S

ODIN W2 series

Stand-alone multiradio modules with Wi-Fi & Bluetooth

Getting Started

Abstract

This document describes how to set up and use the ODIN-W2 series multiradio modules with Wi-Fi and Bluetooth® dual mode 4.0 (Bluetooth and Bluetooth Low Energy). It also provides a technical overview of the ODIN-W2 series and describes how to configure Bluetooth in ODIN-W2.

www.u-blox.com

UBX-15017452 - R08

Document Information

Title	**ODIN W2 series**	
Subtitle	Stand-alone multiradio modules with Wi-Fi & Bluetooth	
Document type	Getting Started	
Document number	UBX-15017452	
Revision and date	R08	11-Jun-2018
Disclosure Restriction		

This document applies to the following products:

Product name	Type number	Software version	PCN reference
ODIN-W260	ODIN-W260-00B-00	1.0.0	N/A
	ODIN-W260-01B-00	2.0.0	
	ODIN-W260-01B-01	2.0.1 2.0.2	
	ODIN-W260-02B-00	3.0.0 3.0.1	
	ODIN-W260-03B-00	4.0.0	
	ODIN-W260-03B-01 ODIN-W260-03X-00	4.0.1	
ODIN-W262	ODIN-W262-00B-00	1.0.0	N/A
	ODIN-W262-01B-00	2.0.0	
	ODIN-W262-01B-01	2.0.1 2.0.2	
	ODIN-W262-02B-00	3.0.0 3.0.1	
	ODIN-W262-03B-00	4.0.0	
	ODIN-W262-03B-01 ODIN-W262-03X-00	4.0.1	

Contents

1 Introduction

The ODIN W2 series is a highly integrated multiradio module developed by u-blox for integration in demanding, reliable devices such as those needed for industrial and medical applications. The module is built around a multiradio chip, which includes Wi-Fi, Bluetooth and Bluetooth Low Energy. This document describes how to set up and use the modules.

1.1 Key features

One of the key features of the ODIN W2 series is the Wireless serial cable replacement functionality. The basic functionality is to transfer data between the serial port and a wireless link. It is possible to configure the ODIN W2 series module to automatically setup a connection and/or accept an incoming connection using AT commands.

For a host, this means that an existing serial cable can be replaced by a wireless solution; in many cases without the need to modify the host.

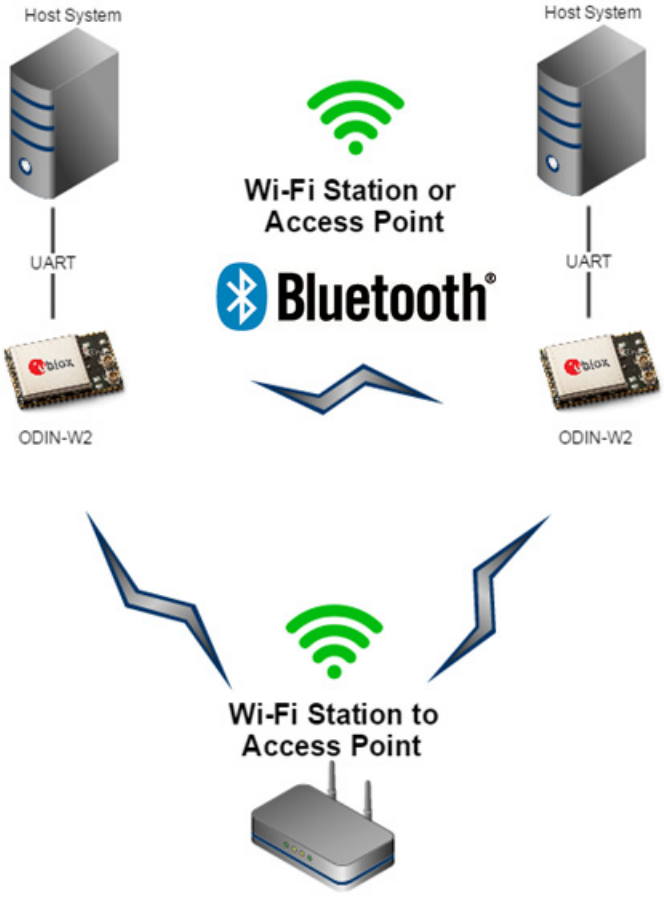

Figure 1: ODIN W2 series Bluetooth setup

1.2 Modes of operation

The ODIN W2 series can operate in the following three different modes:

- Command mode
- Data mode
- Extended Data mode

By default, ODIN-W2 will enter command mode and has to be re-configured to start up in data mode or extended data mode. When in the data mode or extended data mode, it is possible to enter the command mode by transmitting the escape sequence to the module. By default, the escape sequence is:

1. Silence 1 second
2. +++
3. Silence 1 second

☞ The +++ must be sent within 200 ms, which means that it is difficult or impossible to enter the escape sequence manually using a terminal window though the characters can be typically be pasted instead. The module leaves the command mode and enters the data mode or extended data mode using the **ATO1/ATO2** command. It is also possible to toggle the UART DTR pin from High to Low to enter command mode.

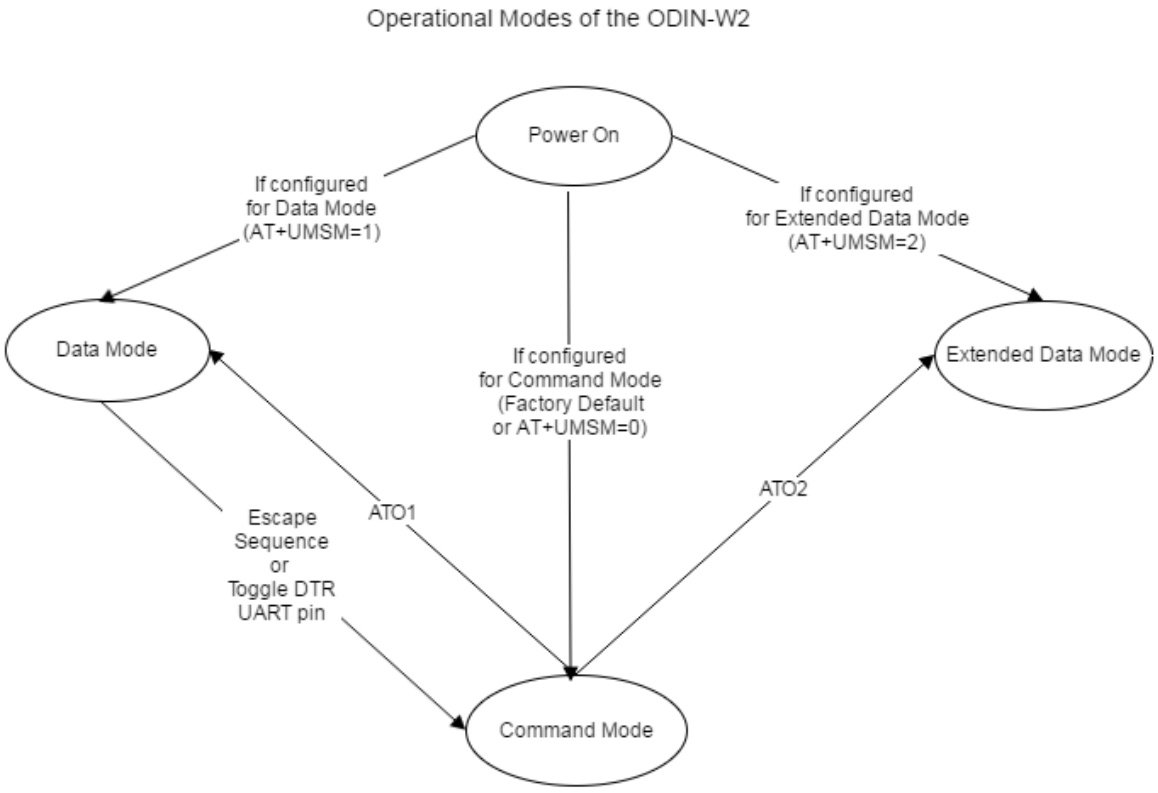

Figure 2: AT data mode

In command mode, the module is configured using AT commands. For information regarding all the available AT commands, see u-blox Short Range Modules AT Commands Manual [1].

In data mode, the module transmits data transparently between the serial UART and the wireless connection(s). There is no additional protocol for the UART. Data transmitted on the UART to the module will be transmitted (and broadcasted for all connections), over air, to all wireless connections. Data received from the wireless connections may be interleaved upon reception and it may be difficult

or impossible to figure out from what remote device data is received. This "multipoint strategy" is called as Wireless Multidrop. It is suitable mainly for master/slave polled protocols such as Modbus and point-to-point communication.

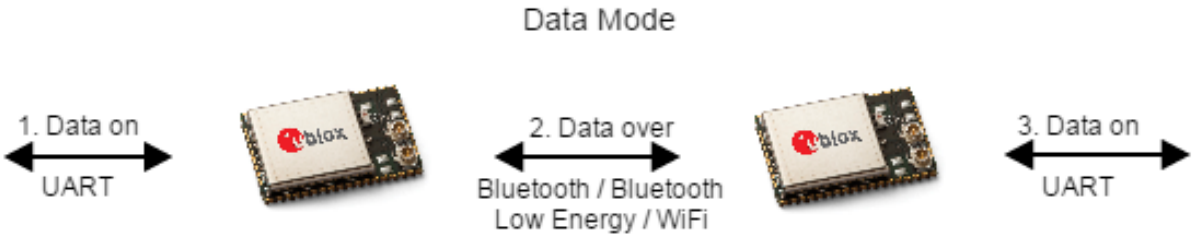

Figure 3: Data mode

The extended data mode is used to enable control of each individual wireless connection (see u-blox Extended Data Mode Protocol Specification [2]). The extended data mode is a simple protocol for the UART, which enables transmission of data to one specific remote device and to know from what remote device the data is received. It is also possible to execute AT commands as part of the extended data mode protocol. Hence, it is not necessary to enter command mode when in the extended data mode. As it is possible to enter command mode from the extended data mode, tools such as the s-center will still work using standard AT commands in the command mode.

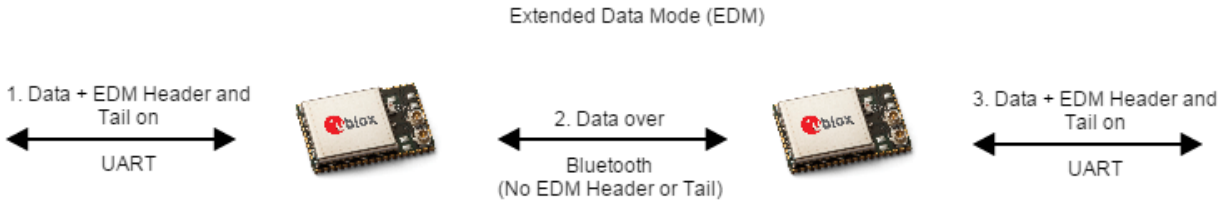

Figure 4: Extended data mode

☞ Over air, there is no extended data mode protocol data. Over air only "raw" data is transmitted in the same way as in the data mode. Hence, it is possible for one side to be configured for extended data mode and the other side for standard data mode.

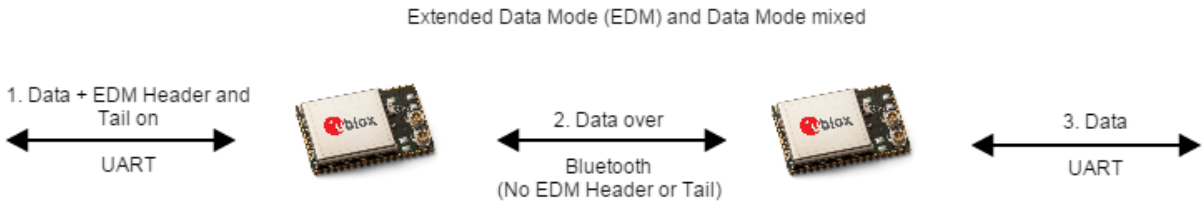

Figure 5: Data mode and extended data mode

1.3 Easy commissioning

It is possible to use Easy commissioning to remotely send AT Commands to the remote device. This can be used over Bluetooth using SPP, Bluetooth Low Energy SPS, or over a UDP/TCP connection.

The command **AT+UDSC** is used for Easy commissioning, to connect to a remote device to let incoming SPP handle AT commands use **AT+UDSC=1,8,3**. To let an incoming UDP connection on port 23 handle AT commands, use **AT+UDSC=2,8,2,23**. See u-blox Short Range Modules AT Commands Manual [1] for more details.

2 Peers

A connection consists of a sender and a receiver of data. It can also consist of a sender and several receivers in the case of a wireless multidrop/broadcast data. In both cases, every sender and receiver in a setup is referred to as a peer. Thus, a peer is capable of either receiving and/or sending data.

There are two kinds of peer classes in the serial port adapter:
- Local peer
- Remote peer

The local peer is (currently) synonymous with the UART. In contrast to the local peer, the remote peer is another device or broadcast range on the network. Several remote peers can be defined if a multi-drop scenario is needed.

A remote peer is addressed using a Uniform Resource Locator, URL. These locators are strings representing nodes on internet or on a local net. This is the same addressing technology used in for example a web browser. For more information about URLs, check out http://www.rfc-base.org/txt/rfc-1738.txt.

In general, URLs are written as follows:
<scheme>:<scheme-specific-part>

Where <scheme> is the scheme or protocol used while communicating and <scheme-specific-part> is normally the address and port number of the remote node.

For example, a web server on the internet can have the following address:
http://www.u-blox.com/

This tells the browser to use the HTTP protocol and connect to the node at address http://www.u-blox.com/. Similar addressing scheme is used by ODIN-W2 to pinpoint the remote peer. The scheme is not "http", but the node addressing is identical.

Available schemes:
- tcp: TCP connection
- udp: UDP connection, broadcast capabilities
- spp: Bluetooth Serial Port Profile
- dun: Bluetooth Dial Up Networking
- sps: Bluetooth Low Energy u-blox Serial Port Service

Syntax:
- tcp/udp: <scheme>://ipaddress<:portnumber>
- spp/dun/sps: <scheme>://bluetooth_address/

Remarks:
- IP address can be either a numeric IP address or a host and domain name that can be resolved using the configured DNS servers.

Examples:
- tcp://10.0.0.9:5003
- tcp://echo.u-blox.com:7
- udp://192.168.0.42:6809
- spp://0012f3000001

A peer can be setup using either the default remote peer command **AT+UDDRP** or dynamically created using the connect peer command **AT+UDCP**. A connection is closed using **AT+UDCC**.

To enable incoming connections, servers must be enabled using the command **AT+UDSC**. One server of each type can be created, but it can allow for multiple incoming connections. By default, the SPP

server is enabled on Server id 0, and in Bluetooth Low Energy, enable the SPS service using the **AT+UDSC** command.

☞ You need to enable Bluetooth Low Energy and send AT&W in order to enable the SPS service.

3 Wi-Fi Network setup

To use TCP and UDP peers, at a Wi-Fi network must be activated and connected. This is done using the **AT+UWSC** and **AT+UWSCA** commands for Wi-Fi Station Configuration and **AT+UWAPC** and **AT+UWAPCA** commands for Wi-Fi Access Point Configuration. To define a network, IP address assignment behavior must be defined. Default behavior is DHCP client, static address is also supported.

Currently only Wi-Fi Station or Wi-Fi Access point can be configured at any given time and not both of them simultaneously.

4 Evaluation board

The evaluation board for ODIN-W2 is EVK-W262.

4.1 LED Indications and buttons

There are two operational buttons and one multi LED as shown in Figure 6.

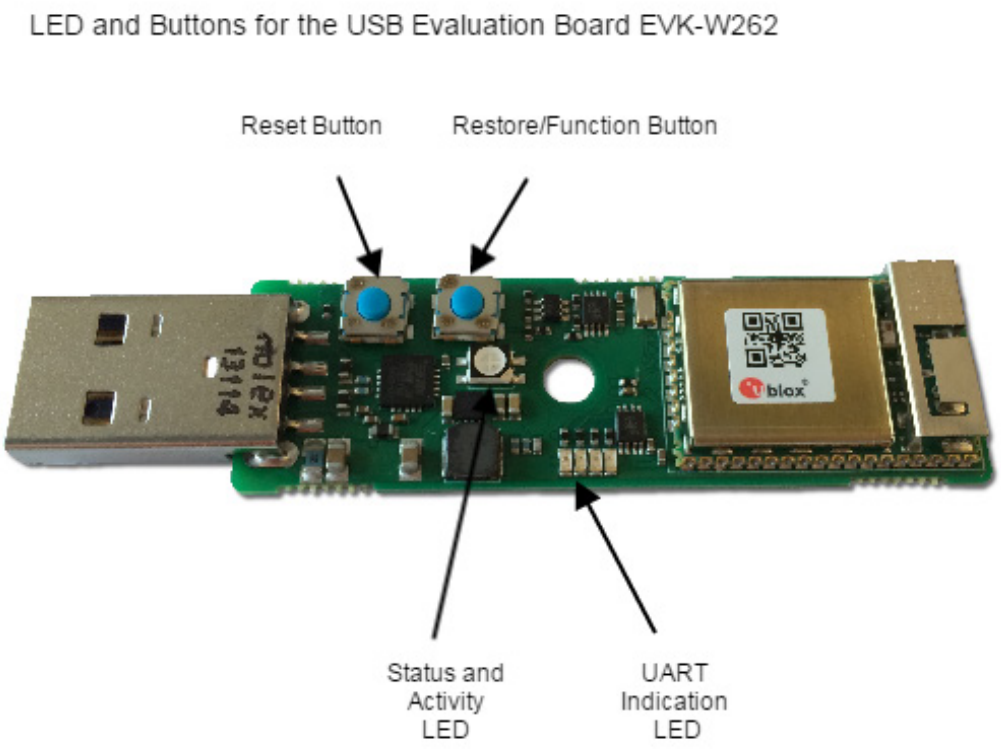

Figure 6 USB adapter board

The LED indicates what mode is currently active and what activity that is currently in progress. The following color indications are used. See EVK-W262U Quick Start Guide [4] for more information about the EVK-W262.

The Restore/Function Button will restore to factory default with serial settings if pressed for 10 seconds during power up. The Restore/Function button will have the "External Connect" functionality when ODIN-W2 is in normal mode.

- **Green:** The current mode is data mode or extended data mode and no connection attempts are in progress.
- **Orange:** The current mode is command mode.
- **Purple:** A connection attempt is in progress.
- **Blue:** A connection is currently active.
- **Blue Blinking:** A connection is active and data is transmitted or received over air.
- **Red Blinking:** Error detected. Typically this means buffer overflow, parity or framing error detected on the UART.

☞ The LED on the USB adapter board is a 3-colour LED which means that, on the module, it corresponds to three IO pins. On another board it may have different meaning.

4.2 Restore default serial settings

If the Restore/Function button is pressed during power on, the module resets the serial settings and escape sequence to the default values.

- Default serial settings is 115.2 kbps, 8N1 and HW flow control enabled
- Default escape sequence is +++
- Default escape sequence timing is 1s silence before and after escape sequence

4.3 Restore factory settings

If both the default serial settings and the external connect button is pressed during power on, the factory settings are restored. You can also restore to factory settings using the **AT+UFACTORY** command followed by power off/on.

5 Bluetooth configuration

You can configure the ODIN-W2 module according to specific customer requirements using AT commands (see u-blox Short Range Modules AT Commands Manual [1]). The easiest way to get started is to use the s-center, which is a graphical user interface for sending AT-commands (see s-center Quick Start Guide [4]). The s-center allows an easy configuration for the most common AT commands.

5.1 Basic settings

There are some basic commands for controlling the general Bluetooth behavior of the module.

- **Connectable** - **AT+UBTCM:** Configures the connectability for incoming connections.
- **Discoverable** - **AT+UBTDM**: Configures the visibility for remote devices making inquiries.
- **Pairable** - **AT+UBTPM**: Configures the ability to pair (authenticate) for remote devices.
- **Bluetooth name** - **AT+UBTLN**: The name presented to remote devices making inquiries or name requests.
- **Class of device** - **AT+UBTLC**: Configuration for the classification of the device. Default settings according to the Bluetooth specification.

Once a pairing has been done with a remote device, it is recommended to disable both discoverable and pairable devices for security reasons and performance.

5.2 Client and server

A client will initiate a connection and the server will accept an incoming connection.

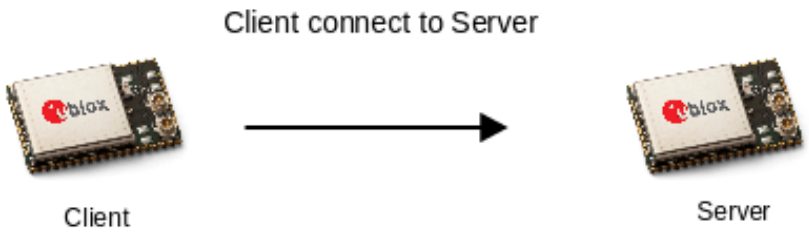

Figure 7 Client connecting to the server

The client and server role is often mistaken for master and slave role. The master/slave role is defined at a lower level (master polls slave at radio level) and has nothing to do with client and server. By default, the client will become master and the server will become slave. However, a master/slave switch during or after connection set-up can change this. The master/slave role is to be considered for the multipoint case only (see Multipoint section).

To configure a client to automatically set up a connection to a server, configure the correct Bluetooth profile and the remote peer. The Bluetooth profile controls the type of connection that is requested (see Bluetooth profiles section) and the preferred server to connect is defined by the remote peer. In a multipoint scenario, see the Multipoint section.

- **Default Remote Peer** **AT+UDDRP**: Configures server (profile and address) to connect and when to initiate the connection. Peer is enumerated starting with id 0.

To configure the server, consider only the Bluetooth profile and a module is configured as a Serial Port Profile (SPP) server by default.

- **Server Configuration** **AT+UDSC**: Will only accept incoming connection attempts for the configured server profile. Some profiles can be configured in parallel.

For more than one connection, see the Multipoint section.

5.3 Bluetooth profiles

The Bluetooth profiles used by the client and server define the type of connection that is accepted.

- **Serial Port Profile (SPP):** Serial cable emulation profile to replace existing serial cables.
- **Dial-Up Network (DUN):** Modem emulation typically used by a Bluetooth device to access the Internet via a mobile phone. It requires the host to have its own TCP/IP stack.

The client profile must match the server profile for a connection to be accepted.

☞ There are some special requirements to make the SPP profile work for iPhone. Contact your local FAE for more information.

5.4 Multipoint

It is possible to configure a module to support up to 7 parallel Bluetooth connections.

The **AT+UBTCFG** command is used to set number of Bluetooth connections. It is recommended to use this configuration since the link will be optimized with respect to this number. In data mode, data is transmitted over air to all connected devices and data received from the remote devices is interleaved.

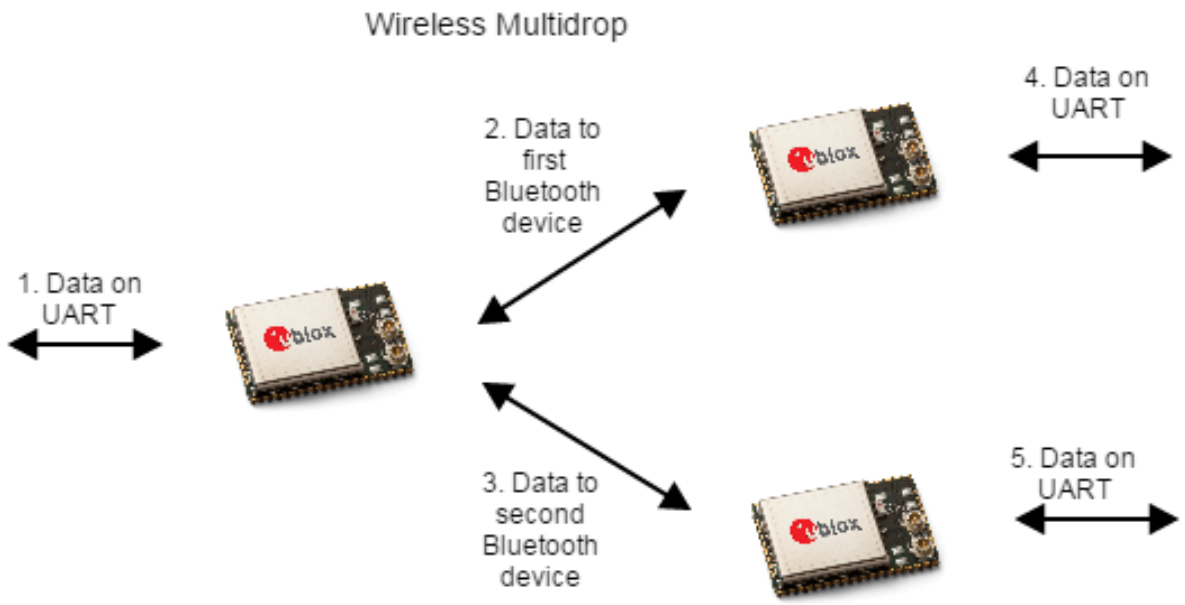

Figure 8 Wireless Multidrop

In extended data mode, it is possible to transmit data to a specific remote device and to know from which remote device data is received.

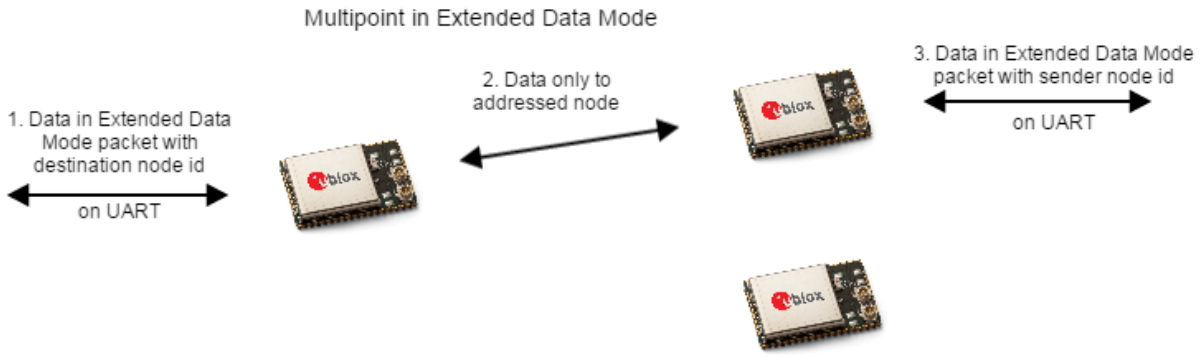

Figure 9 Multipoint in extended data mode

For the multipoint case, it is important to consider the master/slave role (which is not the same as client/server). If a device has multiple Bluetooth connections active and if the device is master for all the connections, this is a piconet. If the device is master for all of the connections expect one where it is the slave this is called a scatternet. Performance for a piconet is better and more robust than scatternet. Only 6 parallel channels can be achieved for a scatternet.

By default, the client becomes the master and the server becomes the slave. If a server wants to support multiple channels and it wants to have a piconet for best performance, the server must request a master/slave switch for every incoming connection. The **AT+UBTMSP** command can set the always master configuration, which requests a master/slave switch for every incoming (not outgoing) connection.

5.5 Bluetooth security

Introducing simple pairing in Bluetooth 2.1 security became more complex. The security in Bluetooth 2.1 must be backward compatible with Bluetooth 2.0 standard.

It is recommended to start with security mode 1 **AT+UBTSM=1**, which is Bluetooth 2.0 security disabled and Bluetooth 2.1 auto accept security for getting started. However, when finalizing the product, security must be analyzed and a more secure solution may be appropriate.

5.6 Power save

The Wi-Fi power save mode is enabled by default and can be turned off using AT+UWCFG=1,0 to get better response time and performance using Wi-Fi. Power save Bluetooth is not yet implemented.

6 Wi-Fi Configuration

To use Wi-Fi as transport for serial data, setup both the network and peers. It is possible to setup both TCP and UDP peers and they can be both client and server.

6.1 Network setup

To setup a network, Wi-Fi Station or Access Point Network configuration AT+UWSC or AT+UWAPC, and Wi-Fi Station or Access Point action AT+UWSCA or AT+UWAPCA command shall be used. With the AT+UWSC or AT+UWAPC command, all necessary Wi-Fi and network parameters are configured, like network address, SSID and security settings. Multiple Wi-Fi networks can be configured, but only one can be active at any given point of time.

☞ Both **AT+UWSCA** and **AT+UWAPCA** can store the parameters to flash memory without using the AT&W command; all other AT commands must be saved to the startup database using the AT&W.

6.2 Wi-Fi security

ODIN-W2 supports several security modes. The matrix below shows its valid security combinations.

	Unencrypted	WEP64	WEP128	TKIP	AES/CCMP
Open	Valid	Valid (only Station)	Valid (only Station)		
Shared					
WPA				Valid	Valid
WPA2				Valid	Valid
LEAP		Valid (only Station)	Valid (only Station)	Valid	Valid
PEAP		Valid (only Station)	Valid (only Station)	Valid	Valid

Table 1: Security combinations

⚠ WEP is considered highly unsecure, is deprecated in the 802.11i specification and should not be used. TKIP is also considered as unsecure.

6.3 Peer setup

Peer setup is used using the "Default Remote Peer" **AT+UDDRP** and "Server Configuration" **AT+UDSC** commands.

6.4 TCP Peer

When a TCP peer is connected, data can flow in both directions irrelevant of whether the peer is a server or client. To optimize the TCP link for short latency the <flush_tx=1> can be specified in the URL; normally this is not needed. For example, to connect to port 8080 with an optimized latency, provide the following URL:

“**tcp://192.168.0.1:8080/?flush_tx=1**” (Using IPv4 address)
“**tcp://[FE80::7AA5:4FF:FE2F:5F01]:8080**” (Using a IPv6 address)

6.5 UDP Peer

For an UDP peer, the behavior differs for servers and clients. A server will accept data from any IP address sent to the activated port number.

A client can be used to both send and receive data to and from the address specified. To listen on a different port than the remote port the <local_port> can be specified in the URL. For example, to send on port 8080 and receive on port 8081 gives the following URL:

“**udp://192.168.0.1:8080/?local_port=8081**”

7 Use case examples - Software 1.0.0

7.1 Establish a Bluetooth SPP connection between two ODIN-W2 modules

- By default, ODIN-W2 accepts incoming connection and replies on Inquiry.
- Make inquiry to find the remote device.
  - **AT+UBTI**
- Note the Bluetooth address for remote device, it is needed for the connection command.
  - **+UBTI:112233445566,-52,000000,"Bluetooth Device"**
- ODIN-W2 will now try to Bluetooth Serial Port Profile on other ODIN-W2
- When the event **+UDCP:1** is received the Bluetooth connection is up.
- ERROR will be received if connection is not established.
  - **AT+UDCP="spp://112233445566"**
- Have a successful connection, remote device will send the following event.
- In the connection event the connection type and Bluetooth Address can be found.
  - **+UUDPC:1,1,1,78A5042F5F00,0**
- Enter Data Mode.
  - **ATO1**

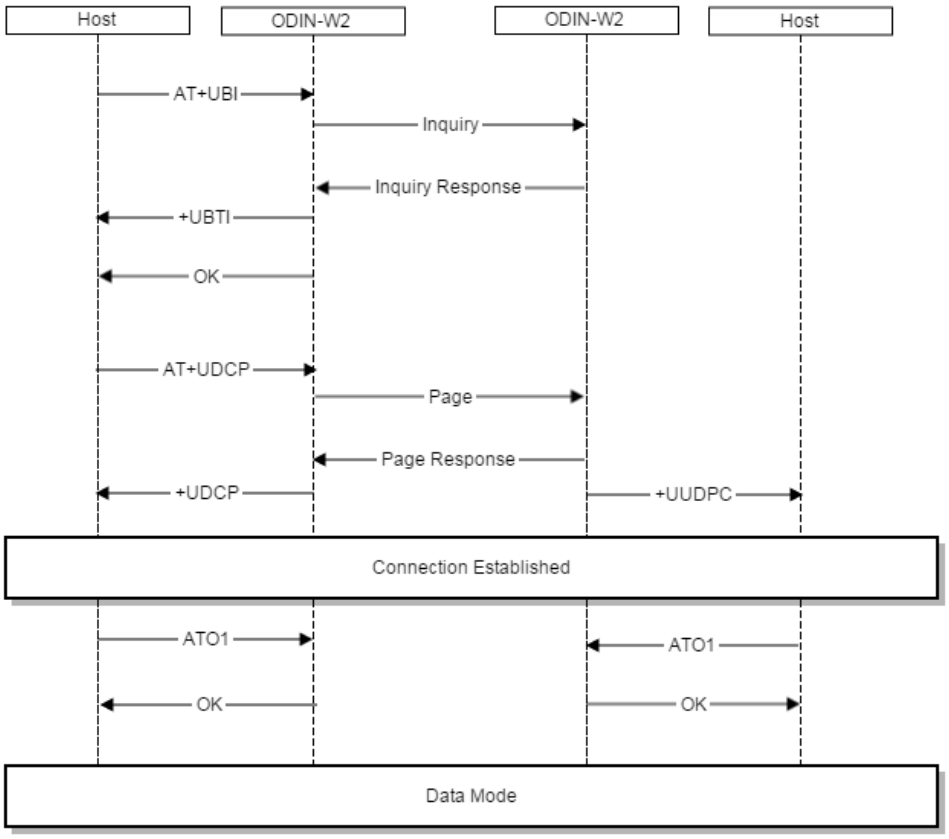

Figure 10: ODIN-W2 Bluetooth SPP Connection

7.2 Establish a Bluetooth SPP connection that connects automatically

- Setup a default remote peer, configured with always connected parameter.
  - **AT+UDDRP=0,"spp://0012f3000001/",2**
- Select startup mode, startup in data mode.
  - **AT+UMSM=1**
- Store configuration in startup database.
  - **AT&W0**
- Reboot to use the new settings.
  - **AT+CPWROFF**

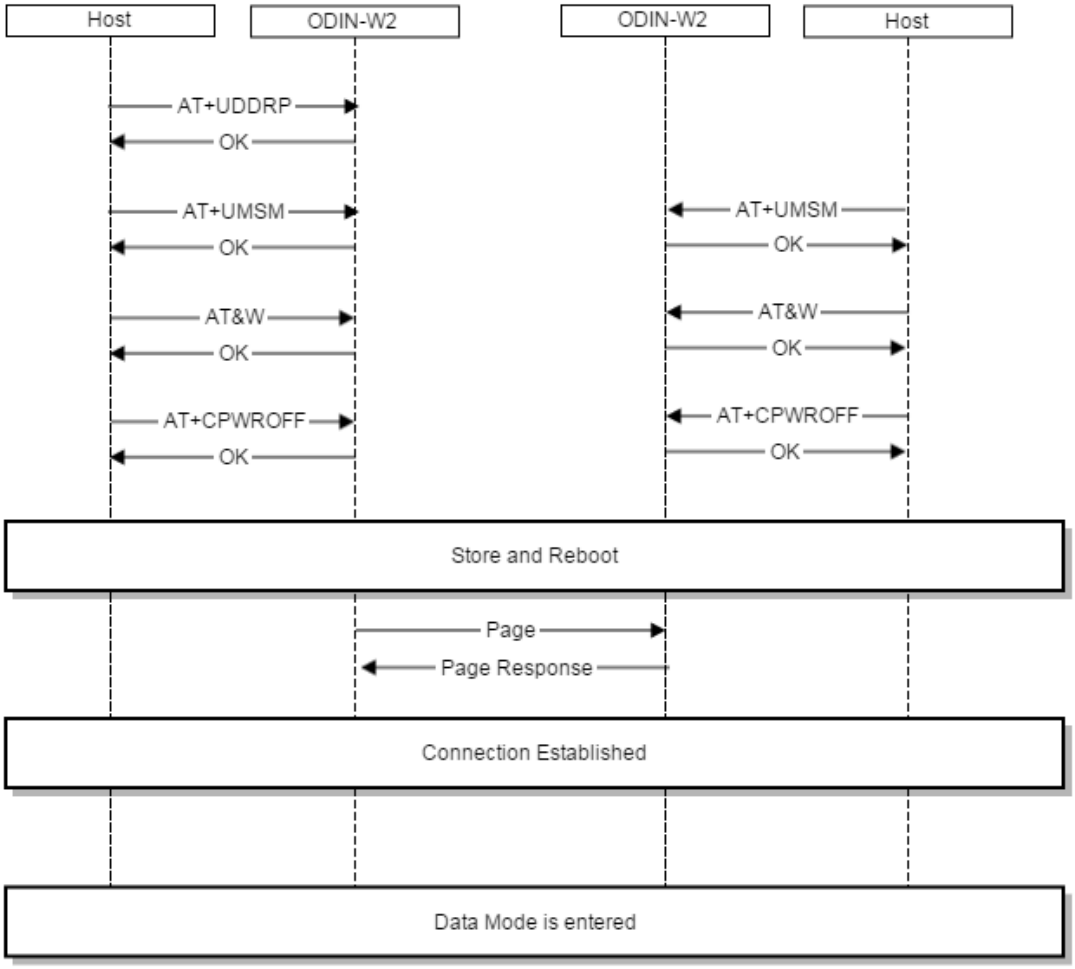

Figure 11: ODIN-W2 Bluetooth SPP connection remote peer

7.3 Set up TCP listener (using Wi-Fi) and a static IP

Station

- **Network part using DHCP**
  - Deactivate network id 0.
    - **AT+UWSCA=0,4**
  - Disable DHCP Client (static IP address will be used).
    - **AT+UWSC=0,100,1**
  - Set Network IP address.
    - **AT+UWSC=0,101,192.168.0.100**
  - Set Network Subnet mask.
    - **AT+UWSC=0,102,255.255.0.0**
  - Configure to be active on startup.
    - **AT+UWSC=0,0,1**
  - Store Wi-Fi configuration.
    - **AT+UWSCA=0,1**
    -
- **TCP and data part**
  - Set server configuration id 1, using TCP and port 8080.
    - **AT+UDSC=1,1,8080**
  - Set startup mode to data mode.
    - **AT+UMSM=1**
    -
- **Restart module for settings to take effect**
  - Store configuration to startup database.
    - **AT&W0**
  - Reboot ODIN-W2, the following will happen:
  - Start to scan for the network with the SSID = "my network".
  - When Wi-Fi is connected and the Network is up, the TCP connection will be set up as well.
    - **AT+CPWROFF**

7.4 Set default remote peer (Wi-Fi and TCP) using DHCP that connects automatically

Station

☞ This use case, prerequisites that a server is available on IP address 192.168.0.100 and accepts connections on port 8080, as explained in chapter 7.3.

- **Network part using DHCP**
  - Deactivate network id 0.
    - **AT+UWSCA=0,4**
  - Active on startup.
    - **AT+UWSC=0,0,1**

- **Wi-Fi part**
  - Set the Network SSID to connect to.
    - **AT+UWSC=0,2,"my ssid"**
  - Use WPA2 as authentication type.
    - **AT+UWSC=0,5,2**
  - Recommended to use a secured WPA2 password.
    - **AT+UWSC=0,8,"my password"**
  - Set Network IP address.
    - **AT+UWSC=0,101,192.168.0.99**
  - Set Network Subnet mask.
    - **AT+UWSC=0,102,255.255.0.0**
  - Store Wi-Fi configuration.
    - **AT+UWSCA=0,1**

- **TCP and data part**
  - Set default remote peer id 0, using TCP and always connected.
    - **AT+UDDRP=0,"tcp://192.168.0.100:8080",2**
  - Configure to startup to data mode.
    - **AT+UMSM=1**

- **Restart module for settings to take effect**
  - Store configuration to startup database.
    - **AT&W0**
  - Reboot ODIN-W2, the following will happen:
  - Start to scan for the network with the SSID = "my network".
  - When Wi-Fi is connected and the Network is up, the TCP connection will be set up as well.
    - **AT+CPWROFF**

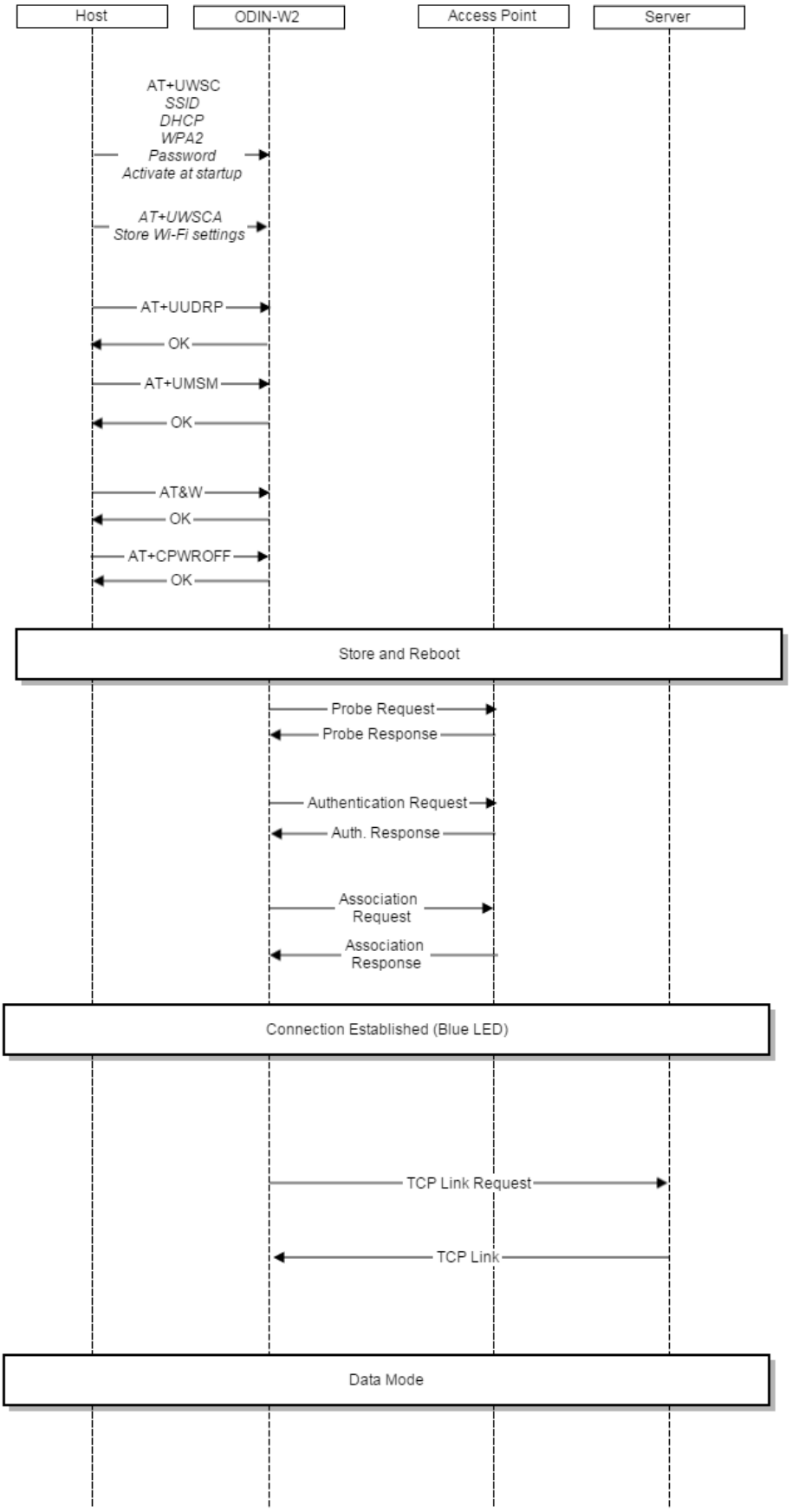

Figure 12: ODIN-W2 Wi-Fi Connection

7.5 Set default remote peer (Wi-Fi and TCP) using static IP address that connects automatically

Station

☞ This use case, prerequisites that a server is available on IP address 192.168.0.100 and accepts connections on port 8080, similar to the one mentioned in chapter 7.3.

- **Network part using Static IP Address**
  - Deactivate network id 0.
    - **AT+UWSCA=0,4**
  - Active on startup.
    - **AT+UWSC=0,0,1**
  - Disable DHCP Client (static IP address will be used).
    - **AT+UWSC=0,100,1**
  - Network IP address.
    - **AT+UWSC=0,101,192.168.0.99**
  - Network Subnet mask.
    - **AT+UWSC=0,102,255.255.0.0**

- **Wi-Fi part**
  - Set the Network SSID to connect to.
    - **AT+UWSC=0,2,"my ssid"**
  - Use WPA2 as authentication type.
    - **AT+UWSC=0,5,2**
  - The secret WPA2 Password.
    - **AT+UWSC=0,8,"my password"**
  - Store Wi-Fi configuration.
    - **AT+UWSCA=0,1**

- **TCP and data part**
  - **AT+UDDRP=0,"tcp://192.168.0.100:8080",2**
    - Set default remote peer id 0, using TCP and always connected.
  - **AT+UMSM=1**
    - Set startup mode to data mode.

- **Restart module for settings to take effect**
  - Store configuration to startup database.
    - **AT&W0**
  - Reboot ODIN-W2, the following will happen:
  - Start to scan for the network with the SSID = "my network".
  - When Wi-Fi is connected and the Network is up, the TCP connection will be set up as well.
    - **AT+CPWROFF**

7.6 Connect ODIN-W2 using Wi-Fi and cellular Internet sharing connection

Station

- **Enable Internet Sharing on the cellular device and select a Wi-Fi password**
  - Settings > Internet Sharing > Enable.
- **Scan for the Internet Sharing network**
  - **AT+UWSCAN**
  - **+UWSCAN:F2A637C90E9E,1,"my phone",6,-33,16,8,8**

- **Wi-Fi setup**
  - Deactivate network id 0.
    - **AT+UWSCA=0,4**
  - Active on startup.
    - **AT+UWSC=0,0,1**
  - Set the Network SSID to connected to.
    - **AT+UWSC=0,2,"my Phone"**
  - Use WPA2 as authentication type.
    - **AT+UWSC=0,5,2**
  - The secret WPA2 Password.
    - **AT+UWSC=0,8,"my password"**
  - Activate Wi-Fi configuration.
  - ODIN-W2 will now try connect immediately.
    - **AT+UWSCA=0,3**

- **Wait for the Wi-Fi link and network to go up**
  - Mac address received and connected on Channel 11.
    - **+UUWLE:0,F2A637C90E9E,11**
  - Network is up, it is now possible to read the IP Address.
    - **+UUNU:0**

- **Read IP address and gateway**
  - ODIN has got the IP Address 172.20.10.2.
    - **AT+UNSTAT=0,101**
    - **+UNSTAT:0,101,172.20.10.2**
  - The gateway on IP Address 172.20.10.1.
    - **AT+UNSTAT=0,103**
    - **+UNSTAT:0,103,172.20.10.1**

Proceed by starting an app on the cellular device. Sample apps that work well are “TCP console” for iOS and “TCP UDP Terminal” for Android, which supports both TCP client and server. Start a TCP Server, the port 5003 is used in this example, but any port can be used on the phone.

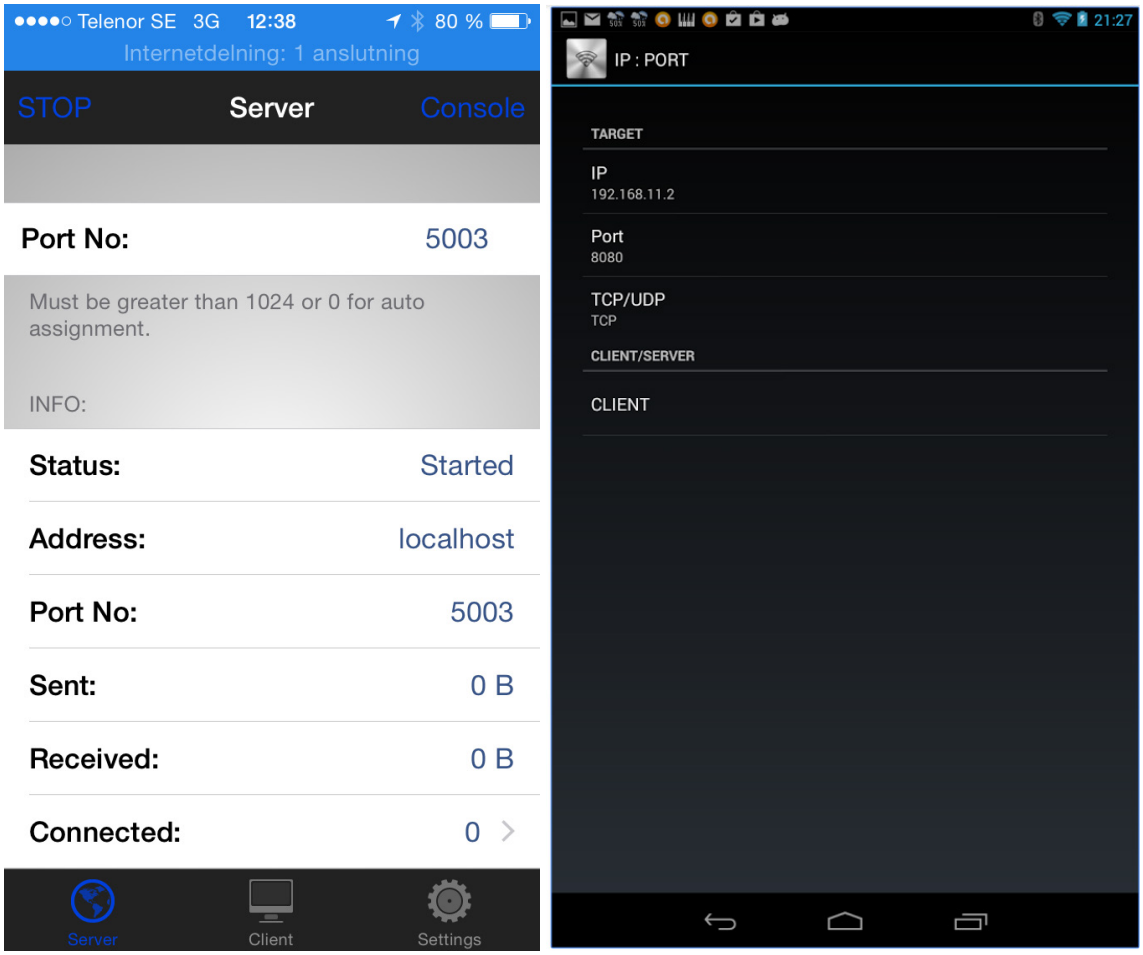

Figure 13: TCP console for iOS and TCP UDP Terminal for Android

You can download the Apps using the following URLs:

https://itunes.apple.com/se/app/tcp-console/id642104251?mt=8

https://play.google.com/store/apps/details?id=nextprototypes.tcpudpterminal

Now connect TCP and enter Data Mode on ODIN-W2.

TCP and data part

- Connect using TCP.
  - `AT+UDCP="tcp://172.20.1:5003"`
- When `+UDCP:1` is received, the TCP is connected.

- Enter Data Mode.
  - `ATO1`

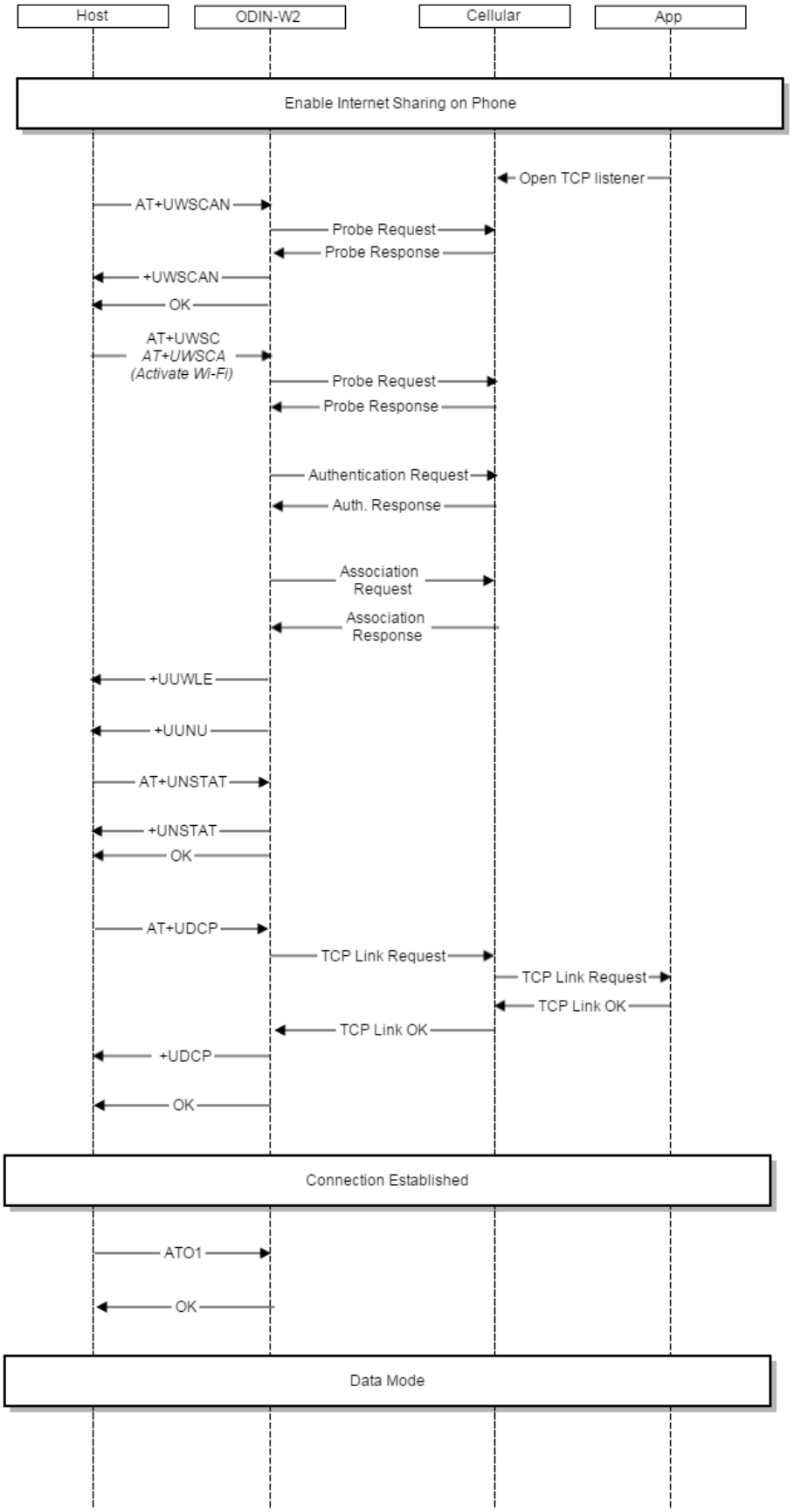

Figure 14: ODIN-W2 Wi-Fi Connection to iPhone

8 Use case examples - Software 2.0.0

8.1 Connect two ODIN-W2 modules using Wi-Fi Access Point and Station

Wi-Fi Access Point +

Wi-Fi Station

On device #1 (Access Point):

- **Network part using Static for AP and DHCP for clients**
  - Deactivate network id 0.
    - **AT+UWAPCA=0,4**
  - Not active on startup.
    - **AT+UWAPC=0,0,0**
  - Set SSID for the Network.
    - **AT+UWAPC=0,2,"UBXWifi"**
  - Set Channel 1 for the Network.
    - **AT+UWAPC=0,4,1**
  - Set WPA2 Security for the Network.
    - **AT+UWAPC=0,5,2,2**
  - Use Password "**my password**"
    - **AT+UWAPC=0,8,"my password"**
  - Static IP address for Access Point.
    - **AT+UWAPC=0,100,1**
  - Network IP address.
    - **AT+UWAPC=0,101,192.168.2.1**
  - Network Subnet mask.
    - **AT+UWAPC=0,102,255.255.255.0**
  - Network Gateway address.
    - **AT+UWAPC=0,103,192.168.2.1**
  - Enable DHCP for connected Clients. DHCP Server will provide addresses according to the following formula: (Static address & subnet mask) + 100. The first client will get the IP address 192.168.2.100.
    - **AT+UWAPC=0,106,1**
  - Activate Wi-Fi Access Point configuration.
    - **AT+UWAPCA=0,3**
    -
- **TCP and data part**
  - Set server configuration id 1, using TCP and port 8080.
    - **AT+UDSC=1,1,8080**
    -
- **Enter Data Mode**
  - Enter Data Mode to send data.
    - **ATO1**

On device #2 (Station):

- **Network part using DHCP IP Address**
  - Deactivate network id 0.
    - **AT+UWSCA=0,4**
  - Not Active on startup.
    - **AT+UWSC=0,0,0**
  - Enable DHCP Client.
    - **AT+UWSC=0,100,2**
    -
- **Wi-Fi part**
  - Set the Network SSID to connect to.
    - **AT+UWSC=0,2,"UBXWifi"**
  - Use WPA2 as authentication type.
    - **AT+UWSC=0,5,2**
  - Use Password “my password”.
    - **AT+UWSC=0,8,"my password"**
  - Activate Wi-Fi Station configuration.
    - **AT+UWSCA=0,3**
    -
- **TCP and data part**
  - Connect to using TCP port on AP.
    - **AT+UDCP="tcp://192.168.2.1:8080"**

- **Enter Data Mode**
  - Enter Data Mode to send data.
    - **ATO1**

8.2 Use ODIN-W2 Wi-Fi Access Point and RMII interface

Wi-Fi Access Point + RMII (Ethernet)

- **Network part using Static for AP and DHCP for clients**
  - Deactivate network id 0.
    - **AT+UWAPCA=0,4**
  - Not active on startup.
    - **AT+UWAPC=0,0,0**
  - Set SSID for the Network.
    - **AT+UWAPC=0,2,”UBXWifi”**
  - Set Channel 1 for the Network.
    - **AT+UWAPC=0,4,1**
  - Set WPA2 Security for the Network.
    - **AT+UWAPC=0,5,2,2**
  - Use Password “**my password**"
    - **AT+UWAPC=0,8,”my password”**
  - Static IP address for Access Point.
    - **AT+UWAPC=0,100,1**
  - Network IP address.
    - **AT+UWAPC=0,101,192.168.0.10**
  - Network Subnet mask.
    - **AT+UWAPC=0,102,255.255.0.0**
  - Network Gateway address.

        - **AT+UWAPC=0,103,192.168.0.1**
    - Enable DHCP for connected Clients. DHCP Server will provide addresses according to the following formula: (Static address & subnet mask) + 100. The first client will get the IP address 192.168.0.100.
        - **AT+UWAPC=0,106,1**
    - Activate Wi-Fi Access Point configuration.
        - **AT+UWAPCA=0,3**
    - Disable interface if Active.
        - **AT+UETHCA=4**
    - Use RMII interface (Ethernet is default).
        - **AT+UETHC=1,0**
    - Use Static IP Address.
        - **AT+UETHC=100,1**
    - Use 192.168.0.101 as IP Address.
        - **AT+UETHC=101,192.168.0.20**
    - Use 255.255.0.0 as Subnet Mask.
        - **AT+UETHC=102,255.255.0.0**
    - Use 192.168.0.1 as Gateway.
        - **AT+UETHC=103,192.168.0.1**
    - Activate the RMII with the current settings.
        - **AT+UETHCA=3**
    - Enable Layer-2 Routing, this will enabled data on Wi-Fi be routed to and from the RMII (Ethernet) interface.
        - **AT+UNL2RCFG=0,1**

Now, the Wi-Fi Station clients can connect to the Access Point on ODIN-W2, and access devices connected to the RMII (Ethernet).

☞ The **AT+UNL2RCFG** for the Access Point setup has been replaced by the Bridge command **AT+UBRGC=0,1,1,2** and **AT+UBRGC=0,2,1,2** from software version 3.0.0 onwards. The **AT+UNL2RCFG** will be available in software 3.0.0 for backwards compatibility reasons with the same functionality as the Bridge command.

☞ Ethernet and Wi-Fi Interfaces are not used when WEA is active.

8.3 Connect ODIN-W2 using PPP and incoming Bluetooth SPP

- **Setup PPP Mode**
    - PPP Network IP address for the client.
        - **AT+UPPPC=101,172.30.0.252**
    - PPP Network Subnet mask for the client.
        - **AT+UPPPC=102,255.255.255.0**
        -
    - Enter PPP Mode.
        - **ATO3**
        -
    - Make sure the Serial Port in your software is closed.
    - Connect the Dial up Modem that supports PPP Client.
    - Ping the Address 172.30.0.251 that ODIN-W2 has received from another device on the same network.

Use a UDP connection to 172.30.0.251 on port 23 to send and receive AT commands.

- Example using Netcat: **nc –u –c 172.30.0.251 23**
- https://en.wikipedia.org/wiki/Netcat
- Setup a Bluetooth SPP connection on other device, ie. Incoming SPP connection on the PPP device
    - Connect to device using SPP from other Bluetooth device.
        - **AT+UDCP="spp://112233445566"**
        -
- Wait for the event Remote Service Connected +UUDRSC.
    - **+UUDRSC:1,"udp://0.0.0.0:1000","spp://11223345566"**

The **udp://0.0.0.0:1000** shows that it is an UDP connection is used, and it is not bonded to any specific address, and that the port 1000 is used. Now the application can connect on UDP port 1000 to send and receive SPP data.

8.4 Use AT commands over RMII on ODIN-W2

☞ Before doing the following setup, make sure the ODIN-W2 is connected to another RMII interface or a compatible PHY Hardware.

- Disable interface if Active.
    - **AT+UETHCA=4**
- Use Static IP Address.
    - **AT+UETHC=100,1**
- Use 192.168.0.101 as IP Address.
    - **AT+UETHC=101,192.168.0.101**
- Use 255.255.0.0 as Subnet Mask.
    - **AT+UETHC=102,255.255.0.0**
- Use 192.168.0.1 as Gateway.
    - **AT+UETHC=103,192.168.0.1**
- Use RMII interface.
    - **AT+UETHC=1,0**
- Activate the RMII settings.
    - **AT+UETHCA=3**
- Enable AT Commands on UDP Port 23.
    - **AT+UDSC=1,8,2,23**

Send a Ping to 192.168.0.101 from another device on the same network, to test that the module responses.

- Example using Ping: **ping 192.168.0.101**

```
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Now you can make a UDP connection on port 23 and send and receive AT Commands.

- Example using Netcat: nc –u –c 192.168.0.101 23
- https://en.wikipedia.org/wiki/Netcat

Send **AT+UWSCAN** to make a Wi-Fi Scan, and send **AT+UBTI** to make a Bluetooth Inquiry executed on the remote device.

8.5 Send data from UART to RMII on ODIN-W2

☞ Before doing the following setup, make sure the ODIN-W2 is connected to another RMII interface or a compatible PHY Hardware.

- Disable interface if Active.
  - **AT+UETHCA=4**
- Use Static IP Address.
  - **AT+UETHC=100,1**
- Use 192.168.0.101 as IP Address.
  - **AT+UETHC=101,192.168.0.101**
- Use 255.255.0.0 as Subnet Mask.
  - **AT+UETHC=102,255.255.0.0**
- Use 192.168.0.1 as Gateway.
  - **AT+UETHC=103,192.168.0.1**
- Use RMII interface.
  - **AT+UETHC=1,0**
- Activate the RMII settings.
  - **AT+UETHCA=3**
- Enable TCP Port 23
  - **AT+UDSC=1,1,23**
- Enter Data Mode to send data.
  - **ATO1**

Now you can make a TCP connection on port 23 and send and the data will be sent to the UART.

- Example using Netcat: **nc -c 192.168.0.101 23**
- https://en.wikipedia.org/wiki/Netcat

8.6 Bluetooth low energy SPS that connects automatically - initiated by central

To set up first ODIN-W2 as a Central (Device A)

- Enable Central Role.
  - **AT+UBTLE=1**
- Store configuration.
  - **AT&W**
- Restart ODIN-W2.
  - **AT+CPWROFF**
- Default peer using Serial Port Service and always connected (use Device B Address).
  - **AT+UDDRP=1,sps://112233445566p,2**
- Startup ODIN-W2 in data mode.
  - **AT+UMSM=1**
- Store configuration.
  - **AT&W**
- Restart ODIN-W2.
  - **AT+CPWROFF**

To set up second ODIN-W2 a Peripheral (Device B)

- Enable Peripheral Role.
  - **AT+UBTLE=2**
- Store configuration.
  - **AT&W**

- Restart ODIN-W2.
  - **AT+CPWROFF**
- Set server configuration id 1 to Serial Port Service.
  - **AT+UDSC=1,6**
- Startup ODIN-W2 in data mode.
  - **AT+UMSM=1**
- Store configuration.
  - **AT&W**
- Restart.
  - **AT+CPWROFF**

8.7 Bluetooth low energy SPS that connects automatically - initiated by peripheral

To set up first ODIN-W2 as a Central (Device A)

- Enable Central Role.
  - **AT+UBTLE=1**
- Store configuration.
  - **AT&W**
- Restart ODIN-W2.
  - **AT+CPWROFF**
- Set server configuration id 1 to Serial Port Service.
  - **AT+UDSC=1,6**
- Startup ODIN-W2 in data mode.
  - **AT+UMSM=1**
- Store configuration.
  - **AT&W**
- Restart ODIN-W2.
  - **AT+CPWROFF**

To set up second ODIN-W2 a Peripheral (Device B)

- Enable Peripheral Role.
  - **AT+UBTLE=2**
- Store configuration.
  - **AT&W**
- Restart ODIN-W2.
  - **AT+CPWROFF**
- Default peer using Serial Port Service and always connected.
  - **AT+UDDRP=1,sps://112233445566,2**
- Startup ODIN-W2 in data mode.
  - **AT+UMSM=1**
- Store configuration.
  - **AT&W**
- Restart.
  - **AT+CPWROFF**

9 Use case examples - Software 3.0.0

9.1 Wireless Ethernet

The Wireless Ethernet is a feature in ODIN-W2 that bridges the Ethernet and Wi-Fi interfaces at Layer-2 and enables any host with Ethernet (or RMII) interface to be connected to a Wi-Fi Network.

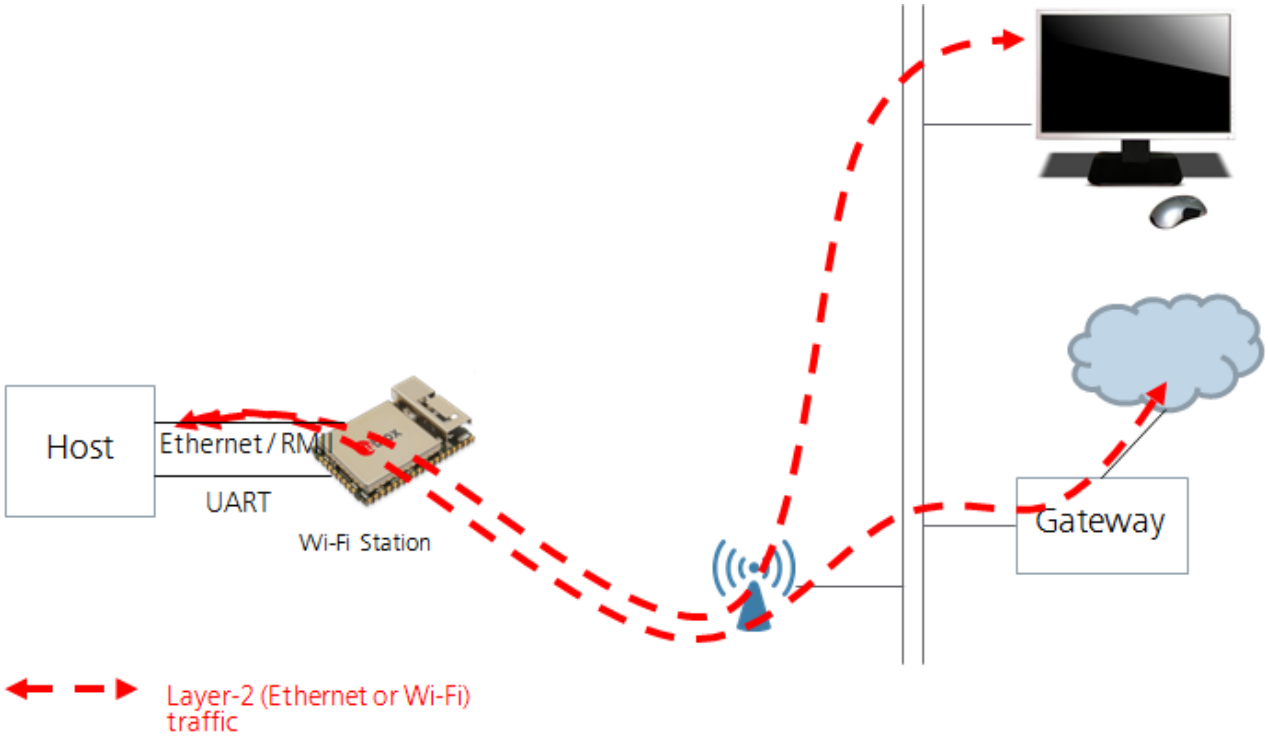

Figure 15: Configuration for Wireless Ethernet

9.1.1 Bridge between Ethernet and Wi-Fi Station

This example will configure the ODIN-W2 to route all Layer-2 traffic between Wi-Fi Station interface and the Ethernet interface. Due to limitation of the Wi-Fi technology, it is required to use the host Ethernet MAC address on the Wi-Fi interface. Restart the ODIN-W2 after changing the MAC address.

- Change the MAC address for the Wi-Fi interface:
  - **AT+UMLA=2,112233AABBCC**
- Store configuration:
  - **AT&W**
- Restart:
  - **AT+CPWROFF**

Bridge configuration

- Enable bridging between 1: Wi-Fi Station and 3: Ethernet interface
  - **AT+UBRGC=0,1,1,3**
- Active on startup
  - **AT+UBRGC=0,0,1**
- Store configuration
  - **AT+UBRGCA=0,1**
- Activate the bridge configuration
  - **AT+UBRGCA=0,3**

Ethernet configuration

- Active on startup
  - **AT+UETHC=0,1**
- Store configuration
  - **AT+UETHCA=1**
- Activate the Ethernet configuration with default values
  - **AT+UETHCA=3**
- Connect Ethernet cable and wait for interface to go up
  - **+UUETHLU**

Wi-Fi Station configuration

- Configure SSID
  - **AT+UWSC=0,2,"my_SSID"**
- Configure security (Open)
  - **AT+UWSC=0,5,1**
- Active on startup
  - **AT+UWSC=0,0,1**
- Store configuration
  - **AT+UWSCA=0,1**
- Activate the Wi-Fi Station.
  - **AT+UWSCA=0,3**
    -
- Wait for Wi-Fi interface to connect.
  - **+UUWLE:0,D0C2823A1650,11**

If a PC is used as a host, it may be necessary to disable the Autonegotiation, AT+UETHC=4,0 (or connect with a switch).

9.1.2 Bridge between Ethernet and Wi-Fi Access Point

This example will configure ODIN-W2, to route all Layer-2 traffic between the Wi-Fi Access Point interface and the Ethernet interface. In this example, it is expected that a DHCP server is active on the network. How to enable the DHCP server in ODIN-W2 is explained in section 8.1.

Bridge configuration

- Enable bridging between 1: Wi-Fi Station and 3: Ethernet interface
  - **AT+UBRGC=0,1,1,3**
- Active on startup
  - **AT+UBRGC=0,0,1**
- Store configuration
  - **AT+UBRGCA=0,1**
- Activate the bridge configuration
  - **AT+UBRGCA=0,3**

Ethernet configuration

- Active on startup
  - **AT+UETHC=0,1**
- Store configuration
  - **AT+UETHCA=1**
- Activate the Ethernet configuration with default values
  - **AT+UETHCA=3**
- Connect Ethernet cable and wait for interface to go up
  - **+UUETHLU**

Wi-Fi Access Point configuration

- Configure Wi-Fi Access Point, in this case and with no security and SSID set to “my_SSID”.
  - **AT+UWAPC=0,2,"my_SSID"**
  - **AT+UWAPC=0,4,1**
  - **AT+UWAPC=0,5,1,1**

- Active on startup
  - **AT+UWAPC=0,0,1**
- Store configuration
  - **AT+UWAPCA=0,1**
- Activate the Wi-Fi configuration.
  - **AT+UWAPCA=0,3**
- Wait for Wi-Fi Access Point interface to be enabled. After this event has been received, the AP is ready and stations can connect.
  - **+UUWAPU:0**

9.2 GATT Client between two ODIN-W2 modules

The Generic Attributes (GATT) is used when Bluetooth low energy devices exchanges data. There are two roles defined in GATT - the Client and Server; for more information about GATT see [5].

The following example shows how to read the manufacturer information via GATT from a remote Bluetooth device (in this case another ODIN-W2). The ODIN-W2 is configured as Central and acts as the GATT Client. The remote device is in Peripheral mode and acts as the GATT Server.

☞ The ODIN-W2 can act as GATT client irrespective of being in the Central or Peripheral mode.

Set up one ODIN-W2 as a Peripheral (by default a GATT Server is available)

- Enable Peripheral Role
  - **AT+UBTLE=2**
- Change name that is easy to find (optional)
  - **AT+UBTLN="ODIN-W2 GATT Server"**
- Store configuration
  - **AT&W**
- Restart
  - **AT+CPWROFF**

Set up another ODIN-W2 as a Central

- Enable Central Role
  - **AT+UBTLE=1**
- Store configuration
  - **AT&W**
- Restart
  - **AT+CPWROFF**

Discover remote device and connect

- Find the other device
  - **AT+UBTD=4,1**
    +UBTD:8C8B83ED94B9p,-55,"ODIN-W2 GATT Server",1,14094F44494573...
- Create an ACL Connection, a low level Bluetooth connection without any profiles or other protocols.
  - **AT+UBTACLC=8C8B83ED94B9p**
    +UUBTACLC:0,0,8C8B83ED94B9p

Use the GATT Client to Discover Services

- Use the connection handle 0 from the **+UUBTACLC** and Discover Services.
  - **AT+UBTGDP=0**
    +UBTGDP:0,1,4,1801
    +UBTGDP:0,5,11,1800
    +UBTGDP:0,12,18,01D7E9014FF344E7838FE226B9E15624
    +UBTGDP:0,19,27,180A
    OK

- In this case, attempt is made to read the “Manufacturer Name String”, that is a part of the “Device Information Service” **180A**; see [6] for a complete list of GATT Services.

☞ The Service **01D7E9014FF344E7838FE226B9E15624** shows the u-blox serial port service. The **1800** is the Generic Access services, and the **1801** is the Generic Attribute Service. More information about the GATT Services can be found here [6].

- After finding the “Device Information Service”, use the start handle **19** and end handle **27** from the **+UBTGDP**, and make a “Discover all Characteristics” of service using **AT+UBTGDCS=0,19,27** command.
  - **AT+UBTGDCS=0,19,27**

    +UBTGDCS:0,20,02,21,2A29
    +UBTGDCS:0,22,02,23,2A24
    +UBTGDCS:0,24,02,25,2A26
    +UBTGDCS:0,26,02,27,2A28
    OK
- To find the manufacturer, we look for the Characteristics **2A29**, that is the “Manufacturer Name String”; for a complete list of GATT Characteristics see [7].

- Use the handle **21** from the **+UBTGDCS** and make a Read Characteristic using **AT+UBTGR**
  - **AT+UBTGR=0,21**
  - **+UBTGR:0,21,752D626C6F78**
  - **OK**

- The response from **+UBTGR** will now include the “Manufacturer Name String”. The result is the manufacturer; **752D626C6F78** in HEX-format.

☞ To use the manufacturer name string, it must be converted to ASCII-format. In the above-mentioned example, the manufacturer will be **“u-blox”** on conversion.

Appendix

A Glossary

Abbreviation	Definition
ACL	Asynchronous Connection-Less
AP	Access Point
ATEX	Equipment for potentially explosive atmospheres
DHCP	Dynamic Host Configuration Protocol
DTR	Data Terminal Ready
EDM	Extended Data Mode
GATT	Generic Attributes
HTTP	Hypertext Transfer Protocol
LED	Light-Emitting Diode
PPP	Point-to-Point Protocol
PHY	Ethernet Physical Transceiver
RMII	Reduced Media Independent Interface
RSSI	Received signal strength indication
SPP	Serial Port Profile
SPS	Serial Port Service
SSID	Service Set Identifier
TCP	Transmission Control Protocol
UDCP	Universal Dispenser Communication Protocol
UDDRP	Uniform Domain Dispute Resolution Policy
UDP	User Datagram Protocol
URL	Uniform Resource Locator
WEA	Wireless Ethernet Adapter

Table 2: Explanation of the abbreviations and terms used

Related documents

[1] u-blox Short Range Modules AT Commands Manual, Document No. UBX-14044127
[2] u-blox Extended Data Mode Protocol Specification, Document No. UBX-14044126
[3] ODIN-W2 series Data Sheet, Document No. UBX-14039949
[4] EVK-W262U Quick Start Guide, Document No. UBX-15016340
[5] https://www.bluetooth.com/specifications/generic-attributes-overview
[6] https://www.bluetooth.com/specifications/gatt/services
[7] https://www.bluetooth.com/specifications/gatt/characteristics

☞ For regular updates to u-blox documentation and to receive product change notifications, register on our homepage (www.u-blox.com).

Revision history

Revision	Date	Name	Comments
R01	01-Jun-2015	cmag	Initial release.
R02	25-Sep-2015	cmag, kgom	Major content updates. Applied u-blox template.
R03	21-Jun-2016	cmag, kgom	Modified the document status to Early Production Information. Fixed the typo AT+UNC as AT+UWSC. Fixed the error in some AT commands. Added chapter about TCP Listener and Static IP address. Removed Classic from Bluetooth Classic as per new Bluetooth SIG brand rules. Updated this document with Firmware 2.0.0 features such as Access Point, PPP, and RMII. Included information about Firmware 2.0.1 on page 2. Classified the use case examples for Firmware 1.0.0 (section 7) and Firmware 2.0.0 (section 8).
R04	04-Oct-2016	cmag, pber, kgom	Updated this document with Firmware 3.0.0 features such as WEA and GATT Client (section 9). Included “Bluetooth Low Energy SPS that connects automatically - initiated by Peripheral" (section 8.7). Modified Power save (section 5.6). Updated section 7.4 in the Use case examples - Firmware 1.0.0. Updated sections 8.2, 8.4 and 8.6 in Use case examples - Firmware 2.0.0
R05	3-Jan-2017	kgom	Included support for ODIN-W2 firmware versions – 2.0.2 and 3.0.1. On page 2, replaced Document status with Disclosure restriction.
R06	30-Mar-2017	kgom	Included support for ODIN-W2 firmware version – 4.0.0 on page 2.
R07	16-Aug-2017	kgom	Included support for ODIN-W2 software version 4.0.1. Replaced firmware with software.
R08	11-Jun-2018	cmag, kgom	After fixing a typo (replaced “AT+UDPC” with “AT+UDCP”).

Contact

For complete contact information, visit us at www.u-blox.com.

u-blox Offices

North, Central and South America

u-blox America, Inc.

Phone: +1 703 483 3180
E-mail: info_us@u-blox.com

Regional Office West Coast:

Phone: +1 408 573 3640
E-mail: info_us@u-blox.com

Technical Support:

Phone: +1 703 483 3185
E-mail: support@u-blox.com

Headquarters
Europe, Middle East, Africa

u-blox AG

Phone: +41 44 722 74 44
E-mail: info@u-blox.com
Support: support@u-blox.com

Asia, Australia, Pacific

u-blox Singapore Pte. Ltd.

Phone: +65 6734 3811
E-mail: info_ap@u-blox.com
Support: support_ap@u-blox.com

Regional Office Australia:

Phone: +61 2 8448 2016
E-mail: info_anz@u-blox.com
Support: support_ap@u-blox.com

Regional Office China (Beijing):

Phone: +86 10 68 133 545
E-mail: info_cn@u-blox.com
Support: support_cn@u-blox.com

Regional Office China (Chongqing):

Phone: +86 23 6815 1588
E-mail: info_cn@u-blox.com
Support: support_cn@u-blox.com

Regional Office China (Shanghai):

Phone: +86 21 6090 4832
E-mail: info_cn@u-blox.com
Support: support_cn@u-blox.com

Regional Office China (Shenzhen):

Phone: +86 755 8627 1083
E-mail: info_cn@u-blox.com
Support: support_cn@u-blox.com

Regional Office India:

Phone: +91 80 405 092 00
E-mail: info_in@u-blox.com
Support: support_in@u-blox.com

Regional Office Japan (Osaka):

Phone: +81 6 6941 3660
E-mail: info_jp@u-blox.com
Support: support_jp@u-blox.com

Regional Office Japan (Tokyo):

Phone: +81 3 5775 3850
E-mail: info_jp@u-blox.com
Support: support_jp@u-blox.com

Regional Office Korea:

Phone: +82 2 542 0861
E-mail: info_kr@u-blox.com
Support: support_kr@u-blox.com

Regional Office Taiwan:

Phone: +886 2 2657 1090
E-mail: info_tw@u-blox.com
Support: support_tw@u-blox.com