercules tool to create UDP client in Windows laptop.

### AT Command Sequence

|  |  |
| --- | --- |
| **AT Command** | **Description** |
| *at* | Check communication state |
| *at+wscan* | Get list of available APs from the vicinity |
| *at+wcon* | Connect to a desired AP from the received scan results |
| *at+wstatus* | Get IP address of Talaria TWO to verify the connection(L2+L3) is successful |
| *at+socsrv* | Start UDP server |
| *at+soccli* | Start UDP client |
| *at+socsend* | Send data |

Table 16: UDP Server - AT Commands

### Procedure

**Step 1**: Connect your laptop to the same access point InnoPhase to which the Talaria TWO is connected.



Figure 56: Connecting to AP

**Step 2**: Start UDP client using Hercules and connect to Talaria TWO UDP server of IP address 192.168.1.2 and port 9000.

Graphical user interface, text, application, email

Description automatically generated

Figure 57: Starting UDP Client

**Step 3**: Get IP address of the server/laptop using the command ipconfig.

Text

Description automatically generated

Figure 58: ipconfig output

**Step 4**: Execute the following commands to associate to an Access Point. Start the UDP server. Start the UDP client.

UDP server socket can only receive data, hence a client socket should be created if data needs to be sent.

|  |
| --- |
| at  at+wscan  at+wcon=InnoPhase,Inno@9070 at+wstatus=0  at+socsrv=0,1,1,9000  at+soccli=0,1,1,9000,192.168.1.6  at+socsend=1,ASCII,5,HELLO |

**Step 5**: Data communication between two application endpoints.

Text

Description automatically generated

Figure 59: Data communication – Tera Term

Graphical user interface, text, application, email

Description automatically generated

Figure 60: Data communication - Hercules

## UDP Client

### Description

This use case is to demonstrate creating TCP client socket and TCP data communication over the created socket.

### Prerequisites

1. Access Point configured with WPA/WPA2 personal security.
2. Any network tool (Hercules tool in this example) to be used to create UDP server in Windows/Linux laptop.

### AT Command Sequence

|  |  |
| --- | --- |
| **AT Command** | **Description** |
| *at* | Check communication state |
| *at+wscan* | Get list of available APs from the vicinity |
| *at+wcon* | Connect to a desired AP from the received scan results |
| *at+wstatus* | Get IP address of T2 to verify the connection(L2+L3) is successful |
| *at+soccli* | Create UDP client socket |
| *at+socsend* | Send data |

Table 17: UDP Client – AT Commands

### Procedure

**Step 1**: Connect your laptop to the same access point “InnoPhase” to which the Talaria TWO is connected.

Graphical user interface, text

Description automatically generated

Figure 61: Connecting to AP

**Step 2**: Using Hercules tool create UDP socket.

Graphical user interface, text, application, email

Description automatically generated

Figure 62: Creating TCP server socket

**Step 3**: Get IP address of the server/laptop using the command ipconfig.

Text

Description automatically generated

Figure 63: Getting the IP address

**Step 4**: Execute the following commands on Talaria TWO:

|  |
| --- |
| at  at+wscan  at+wcon=InnoPhase,Inno@9070  at+wstatus=0  at+soccli=0,1,1,8000,192.168.1.6  at+socsend=0,ASCII,12,Hi InnoPhase |

**Step 5**: Data communication between the application endpoints.

Graphical user interface, text, application

Description automatically generated

Figure 64: Data communication – Tera Term

Graphical user interface, text, application

Description automatically generated

Figure 65: Data communication – Hercules

## HTTP Client

### Non-Secured HTTP Client

#### Description

This use case is to demonstrate HTTP client and perform GET/POST operations.

#### Prerequisites

1. Access Point configured with WPA/WPA2 personal security.
2. HFS tool to start local HTTP server.

#### AT Command Sequence

|  |  |
| --- | --- |
| **AT Command** | **Description** |
| *at* | Check communication state |
| *at+wscan* | Get list of available APs from the vicinity |
| *at+wcon* | Connect to a desired AP from the received scan results |
| *at+wstatus* | Get IP address of Talaria TWO to verify the connection(L2+L3) is successful |
| *at+hchdrset* | Set HTTP client header |
| *at+hcstart* | Start HTTP Client |
| *at+hcreqsnd* | Send GET request from the HTTP client |

Table 18: HTTP Client (non-secured) - AT Commands

#### Procedure

**Step 1**: Connect your laptop to the same access point “InnoPhase” to which the Talaria TWO is connected.

Graphical user interface, text

Description automatically generated

Figure 66: Connecting to AP

**Step 2**: Start HFS server and add data.txt file into the data path, as shown in Figure 67.

Graphical user interface, text, table

Description automatically generated

Figure 67: Starting HFS server

**Step 3**: Execute the following commands on Talaria TWO:

|  |
| --- |
| at  at+wscan  at+wcon=InnoPhase,Inno@9070  at+wstatus=0  at+hchdrset=13,192.168.1.5  at+hcstart=192.168.1.5,80  at+hcreqsnd=0,1,/data.txt |

#### Serial Log

Text

Description automatically generated

Figure 68: HTTP Client (non-secured) - Serial Log

### Secured HTTP Client without Server Certificate Validation

#### Description

This use case is to demonstrate secured HTTP client connection without server certificate validation (time validation).

#### Prerequisites

1. Access Point configured with WPA/WPA2 personal security.
2. HTTPs server.

#### AT Command Sequence

|  |  |
| --- | --- |
| **AT Command** | **Description** |
| *at* | Check communication state |
| *at+wscan* | Get list of available APs from the vicinity |
| *at+wcon* | Connect to a desired AP from the received scan results |
| *at+wstatus* | Get IP address of Talaria TWO to verify the connection(L2+L3) is successful |
| *at+hcstart* | Start HTTP Client |
| *at+hcclose* | Close HTTP connection |

Table 19: HTTP Client (secured without server certificate validation) - AT Commands

#### Procedure

**Step 1:** Ensure that the server is running before triggering connection from Talaria TWO**.** In this example, httpbin.org server is used for connecting to the secure port.

**Step 2:** Execute the following commands on Talaria TWO:

|  |
| --- |
| at  at+wscan  at+wcon=InnoPhase,Inno@9070  at+wstatus=0  at+hcstart=httpbin.org,443,1  at+hcclose=0 |

#### Serial Log

Text

Description automatically generated

Figure 69: HTTP Client (secured without server certificate validation) - Serial log

### Secured HTTP Client (with Server Certificate Validation)

#### Description

This use case is to demonstrate secured HTTP client connection with server certificate validation (load CA certificate).

#### Prerequisites

1. Access Point configured with WPA/WPA2 personal security.
2. HTTPs server.

#### AT Command Sequence

|  |  |
| --- | --- |
| **AT Command** | **Description** |
| *at* | Check communication state |
| *at+wscan* | Get list of available APs from the vicinity |
| *at+wcon* | Connect to a desired AP from the received scan results |
| *at+wstatus* | Get IP address of Talaria TWO to verify the connection(L2+L3) is successful |
| *At+certadd* | To load certificate |
| *at+hcstart* | Start HTTP Client |
| *at+hcclose* | Close HTTP connection |

Table 20: HTTP Client (secured with server certificate validation) – AT Commands

#### Procedure

**Step 1:** Ensure that the server is running and ready for any incoming connection, before triggering the HTTP client connection from Talaria TWO**.** In this example, httpbin.org server is used for connecting to the secure port (443).

**Step 2:** Execute the following commands on Talaria TWO:

|  |
| --- |
| at  at+wscan  at+wcon=InnoPhase,Inno@9070  at+wstatus=0  at+certadd=httpbin-org-chain,4754  at+hcstart=httpbin.org,443,2,httpbin-org-chain  at+hcclose=0 |

#### Serial Log

Text

Description automatically generated

Figure 70: HTTP Client (secured with server certificate validation) - Serial log

## MQTT Client

### Description

This use case is to demonstrate MQTT client and data communication using Publish and Subscribe methods.

### Prerequisites

1. Access Point configured with WPA/WPA2 personal security.
2. MQTT.fx tool to start another MQTT client to perform Publish/Subscribe b/w two clients.

### AT Command Sequence

|  |  |
| --- | --- |
| **AT Command** | **Description** |
| *at* | Check communication state |
| *at+wscan* | Get list of available APs from the vicinity |
| *at+wcon* | Connect to a desired AP from the received scan results |
| *at+wstatus* | Get IP address of Talaria TWO to verify the connection(L2+L3) is successful |
| *at+mqttconf* | Set MQTT configurations |
| *at+mqttconn* | Connect to MQTT Broker |
| *at+mqttpub* | Publish the MQTT topic with Payload |
| *at+mqttsub* | Subscribe to the MQTT topic |
| *at+mqttdisconn* | Disconnect MQTT client connection |

Table 21: MQTT Client - AT Commands

### Procedure

**Step 1**: Connect your laptop to the same access point “InnoPhase” to which the Talaria TWO is connected.

Graphical user interface, text

Description automatically generated

Figure 71: Connecting to AP

**Step 2**: Start another MQTT client in the PC using MQTT.fx tool to send data to Talaria TWO using Publish method and receive data sent from Talaria TWO using Subscribe method.

Configure the following settings from MQTT.fx to configure MQTT parameters for the public broker mqtt.eclipseprojects.io.Click on the settings button:

Graphical user interface, text, application, Word

Description automatically generated

Figure 72: MQTT.fx – settings

Graphical user interface, application

Description automatically generated

Figure 73: MQTT.fx - Connection Profile

**Note**: Ensure the client ID is unique to the device.

**Step 3**: Click on Connect and check the green color button for successful connection.

**Step 4**: Click on Subscribe and enter topic as PUBMSG to receive any data sent from Talaria TWO MQTT client.

Graphical user interface, text, application, chat or text message

Description automatically generated

Figure 74: MQTT.fx – Subscribe

**Step 5**: Execute the following commands on Talaria TWO:

|  |
| --- |
| at  at+wscan  at+wcon=InnoPhase,Inno@9070  at+wstatus=0  at+mqttconf=clientid,12345678  at+mqttconf=admin,admin  at+mqttconf=password,xyz  at+mqttconn=mqtt.eclipseprojects.io,1883  at+mqttpub=0,PUBMSG,0,5,Hello  at+mqttsub=0,SUBMSG,0 |

Text

Description automatically generated

Figure 75: MQTT Client - Serial log

**Step 6**: Click on Publish and enter topic as SUBMSG to send the data to Talaria TWO MQTT client.

Graphical user interface, application

Description automatically generated

Figure 76: MQTT.fx – Publish

**Step 7**: Data communication between two application end points.

Graphical user interface, text, application, chat or text message

Description automatically generated

Figure 77: Data communication

## Secure MQTT

### Description

This use case is to demonstrate MQTT client connection over secured layer(SSL/TLS).

### Prerequisites

1. Secure MQTT broker with client certificates- Root CA, Client cert and client private key
2. Mosquito tool for windows

### Procedure

Following are the two methods to load the certificate to the filesystem. Use any one of them to add the certificates:

1. **Using Download tool**: Write the certificates to Talaria TWO’s FLASH using the Download tool.

For more information on writing certificates, refer section: *Show File System Contents -> Write Files* of the document: UG\_Download\_Tool.pdf (*freertos\_sdk\_x.y\pc\_tools\Download\_Tool\doc)*.

**Note**: x and y in freertos\_sdk\_x.y refer to the SDK release version.

1. Using AT Commands: The AT command will load the certificates on to the Talaria TWO’s RAM.
   1. Issue the below commands to load the certificates:

|  |
| --- |
| at+certadd=<cert name>,<cert length> |

* 1. Once the command is issued, Talaria TWO will send “<” as response to the command:

Shape, rectangle

Description automatically generated

Figure 80: Command Validation

* 1. Send the certificate after receiving the command response (<).
  2. Go to File -> Send file… from the Tera Term and browse the certificates

Graphical user interface, application

Description automatically generated

Figure 81: Send Certificate

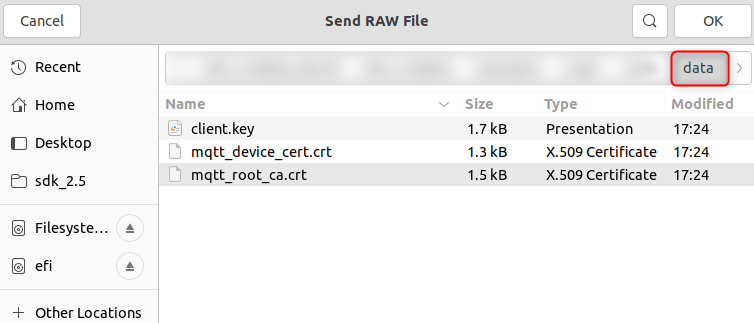


Figure 82: Browse to add the Certificates

* 1. Execute this step to add all three certificates:

Text

Description automatically generated with medium confidence

Figure 83: AT Commands- To add the certificate

|  |
| --- |
| at  at+certadd=mqtt\_root\_ca,1452  at+certadd=mqtt\_device\_cert,1330  at+certadd=client.key,1679 |

### AT Command Sequence

|  |  |
| --- | --- |
| **AT Command** | **Description** |
| *at* | To check the connection state |
| *at+certadd* | To load the certificate |
| *at+wcon* | To connect to a secured access point |
| *at+mqttconf* | Set MQTT configurations |
| *at+mqttconn* | Connect to MQTT broker |
| *at+mqttsub* | Subscribe to a MQTT topic |
| *at+mqttpub* | Publish the MQTT topic with Payload |

Table 22: Secure MQTT - AT Commands

### Procedure

**Step 1**: Execute the following commands on Talaria TWO:

|  |
| --- |
| at+wcon=InnoPhase,43083191  at+mqttconf=clientid,789012  at+mqttconf=username,innophase  at+mqttconf=password,123  at+mqttconf=kainterval,10  at+mqttconn=test.mosquitto.org,8884,1,1,/data/mqtt\_root\_ca.crt,/,/data/mqtt\_device\_cert.crt,/data/client.key  at+mqttsub=0,inno/test,0  at+mqttpub=0,inno/test,0,5,hello |

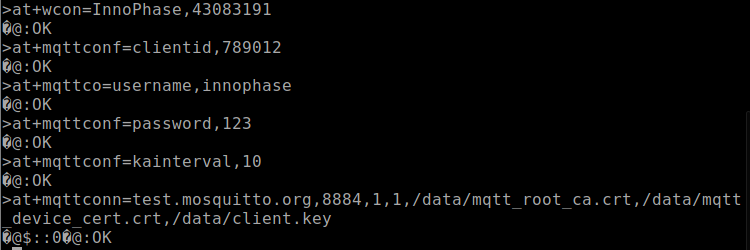


Figure 84: Secure MQTT- serial log

**Step 2**: To observe Publish messages and to Subscribe any message, execute the following commands on the command prompt:

1. To publish:
   1. Start a mosquito server to subscribe to inno/test topic:

|  |
| --- |
| mosquitto\_sub.exe -h test.mosquitto.org -P 8884 -u innophase -P 123 -t inno/test |

Text

Description automatically generated

Figure 85: Command Prompt Output (Publish message)

* 1. Issue the following command to publish message to the subscribed topic from the serial terminal:

|  |
| --- |
| at+mqttpub=0,inno/test,0,5,hello |

Text

Description automatically generated

Figure 86: To publish

1. To subscribe
   1. Start a mosquito server to publish to inno/test topic:

|  |
| --- |
| mosquitto\_pub.exe -h test.mosquitto.org -P 8884 -u innophase -P 123 -t inno/test -m "Hii Innophase" |

Text

Description automatically generated

Figure 87: Command Prompt Output (Subscribe message)

* 1. Issue the following command to subscribe to inno/test topic on the serial terminal and get the published message:

|  |
| --- |
| at+mqttsub=0,inno/test,0 |

Text

Description automatically generated

Figure 88: To subscribe

## DNS Lookup – Get host IP by name

### Description

This use case is to demonstrate getting IP address from the host name.

### Prerequisites

Access Point configured with WPA/WPA2 personal security.

### AT Command Sequence

|  |  |
| --- | --- |
| **AT Command** | **Description** |
| *at* | Check communication state |
| *at+wscan* | Get list of available APs from the vicinity |
| *at+wcon* | Connect to a desired AP from the received scan results |
| *at+wstatus* | Get IP address of Talaria TWO to verify the connection(L2+L3) is successful |
| *at+nhostipget* | Get host IP address by name |

Table 23: DNS Lookup – Get host IP by name - AT Commands

### Procedure

**Step 1**: Execute the following commands on Talaria TWO:

|  |
| --- |
| at  at+wscan  at+wcon=InnoPhase,Inno@9070  at+wstatus=0  at+nhostipget |

### Serial Log

Text

Description automatically generated

Figure 89: DNS Lookup – Get host IP by name - Serial log

## Service Discovery using mDNS

### Description

This module is used to start the mDNS procedure of the node with IPv4 network.

It supports following services:

1. mDNS Service Announce.
2. mDNS Service Discover.

### Prerequisites

1. Access Point configured with any Wi-Fi security types (WPA/WPA2/WPA3 Personal/Enterprise protocols).
2. Bonjour Browser for windows OS or from a Windows command line, use dns-sd command to browse for services that are being broadcast on the local network by Talaria TWO.

### AT Command Sequence

|  |  |
| --- | --- |
| **Command** | **Description** |
| *at* | Check communication state |
| *at+wscan* | Get list of available APs from the vicinity |
| *at+wcon* | Connect to a desired AP from the received scan results |
| *at+wstatus* | Get IP address of Talaria TWO to verify the connection(L2+L3) is successful |
| *at+mdnsstart* | Starts mDNS |
| *at+mdnsreg* | Register the mDNS service by passing the service name,type,proto,port and the description |
| *at+mdnsdreg* | De-Register mDNS Service by providing the service Identifier that was captured when the registration was done |
| *at+mdnstop* | Stops mDNS |

Table 24: Service Discovery using mDNS - AT Commands

### Procedure

**Step 1**: Connect your laptop to the same access point “InnoPhase” to which the Talaria TWO is connected.

Graphical user interface, text

Description automatically generated

Figure 90: Connecting to an Access Point

**Step 2**: Issue the following commands to advertise the services on local network. Connect the Talaria TWO module to an AP of SSID "InnoPhase" and passphrase "43083191".

Check the WLAN status with at+wstatus command. Start the mDNS service and register to service name “Inno\_Provisioning“ of service type “TCP” on port number 80 and “Provisioning” as service description.

|  |
| --- |
| at  at+wscan  at+wcon=InnoPhase,43083191  at+wstatus=0  at+mdnsstart  at+mdnsreg=Inno\_Provisioning,\_http,1,80,Provisioning |

**Step 3**: Start Bonjour Browser and Scan for the services that are announced by Talaria TWO.

Graphical user interface, text, application

Description automatically generated

Figure 91: Starting Bonjour Browser and Scanning for the services

Alternate way of Service discovery can be done from a Windows command line, using the dns-sd command to browse for services that are being broadcast on the local network by Talaria TWO.

Text

Description automatically generated

Figure 92: Service discovery from Windows command line

Serial Log:

Text

Description automatically generated

Figure 93: Service Discovery using mDNS - Serial log

**Step 3**: De-register mDNS service, registered using command AT+MDNSREG and stop the mDNS service using the following commands:

|  |
| --- |
| at+mdnsdreg=0  at+mdnsstop |

Text

Description automatically generated

Figure 94: De-registering from mDNS service

## Get Time from NTP Server

### Description

This use case is to demonstrate getting time from the NTP server.

### Prerequisites

Access Point configured with WPA/WPA2 personal security.

### AT Command Sequence

|  |  |
| --- | --- |
| **AT Command** | **Description** |
| *at* | Check communication state |
| *at+wscan* | Get list of available APs from the vicinity |
| *at+wcon* | Connect to a desired AP from the received scan results |
| *at+wstatus* | Get IP address of Talaria TWO to verify the connection(L2+L3) is successful |
| *at+ntptimeget* | Get time from NTP server |

Table 25: Get Time from NTP Server - AT Commands

### Procedure

**Step 1**: Execute the following commands on Talaria TWO:

|  |
| --- |
| at  at+wscan  at+wcon=InnoPhase,Inno@9070  at+wstatus=0  at+ntptimeget |

### Serial Log

Text

Description automatically generated

Figure 95: Get Time from NTP Server - Serial log