AT Commands

This document describes how to use AT commands in RA6W1, RRQ61001 , RA6W2, and RRQ61051 MCU and SoM devices. Unless otherwise specified, the term RA6W1 used throughout this document collectively refers to RA6W1/RA6W2/RRQ61001/RRQ61051.

Contents

1. Introduction **6**
1.1 AT Command Type 6
1.1.1 Basic Commands 6
1.1.2 Extended Commands 6
1.1.3 Responses 7
2. AT Command Sets **8**
2.1 Basic Function Commands 8
2.2 Network Function Commands 13
2.3 Wi-Fi Function Commands 19
2.4 Wi-Fi Function Commands for WPA3 37
2.5 Wi-Fi Function Commands for WPA-Enterprise 40
2.5.1 WPA-Enterprise Connection Example 41
2.6 Advanced Function Commands 42
2.6.1 MQTT Commands 42
2.6.2 HTTP-Client Commands 61
2.6.3 HTTP-Server Commands 65
2.6.4 WebSocket-Client Commands 66
2.6.5 OTA Commands 66
2.6.6 Transfer Function Commands 75
2.6.7 Power Manager Commands 84
2.7 Bluetooth® LE Commands 89
2.8 RF Test Function Commands 96
2.9 Matter Commands 99
2.10 LittleFS Commands 102
3. AT Command Examples **103**
3.1 Data Transfer Test 103
3.1.1 TCP Server Socket Test 103
3.1.2 TCP Client Socket Test 104
3.1.3 UDP Socket Test 104
Appendix A License Information **106**
Appendix B HTTP Client Result Codes **107**
Appendix C Fast-Reconnect on Sleep Mode 2 ..... **108**
C.1 Technical Overview 108
C.1.1 Direct Probe Request for Wi-Fi Scan 108

© 2026 Renesas Electronics

C.1.2 Network Address without DHCP Client Procedure 108
Appendix D RA6W1 Cipher Suites 109
Appendix E Reason Code for Wi-Fi Connection Failure or Disconnection 111
Appendix F Detailed Error Codes for AT Commands 113
Appendix G RA6W1 vs DA16200 AT Command Response 124
Appendix H Wi-Fi RF Parameters 129
Appendix I Special Characters Support in SSID or PSK 130
4. Revision History 131

Figures

Figure 1. Broker console – CleanSession=1 connection 56
Figure 2. Broker console – CleanSession=0 connection 56
Figure 3. IO Ninja – TCP client socket setting 103
Figure 4. IO Ninja – TCP server socket setting 104
Figure 5. IO Ninja – UDP socket setting 105

Tables

Table 1. Basic function command list 8
Table 2. Initiation response list 13
Table 3. Network function command list 13
Table 4. Certificate command 19
Table 5. Wi-Fi function command list 19
Table 6. Wi-Fi function response list 36
Table 7. List of WPA3-relevant Wi-Fi function commands 38
Table 8. WPA-enterprise Wi-Fi function commands 40
Table 9. MQTT configuration command list 42
Table 10. MQTT operation command list 49
Table 11. MQTT optional configuration commands 52
Table 12. MQTT response list 53
Table 13. CleanSession and QoS matrix in message RX 57
Table 14. CleanSession and QoS matrix in message TX 58
Table 15. HTTP-client command list 61
Table 16. HTTP-client response list 63
Table 17. HTTP-server command list 65
Table 18. WebSocket-client command list 66
Table 19. WebSocket-client response list 66
Table 20. OTA command list 66
Table 21. OTA response list 72
Table 22. OTA response code list 72
Table 23. Socket command list 75
Table 24. Socket connection response list 78
Table 25. Data transmission command 78
Table 26. Data reception responses 80
Table 27. Secure socket command list 80
Table 28. Secure socket response list 84
Table 29. Power manager command list 84
Table 30. Bluetooth LE commands list 90
Table 31. RF test command list 96
Table 32. AT commands from MCU TO RA6W2 99

Table 33. AT commands from RA6W2 to MCU 100
Table 34. LittleFS Command list 102
Table 35. HTTP client result codes 107
Table 36. RA6W1 cipher suites 109
Table 37. Common AT command error codes 113
Table 38. Flash AT command error codes 113
Table 39. NVRAM AT command error codes 113
Table 40. Basic AT command error codes 114
Table 41. UART AT command error codes 114
Table 42. PMGR AT command error codes 114
Table 43. Wi-Fi AT command error codes 114
Table 44. CLI AT command error codes 117
Table 45. Network basic AT command error codes 118
Table 46. DHCP Client AT command error codes 118
Table 47. DHCP Server AT command error codes 118
Table 48. SNTP Client AT command error codes 119
Table 49. MQTT Client AT command error codes 119
Table 50. MQTT Broker AT command error codes 119
Table 51. MQTT TLS AT command error codes 119
Table 52. MQTT Sub-Topic AT command error codes 120
Table 53. MQTT Pub-Topic AT command error codes 120
Table 54. MQTT WILL Message AT command error codes 120
Table 55. MQTT Common AT command error codes 120
Table 56. HTTP(s) Server AT command error codes 121
Table 57. HTTP(s) Client AT command error codes 121
Table 58. Web-Socket Client AT command error codes 121
Table 59. Certificate AT command error codes 121
Table 60. Transport Function (TCP/UDP) AT command error codes 121
Table 61. SSL/TLS AT command error codes 122
Table 62. SSL Certificate AT command error codes 123
Table 63. The differences in AT Command Response between RA6W1 and DA16200 124
Table 64. TX rate and TX power descriptions for Wi-Fi 129

Terms and Definitions

AP	Access Point
ASCII	American Standard Code for Information Interchange
AT	Attention
Bluetooth LE	Bluetooth® Low Energy
CA	Certificate Authority
CCMP	Counter Mode Cipher Block Chaining Message Authentication Code Protocol
CID	Client ID
CMD	Command
COM	Communication Port
CRC	Cyclic Redundancy Check
CW	Continuous Wave
DHCP	Dynamic Host Configuration Protocol
DPM	Dynamic Power Management
EAP	Extensible Authentication Protocol
ESS	Extended Service Set
GPIO	General Purpose Input Output
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
JSON	JavaScript Object Notation
LMAC	Low MAC
MAC	Medium Access Control
MCU	Microcontroller Unit
MQTT	Message Queuing Telemetry Transport
MQTTC	MQTT Client
NVRAM	Non-Volatile RAM
OTA	Over the Air
OTP	One-Time Programmable
OWE	Opportunistic Wireless Encryption
PBC	Push Button Connection
PER	Packet Error Rate
PMGR	Power Manager
PSK	Pre-Shared Key
QoS	Quality of Service
RAM	Random Access Memory
RTC	Real-Time Clock

RTOS	Real-Time Operating System
RTS	Request to Send
RX	Receive
SAE	Simultaneous Authentication of Equals
SDK	Software Development Kit
SDIO	Secure Digital Input Output
SNTP	Simple Network Time Protocol
SoM	System on Module
SPI	Serial Peripheral Interface
SSID	Service Set Identifier
STA	Station
TCP	Transport Control Protocol
TIM	Traffic Indication Map
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TX	Transmit
TWT	Target Wake Time
UART	Universal Asynchronous Receiver-Transmitter
UDP	User Datagram Protocol
USB	Universal Serial Bus
URL	Universal Resource Locator
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WMM	Wi-Fi Multimedia
WPA	Wi-Fi Protected Access version 1
WPA2	Wi-Fi Protected Access version 2
WPS	Wi-Fi Protected Setup
XTAL	Crystal Oscillator

1. Introduction

The RA6W1 can be configured and controlled through an ASCII based command string called AT Command. Originally defined by the modem maker Hayes, AT commands, the "AT" stands for "come to attention" are a universal instruction standard for controlling smart modems and are widely used in various products.
AT command has a very simple structure consisting of a prefix "AT" concatenated with a command string. This is a very convenient method for sending a series of commands over a serial interface such as UART. Commands consist of capital letters, lowercase letters, spaces, and some special characters.
For AT command UART configurations, RA6W1 binaries, and bring up, see *RA6W1/RRQ61001 Quick Start Guide*.
Usually AT command is enabled by default in the SDK. If you want to disable the command, see *RA6W1/RRQ61001 Quick Start Guide*.

1.1 AT Command Type

AT commands can be classified into three sets: Basic commands, Extended commands, and Response commands. Commands and parameters are not case sensitive.

1.1.1 Basic Commands

Basic commands consist of **Set** commands and **Get** commands.

- **Set** commands used to set parameters or execute commands. Command format is `ATXX`:
  - Example command: `ATZ`
  - Example response: `OK`
- **Get** commands used to query parameters or get status of the commands. Command format is `ATXX=?`:
  - Example command: `ATQ=?`
  - Example response: `OK`

1.1.2 Extended Commands

1.1.2.1 Set Commands

Set commands set parameters or execute commands with additional parameters.
Command format: AT+XXX=<param1>,<param2>,<param3>,<param4>…<paramN>

- Example command: `AT+NWIP=0,172.16.0.100,255.255.255.0,172.16.0.1`
- Example response: **OK**

If the SSID contains a comma or single quote, the SSID must be enclosed in single quotes.
Example:

```
SSID = MY,SSID'CS
sec = 4
idx = 2
Password = N12345678
```

Is encoded as:

```
AT+WFJAP='MY,SSID'CS',4,2,N12345678'
OK
```

1.1.2.2 Get Commands

Get commands query parameters or get status of the commands with additional parameters.
Command format: AT+XXX=?

- Example command: `AT+NWIP=?`
- Example response:

```
+NWIP:172.16.0.17,255.255.255.0,172.16.0.1
OK
```

NOTE

Not all commands support the AT+XXX=? query function. Some commands such as AT+RESTART and ATF do not require the query function. Check the command table for the valid operation of each command.

1.1.3 Responses

- **Startup** response - this code is received when RA6W1 is rebooted.

```
<CR><LF>+INIT:DONE,<mode><CR><LF>
```

- **Normal** response - this code is received for normal operation.

```
<CR><LF>OK<CR><LF>
```

- **Error** response - this code is received when an operation fails for some reason.

```
<CR><LF>ERROR:<error code><CR><LF>
```

- **Extended** response - this code is received in basic response format along with the command setting values.

```
<CR><LF>+XXX:[value1],[value2],…
<CR><LF>OK<CR><LF>
```

NOTE

When an MCU (AT Command Host) waits for a response of a command (for those commands that give extended response) to take the next action, it should wait for both normal response (**OK** or **ERROR**) and extended response (also known as **Operation Result**).

For error response codes, see Appendix F Detailed Error Codes for AT Commands.

2. AT Command Sets

AT commands can be used in various Wi-Fi configurations as well as other network configurations. The following tables provide a brief description of each functionality and its sample configuration.

2.1 Basic Function Commands

Table 1. Basic function command list

Command	Parameters	Description
?	(none)	Show the usage of AT commands.
	Example AT Commands: ? - Question mark shows a list of AT commands, and their usage enabled in a particular build. HELP=<command> - Print help message AT - Attention command AT+ - List available commands ATZ - Initialize AT commands ATF - Restore to Factory mode (NVRAM clean) ATE - Command echo ATQ - Result Codes On/Off AT+RESTART - System restart --- Middle omission --- AT+TRSAVE - Save status of all sessions === User AT Command ====== OK	

Command	Parameters	Description
HELP	<cmd_name>	AT command name to query the use of commands.
	(none)	Same as the "?" command.
	Example HELP AT Commands: ? - Commands list with brief and usage HELP=<command> - Print help message AT - Attention command AT+ - List available commands ATZ - Initialize AT commands ATF - Restore to Factory mode (NVRAM clean) ATE - Command echo ATQ - Result Codes On/Off AT+RESTART - System restart … --- Middle omission --- OK HELP=ATE ATE - Command echo OK	
AT+	(none)	Show a list of AT commands.
	Example AT+ AT AT+ ATZ ATF ATE ATQ AT+RESTART --- Middle omission --- AT+TRSAVE OK	
ATZ	(none)	Initialize AT commands.
	Example ATZ Display result on Echo off OK	
ATF	(none)	RA6W1 factory reset. Response: "+INIT:DONE,0" Note: All NVRAM parameters that include Wi-Fi profile (Soft AP or STA)

Command	Parameters	Description
		settings are removed, DUT restarts, and "+INIT:DONE,0" is received.
	Example ATF +INIT:DONE,0	
ATE	(none)	ECHO on/off.
	?	Show Echo status – on/off.
	Example ATE Echo on OK ATE Echo off OK ATE=? Echo on OK	
ATQ	(none)	Turn on/off to display the result code.
	?	Show the status whether to display result codes.
	Example ATQ Display results off ATQ=? Display result on OK	
ATB	<baudrate> [[,<databits>] [,<parity>] [,<stopbits>] [,<persistence>]]	Set UART parameters (the main purpose is to change baud rate) <baudrate>: 9600/19200/38400/57600/115200/230400/460800/921600 <databits>: [optional], 5/6/7/8 (Default) <parity>: [optional], n (None, Default)/e (Even)/o (Odd) <stopbits>: [optional], 1 (Default)2 <persistence>:[optional], 0(Default, Do NOT store UART settings into NVRAM) 1 (Store UART settings into NVRAM)
	Example: Case 1) Update baud rate and store the updated value in persistent area. ATB=230400 OK Case 2) Update baud rate but do NOT store the updated value in persistent area. ATB=230400,0 OK Case 3) Update baud rate and store the updated value in persistent area. ATB=230400,1 OK Case 4) Update UART settings and store the updated value in persistent area. ATB=230400,8,n,1 OK Case 5) Update UART settings but do NOT store and the updated value in persistent area. ATB=230400,8,n,1,0 OK	

Command	Parameters	Description
	Case 6) Update UART settings and store and the updated value in persistent area. ATB=230400,8,n,1,1 OK	
AT+RESTART	(none)	System restart.
	Example AT+RESTART OK +INIT:DONE,0	
AT+CHIPNAME	(none)	Get a chip name, RA6W1 or RA6W2.
	Example AT+CHIPNAME +CHIPNAME:RA6W1-RRQ61001 OK	
AT+VER	(none)	Get version information. Response: +VER:<main version>
	Example AT+VER +VER:GEN01-01-a05c53e68e-001945 OK	
AT+SDKVER	(none)	Get the SDK version information. Response: +SDKVER:<major>.<minor >.<revision>.<eng_number> ■ <major>: SDK major number ■ <minor>: SDK minor number ■ <revision>: SDK Revision number ■ <eng_number>: SDK engineering number
	Example AT+SDKVER +SDKVER:6.0.0.0 OK	
AT+TIME	<date>,<time>	Set the current time. <date>: yyyy-mm-dd <time>: hh:mm:ss Response: OK or ERROR
	?	Get the current time. Response: +TIME:<yyyy-mm-dd> <hh:mm:ss>
	Example AT+TIME=2021-07-15,16:14:30 OK AT+TIME=? +TIME:2021-07-15,16:14:32 OK	
AT+RLT	(none)	Get system running time. Response: +RLT:<days>,<hh:mm.ss>
	Example AT+RLT +RLT:0,01:06.18 OK	
AT+TZONE	<sec>	GMT time zone setting (-43200 ~ 43200).

Command	Parameters	Description
		<sec>: Time zone setting parameter Response: OK or ERROR Note: The <sec> parameter must be a multiple of 60 seconds. If the value for <sec> is not a multiple of 60 seconds, then the remainder is discarded.
	?	Get GMT time zone parameter. Response: +TZONE:<sec>
	Example AT+TZONE=? +TZONE:0 OK AT+TZONE=32400 OK AT+TZONE=? +TZONE:32400 OK	
AT+GETNVRWIFIPF	(none)	Get wifiprofile stored in NVRAM in the specified format. If <name>:<data> appears multiple times, they are separated by commas. The last <name>:<data> has no comma. Response:+GETNVRWIFIPF:<Tag_Name>:<Data>,<Tag_ Name>:<Data>
	AT+GETNVRWIFIPF +GETNVRWIFIPF:country_code:KR,sysmode:0,band:2,channel:6... OK	
AT+DEFAP	(none)	All profiles in NVRAM are removed and set up in Soft AP mode with the default configuration. To initialize the Soft AP interface, the system reboots automatically. Response: OK or ERROR (reboot)
	Example AT+DEFAP OK +INIT:DONE,1 Note: ■ Default configuration: ■ SSID: RA6W1_ XXXXXX (for example, 9FFCF3: the last three hexadecimal values of the board's MAC address) ■ Authentication: WPA2/CCMP ■ IP address: 10.0.0.1 ■ Netmask: 255.255.255.0 ■ Gateway: 10.0.0.1 ■ PSK: 12345678 ■ DHCP server started ■ DHCP range: 10.0.0.2 ~ 10.0.0.11 ■ DHCP DNS: 8.8.8.8 ■ To query the configuration status, use AT+WFSAP and/or AT+NWDHR.	
AT+DEFCCRNT	(none)	All profiles in NVRAM are removed and set up Concurrent mode: Soft AP + STA with the default configuration. To initialize the Concurrent interfaces, the system reboots automatically. Response: OK or ERROR (reboot)
	Example AT+ DEFCCRNT AT+WFJAP=AP_24G,4,2,12345678	

Command	Parameters	Description
	Note: ■ AT+ DEFCCRNT sets AT+DEFAP, AT+WFMODE=4, and AT+RESTART. To complete the process and connect the STA, "AT+WFJAP" should be used.	
AT+HOSTINITDONE	(none)	
	Example AT+HOSTINITDONE +INIT:DONE,0	

Table 2. Initiation response list

Response	Parameters	Description
+INIT	DONE,<mode>	The RA6W1 booting is complete. <mode>:0 (STA), 1 (Soft AP) Example: +INIT:DONE,0

2.2 Network Function Commands

Table 3. Network function command list

Command	Parameters	Description
AT+NWIP	<iface>,<ip_addr>,<netmask>,<gw>	Set the IP address. ■ <iface>: WLAN interface. 0 (WLAN0, STA), 1 (WLAN1, Soft AP) ■ <ip_addr>: IP Address ■ <netmask>: Subnet mask ■ <gw>: Gateway Response: OK or ERROR Note: ■ In Soft AP mode, after changing the IP address, DHCP server pool range must also be updated based on the class of the changed IP address. Use AT+NWDHR to redefine DHCP server pool range after running AT+NWIP. ■ In Soft AP mode, if the IP configuration is changed while the DHCP server is running, then the DHCP server must be restarted using the AT+RESTART or AT+NWDHS=0 > AT+NWDHS=1 command.
	?	Get the IP address of the current WLAN interface. Response: +NWIP: <iface>,<ip_addr>,<netmask>,<gw>
	(none)	
	Example AT+NWIP=0,192.168.0.100,255.255.255.0,192.168.0.1 OK AT+NWIP +NWIP:0,192.168.0.100,255.255.255.0,192.168.0.1 OK At+NWIP=? +NWIP:0,192.168.0.100,255.255.255.0,192.168.0.1 OK	
AT+NWDNS	<dns_ip>	Set the DNS server IP address of STA interface. <dns_ip>: DNS server IP address Response: OK or ERROR Note: ■ If AT+NWDNS=? is running under DHCP mode, it returns the DNS IP address from DHCP provision data regardless of any DNS IP address set with AT+NWDNS=<dns_ip>. ERROR: 0x500007 ("No result" or "Not configured") can be returned if there is no DHCP provision data existing. ■ If AT+NWDNS=? is running under Static IP mode, it returns the DNS IP address from AT+NWDNS=<dns_ip> that run previously.

Command	Parameters	Description
		■ Restart the system if AT+NWDNS=<dns_ip> is running under DHCP mode and it needs to apply the changes in Static IP mode.
	?	Get the DNS server IP address of STA interface. Response: +NWDNS:<dns_ip>
	(none)	
	Example AT+NWDNS=8.8.8.8 OK AT+NWDNS +NWDNS:8.8.8.8 OK	
AT+NWDNS2	<dns_ip>	Set the second DNS server IP address of STA interface. <dns_ip>: DNS server IP address Response: OK or ERROR
	?	Get the second DNS server IP address of STA interface. Response: +NWDNS2:<dns_ip>
	(none)	
	Example AT+NWDNS2=8.8.8.8 OK AT+NWDNS2 +NWDNS2:8.8.8.8 OK	
AT+NWHOST	<name>	Get the host IP address by name. <name>: Domain name Response: +NWHOST:<ip>
	Example AT+NWHOST=www.renesas.com +NWHOST:54.192.175.64 OK	
AT+NWPING	<iface>,<dst_ip>,<count>	Ping test. <iface>: WLAN interface. 0 (WLAN0), 1 (WLAN1) <dst_ip>: Target IP address <count>: The number of ICMP message transmissions. Response: +NWPING:<sent_count>,<recv_count>, <avg_time>,<min_time>,<max_time>
	Example AT+NWPING=0,192.168.0.1,4 +NWPING:4,4,0,0,0 OK	
AT+NWDHC	<dhcpc>	Start/Stop the DHCP client. <dhcpc>: 0 (stop), 1 (start) Response: OK or ERROR
	?	Get the DHCP client status. Response: +NWDHC:<dhcpc>
	(none)	
	Prerequisite The RA6W1 should be connected to AP. Example AT+NWDHC=1 OK AT+NWDHC +NWDHC:1 OK	

Command	Parameters	Description
AT+NWDHCHN	<hostname>	Save the DHCP client host-name. <hostname> DHCP client host-name Response: OK or ERROR Note: The hostname can contain only uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and minus sign (-).
	?	Get the DHCP client host-name which is stored by user. Response: +NWDHCHN=<hostname>
	(none)	
	Example AT+NWDHCHN=TEST_DHCP*HOSTNAME ERROR:0x500267 AT+NWDHCHN=TEST-DHCP-HOSTNAME OK	
AT+NWDHCHNDEL	(none)	Delete DHCP client host-name which was stored by user.
	Example AT+NWDHCHNDEL OK	
AT+NWDHR	<start_ip>,<end_ip>	Set an IP address range of the DHCP server. <start_ip>: Starting IP address assigned by the DHCP server. <end_ip>: Ending IP address assigned by the DHCP server. Response: OK or ERROR Note: Restart the DHCP server (AT+RESTART or AT+NWDHS=0 > AT+NWDHS=0) to apply the changes.
	?	Get an IP address range of the DHCP server. Response: +NWDHR:<start_ip>,<end_ip>
	(none)	
	Prerequisite Soft AP mode Example AT+NWDHR=10.0.0.2,10.0.0.11 OK AT+NWDHR +NWDHR:10.0.0.2,10.0.0.11 OK	
AT+NWDHLT	<lease_time>	Set an IP lease time (in seconds) of the DHCP server. <lease_time>: IP lease time (from 60 to 86400 seconds) Response: OK or ERROR Note: Restart the DHCP server (AT+RESTART or AT+NWDHS=0 > AT+NWDHS=1) to apply the changes.
	?	Get an IP lease time of the DHCP server. Response: +NWDHLT:<lease_time>
	(none)	
	Prerequisite Soft AP mode Example AT+NWDHLT=1800 OK AT+NWDHLT +NWDHLT:1800 OK	
AT+NWDHS	<dhcpd>	Start/Stop DHCP server. <dhcpd>: 0 (stop), 1 (start) Response: OK or ERROR
	<dhcpd>,<start_ip>,<end_	Start the DHCP server with options.

Command	Parameters	Description
	ip>,<lease_time>	■ <dhcpd>: 1 (start) ■ <start_ip>: Starting IP address for the DHCP client ■ <end_ip>: Ending IP address for the DHCP client ■ <lease_time>: IP lease time (optional, in second, default is 1800) Response: OK or ERROR
	?	Get the DHCP client status. Response: +NWDHS:<dhcpd>
	(none)	
	Prerequisite Soft AP mode Example AT+NWDHS=1 OK AT+NWDHS=1,10.0.0.2,10.0.0.10,1800 OK AT+NWDHS +NWDHS:1,10.0.0.2,10.0.0.10,1800 OK	
AT+NWDHIP	(none)	Show the information of the DHCP Client(s) connected. Response: OK or ERROR When the response is OK, the following response comes first before OK. +NWDHIP:<mac_addr_1>,<ip_addr_1>;<mac_addr_2>,<ip_addr_2>;…. Note: Use this command when DHCP server is running.

	Example
	// One DHCP client is in a connected state.
	AT+NWDHIP
	+NWDHIP:80:35:c1:79:c1:da,10.0.0.2
	OK
	// Two DHCP clients are in a connected state.
	AT+NWDHIP
	+NWDHIP:80:35:c1:79:c1:da,10.0.0.2;b4:f1:da:b4:27:11,10.0.0.3
	OK
	// No DHCP client exists.
	AT+NWDHIP
	ERROR: 5243502 // Clients are not connected.	

AT+NWSNS AT+NWSNS1 AT+NWSNS2	<server_ip>	Set the SNTP server IP address/domain name. <server_ip>: SNTP server IP address/domain name Response: OK or ERROR Note: ■ You can specify up to three SNTP servers; an SNTP server is contacted in a round robin manner if the RA6W1 fails to synchronize the system time with a server. ■ If not specified, the default SNTP server is used.
	?	Get the SNTP server IP address. Response: +NWSNS:<sntp>
	(none)	
	Example AT+NWSNS=8.8.8.8 OK AT+NWSNS +NWSNS:8.8.8.8 OK	
AT+NWSNUP	<period>	Set the SNTP client update period (in seconds). <period>: SNTP client update period (from 60 to 129600 seconds)

Command	Parameters	Description
		Response: OK or ERROR
	?	Get the SNTP client update period. Response: +NWSNUP:<period>
	(none)	
	Example AT+NWSNUP=86400 OK AT+NWSNUP +NWSNUP:86400 OK	
AT+NWSNTP AT+NWSNTP1 AT+NWSNTP2	<sntp>	Start/Stop the SNTP client. <sntp>: 0 (stop), 1 (start) Response: OK or ERROR Note: If <sntp> is 1, SNTP client is started immediately and tries to do time sync with the specified server. <sntp>=1 also enables "auto-start" of the SNTP client if the RA6W1 reboots. <sntp>=0 removes "auto-start" flag from NVRAM, so the RA6W1 does not try to sync the time when rebooted.
	<sntp>,<server_ip>,<period>	Start the SNTP client with options. ■ <sntp>: 1 (start) ■ <server_ip>: SNTP server IP address (or domain) ■ <period>: SNTP client update period (optional, second, default is 86400) Response: OK or ERROR
	?	Get the SNTP status. Response: +NWSNTP:<sntp>
	(none)	
	Example AT+NWSNTP=0 OK AT+NWSNTP=1,pool.ntp.org,86400 OK AT+NWSNTP +NWSNTP:1,pool.ntp.org,86400 OK	
AT+NWCCRT	<module>	Check if certificates exist. There are five sets of certificates, and four types for each set. ■ <Module> ■ 0: MQTT Client ■ 1: HTTPs Client ■ 2: WPA-Enterprise ■ 3: HTTPs Client for OTA ■ 4: HTTPs Server ■ Types: ■ RootCA ■ Cert ■ Key ■ DH param Response: +NWCCRT:<module>,<status> <status> bit 0 to bit 3 are used [DH param] [Key] [Cert] [RootCA] [3] [2] [1] [0] Each bit indicates the empty (0) or filled (1). For example, if there are only Root CA and Cert stored in Set #0, the response is +NWCCRT:0,3.
	Example	

Command	Parameters	Description
	AT+NWCCRT=0 +NWCCRT:0,7 // MQTT OK AT+NWCCRT=1 +NWCCRT:1,7 // HTTPS Client OK	
AT+NWDCRT	<module>	Delete TLS certificates for the specified module. ■ <Module> ■ 0: MQTT Client ■ 1: HTTPs Client ■ 2: WPA-Enterprise ■ 3: HTTPs Client for OTA ■ 4: HTTPs Server ■ All: All modules If <module> is "all", all certificates are removed. Response: OK or ERROR
	Example AT+NWDCRT=0 OK AT+NWDCRT=1 OK	
AT+NWCCRTR	<module>, <certificate type>	Reads TLS certificates for the specified module. ■ <Module>: 0: MQTT 1: HTTPs Client 2: WPA-Enterprise 3: HTTPs Client for OTA 4: HTTPs Server 5: ATCMD 6: AWS 7: Matter 8: Miscellaneous Application 1 9: Miscellaneous Application 2 10: Miscellaneous Application 3 11: Miscellaneous Application 4 12: Miscellaneous Application 5 13: Miscellaneous Application 6 14: Miscellaneous Application 7 15: Miscellaneous Application 8 ■ <certificate type>: 0 - CA certificate 1 - Certificate 2 - Private key 3 - DH params
	Example AT+NWCCRTR=0,0 +NWCCRTR:0,0,1,976,-----BEGIN CERTIFICATE-----... OK	

Table 4. Certificate command

Escape sequence	Parameters	Description
<ESC>CERT	<module>, <certificate type>, <mode>[, <format>, <length>, <content>]	Save or delete certificate/CA/private key/DH params. <ESC>CERT: To enter certificate input mode, ■ <Module>: Module ID. ■ 0: MQTT ■ 1: HTTPs Client ■ 2: WPA-Enterprise ■ 3: HTTPs Client for OTA ■ 4: HTTPs Server ■ 5: ATCMD ■ 6: AWS ■ 7: Matter ■ 8: Miscellaneous Application 1 ■ 9: Miscellaneous Application 2 ■ 10: Miscellaneous Application 3 ■ 11: Miscellaneous Application 4 ■ 12: Miscellaneous Application 5 ■ 13: Miscellaneous Application 6 ■ 14: Miscellaneous Application 7 ■ 15: Miscellaneous Application 8 ■ <certificate type>: Certificate type, 0 - CA certificate, 1 - Certificate, 2 - Private key, 3 - DH params, 4 - AWS initial certificate, 5 - AWS Initial private key, 6 - AWS unique certificate, 7 - AWS unique private key, 8 - Any negotiation parameter used, 9 - Matter certificate declaration, 10 - Matter DAC certificate, 11 - Matter PAI certificate, 12 - Matter DAC private key, 13 - Matter DAC public key ■ <mode>: Input mode. 0 - Store, 1 - Deletion ■ <format>: Certificate format, 0 - DER, 1 - PEM if mode is 0 (Store) ■ <length>: Length of certificate if mode is 0 (Store) ■ <content>: Certificate data if mode is 0 (Store) ■ Response: OK or ERROR Example: <ESC>CERT,0,1146,----- BEGIN CERTIFICATE -----MIIDFDCCAf...
	Example <ESC>CERT,0,0,0,1,980,-----BEGIN CERTIFICATE-----… OK <ESC>CERT,0,1,0,1,990,-----BEGIN CERTIFICATE-----… OK <ESC>CERT,0,2,0,1,310,-----BEGIN EC PRIVATE KEY-----… OK <ESC>CERT,0,3,0,1,432,-----BEGIN DH PARAMETERS-----… OK <ESC>CERT,7,10,0,1,696,----BEGIN CERTIFICATE----	

2.3 Wi-Fi Function Commands

NOTE
For special characters input in <ssid> or <key>, see Appendix I Special Characters Support in SSID or PSK.

Table 5. Wi-Fi function command list

Command	Parameters	Description
AT+WFMODE	<mode>	Set the Wi-Fi mode. <mode>: 0 (STA), 1 (Soft AP), 2 (WiFi Direct), 3 (WiFi Direct GO Fixed), 4 (STA + Soft AP) Response: OK or ERROR Note: ■ Wi-Fi mode is stored in NVRAM.

Command	Parameters	Description
		■ Restart the system to apply the changes.
	?	Get the current Wi-Fi mode. Response: +WFMODE:<mode>
	(none)	
	Example AT+WFMODE=0 // Set Station mode OK AT+WFMODE=1 // Set Soft AP mode OK AT+WFMODE // Get current Wi-Fi mode +WFMODE:1 OK AT+WFMODE=? // Get current Wi-Fi mode +WFMODE:1 OK	
AT+WFMAC	<mac>	Write a user MAC address in the NVRAM. Response: OK or ERROR Note: ■ The last digit should be an even number to be a valid MAC address. ■ A user MAC address is stored in NVRAM and restart the system to apply the changes. ■ RA6W1 provides three types of MAC address, and the priority is in the following order: Spoofing MAC address, User MAC address, and OTP MAC address. ■ When reading the MAC address in Soft AP mode, it becomes the MAC address that is written + 1.
	?	Get the current MAC address of the activated WLAN interface. Response: +WFMAC:<mac>
	(none)	
	Example AT+WFMAC=EC:9F:0D:9F:FA:64 OK AT+WFMAC=? +WFMAC:EC:9F:0D:9F:FA:64 OK AT+WFMAC +WFMAC:EC:9F:0D:9F:FA:64 OK AT+WFMAC=? // In Soft AP mode +WFMAC:EC:9F:0D:9F:FA:65 OK	
AT+WFSPF	<mac>	Write the spoofing MAC address in the NVRAM. Response: OK or ERROR Note: ■ Either odd or even number for last digit of MAC address is accepted. Use this command only in STA mode. ■ A spoofing MAC address is stored in NVRAM. Restart the system to apply the changes. ■ RA6W1 provides three types of MAC address, and the priority is in the following order: Spoofing MAC address, User MAC address, and OTP MAC address.

Command	Parameters	Description
	Example AT+WFSPF=EC:9F:0D:90:00:48 OK AT+WFSPF=? +WFSPF:EC:9F:0D:90:00:48 OK	
AT+WFSTAT	(none)	Get Wi-Fi configuration. Response: +WFSTAT:Interface <num> SSID_LENGTH:<length> SSID:<ssid> CHANNEL:<channel >+WFSTAT:<Wi-Fi interface><var>…WIFI GENERATION 6 Note: A response can be different depending on the current RA6W1 status/mode or whether the RA6W1 is configured as a STA or Soft AP. When the device status is disconnected, the response obtained is ERROR:0x5001F4.
	Example AT+WFSTAT +WFSTAT:Interface 0: SSID_LENGTH:15 SSID:RA6W2_9FFFFE BSSID:ec:9f:0d:9f:ff:ff SECURITY:0(No Security) CHANNEL:1 WIFI GENERATION:6 OK AT+WFSTAT +WFSTAT:Interface 0: SSID_LENGTH:9 SSID:IperfDemo BSSID:be:5f:ed:59:db:e5 SECURITY:3(WPA2 Security) CHANNEL:1 WIFI GENERATION:6 OK	
AT+WFPBC	(none)	Run the WPS PBC method. Response: OK or ERROR Note: ■ A WPS button can be pressed after issuing the command. ■ A router should support WPS and PBC. ■ The existing connection, if there is any, is lost when this command is run.
	Example AT+WFPBC OK +WFJAP:1,'MY_APS_SSID',192.168.0.3	
AT+WFPIN	<pin>	Run the WPS PIN method. ■ <pin>: PIN (eight digits) ■ (none): Generate a random PIN Response: +WFPIN:<pin> OK or ERROR Note: AP must support WPS PIN.
	(none)	Get the current PIN. Response: +WFPIN:<pin>
	?	
	Example AT+WFPIN=13557799 +WFPIN:13557799 OK	

Command	Parameters	Description
	AT+WFPIN +WFPIN:36269112 // Generate random number. OK AT+WFPIN=? +WFPIN:36269112 OK	
AT+WFCWPS	(none)	Cancel WPS (both PBC and PIN). Response: OK or ERROR Prerequisite ■ WPS should be in progress. Note: Return errors if WPS is not in progress.
	Example AT+WFCWPS OK	
AT+WFCC	<code>	Set a country code. <code>: Country code (defined by ISO 3166-1 alpha-2 standard) such as KR, US, JP, and CH Response: OK or ERROR Note: ■ A country code is stored in the NVRAM. ■ A country code consists of two characters. ■ If a country is invalid, the RA6W1 returns an error code with 0x500071. ■ Restart the system to apply the changes. ■ If this command is running in Soft AP mode with a new country code and the operating channel range of the new country does not cover the operating channel currently set, the operating channel is automatically switched to channel 1.
	?	Get the current country code. Response: AT+WFCC=<code>
	(none)	
	Example AT+WFCC=KR OK AT+WFCC +WFCC:KR OK AT+WFCC=? +WFCC:KR OK	
AT+WFRSSI	(none)	Get the current RSSI value. Response: +RSSI: -34 Prerequisite ■ The RA6W1 should be connected to AP. Note: The RA6W1 responds "+RSSI:NOT_CONN" with error (0x500190) if the connection is not established.
	Example AT+WFRSSI +RSSI:-25 OK …. (if there is no connection to an AP)	

Command	Parameters	Description
	AT+WFRSSI +RSSI:NOT_CONN ERROR: 5243280	
AT+WFSCAN	(none)	Scan APs. Response: +WFSCAN:<bssid><\t><signal><\t><ch><\t><security><\t><ssid><LF>… Prerequisite ■ The country code should be set through AT+WFCC. Note: An SSID can be missed in case of hidden AP. The security is based on the AP's security mode like the following: Open - No Security: (No Security) WEP Security: (WEP Security) WPA Security: (WPA Security) WPA2 Security: (WPA2 Security) WPA2 Enterprise Security: (WPA2 Enterprise Security) WPA3 Security: (WPA3 Security) WPA Enterprise Security: (WPA Enterprise Security) WPA + WPA2 Enterprise Security: (WPA/WPA2 Enterprise Security) WPA2 + WPA3 Enterprise Security: (WPA2/WPA3 Enterprise Security) WPA3 128 Bits Enterprise Security: (WPA3 Enterprise Security) WPA3 192 Bits Enterprise Security: (WPA3 192B Enterprise Security) WPA + WPA2 Security: (WPA/WPA2 Security) WPA2 + WPA3 Security: (WPA2/WPA3 Security) WPA3 OWE Security: (OWE Security)
	Example AT+WFSCAN +WFSCAN:34:98:b5:d3:70:9c -48 10 (WPA2 Security) NETGEAR_RAX50_v2 70:5d:cc:35:61:40 -60 11 (WPA2 Security) IPTIME_N704BCM e6:55:b8:27:14:b8 -60 104 (WPA2 Enterprise Security) REL-GLOBAL c0:c9:e3:c6:29:46 -62 36 (WPA2/WPA3 Security) TPLINK_Archer_AX21_5G_R OK Note: For hidden access points (APs), the network name (SSID) is not broadcast and appears as blank or empty in the list of available Wi-Fi networks. However, other information such as the BSSID (MAC address), signal strength, channel, and security type remains available during network scans	
AT+WFJAP	<ssid>,<sec>[,<hidden>] [,'ch=<channel1> [,<channel2>...]'] (sec=0|5)	Connect to an AP. ■ <ssid>: AP SSID ■ <sec>: Security protocol. 0 (OPEN), 1 (WEP), 2 (WPA), 3 (WPA2), 4 (WPA+WPA2), 5 (WPA3 OWE), 6 (WPA3 SAE), 7 (WPA2 RSN & WPA3 SAE) ■ <idx>: Key index for WEP. 0~3 ■ <enc>: Encryption. 0 (TKIP), 1 (AES), 2 (TKIP+AES) ■ <key>: Passphrase. 8 ~ 63 characters are allowed ■ <hidden>: 1 or [not specified] (<ssid> is hidden), 0 (<ssid> is NOT hidden) ■ ch=<channel1>[,<channel2>...]: Optional channel list for AP scan during connection. ■ Channel value range: 1 to 14 (2.4 GHz), 36 to 165 (5 GHz). ■ Multiple channels are comma-separated. ■ Maximum channel entries in one command: 20. ■ The ch= prefix is case-insensitive.

<table>
<tr><th>Command</th><th>Parameters</th><th>Description</th></tr>
<tr><td rowspan="4"></td><td></td><td rowspan="3">Response: OK or ERROR
Operation Results:
■ +WFJAP:<OPS_RESULT>['<SSID>','<IP_ADDRESS>']
■ +WFJAP:<OPS_RESULT>,<REASON>,[<REASON_CODE>]
■ <OPS_RESULT>: 1 (SUCCESS), 0 (FAILED)
■ If <OPS_RESULT>: 1
■ <SSID>: The SSID is surrounded by single quotation marks
■ <IP_ADDRESS>: Assigned IP address and format is xxx.xxx.xxx.xxx
■ If <OPS_RESULT>: 0
■ <REASON>: Well-known reason in text
■ <REASON_CODE>: if < REASON > is OTHER, this shows the reason code
For details about <REASON> or <REASON_CODE>, see Appendix E Reason Code for Wi-Fi Connection Failure or Disconnection.
Note:
■ The host should wait for both command responses OK or ERROR and Operation Result; wait for OK and +WFJAP:1,'<SSID>',<IP Address> for successful connection.
■ Depending on the network conditions, it might take more time to get an Operation Result because of internal connection retry.
■ No system reboot is required after running this command.
■ The AP configuration parameters (AP Profile) are stored in NVRAM.
■ See the example.
■ If <sec> is set to 6 (WPA3 SAE) or 7 (WPA2 RSN & WPA3 SAE), 1 (AES) is only valid as <enc> because WPA3 SAE allows only CCMP.
■ If channel list is specified, connection attempt is limited to the specified channel set. If no matching AP is found on those channels, connection fails/timeouts as normal.</td></tr>
<tr><td><ssid>,<sec>,<idx>,<key>[,<hidden>][,'ch=<channel1>[,<channel2>...]']
(sec=1)</td></tr>
<tr><td><ssid>,<sec>,<enc>,<key>[,<hidden>][,'ch=<channel1>[,<channel2>...]']
(sec=2|3|4|6|7)</td></tr>
<tr><td>?</td><td rowspan="2">Get the AP provisioning information.
■ Operation Results:
● If provisioning data is available:
● +WFJAP:'<SSID>',<sec>,<enc>,'<Passphrase>'
● If provisioning data is not available:
● ERROR: 5243290 (No SSID is found)</td></tr>
<tr><td>(none)</td></tr>
<tr><td colspan="2">Example
AT+WFJAP=MY_AP_SSID,0 // Open security
OK
+WFJAP:1,'MY_AP_SSID',192.168.43.32
AT+WFJAP=MY_AP_SSID,0,1 // Open security + hidden SSID
OK
+WFJAP:1,'MY_AP_SSID',192.168.43.32
AT+WFJAP=MY_AP_SSID,1,0,12345 // WEP security
OK
+WFJAP:1,'MY_AP_SSID',192.168.0.7
AT+WFJAP=MY_AP_SSID,1,0,12345,1 // WEP + hidden AP
OK
+WFJAP:1,'MY_AP_SSID',192.168.0.7
AT+WFJAP=MY_AP_SSID,4,2,N12345678 // WPA2 security
OK
+WFJAP:1,'MY_AP_SSID',192.168.0.7
AT+WFJAP=MY_AP_SSID,4,2,N12345678,1 // WPA2 + hidden AP
OK</td></tr>
</table>

Command	Parameters	Description
	+WFJAP:1,'MY_AP_SSID',192.168.0.7 AT+WFJAP=? +WFJAP:'MY_AP_SSID',4,2,'N12345678' OK AT+WFJAP=SSID,3,1,12345678,'ch=1,6,11' //WPA2 security + channel specified OK +WFJAP:1,'SSID',10.103.233.52	
AT+WFJAPA	<ssid>[,<key>][,<hidden>] [,'ch=<channel1> [,<channel2>...]']	Connect to an AP. ■ If <key> exists, security protocol is WPA+WPA2 and encryption is TKIP+AES. ■ If <key> is omitted, security protocol is OPEN. ■ <hidden>: 1 (<ssid> is hidden), 0 or [not specified] (<ssid> is NOT hidden) ■ If <hidden> is omitted, <ssid> is not hidden. ■ ch=<channel1>[,<channel2>...]: Optional channel list for AP scan during connection. ■ Channel range: 1 to 14 (2.4 GHz), 36 to 165 (5 GHz). ■ Multiple channels are comma-separated. ■ Maximum channel entries in one command: 20 ■ ch= prefix is case-insensitive. ■ <ssid>: AP SSID ■ <key>: Passphrase. 8 ~ 63 characters are allowed. Response: OK or ERROR Operation Results: ■ +WFJAP:<OPS_RESULT>['<SSID>','<IP_ADDRESS>'] ■ +WFJAP:<OPS_RESULT>,<REASON>,[<REASON_CODE>] ■ <OPS_RESULT>: 1 (SUCCESS), 0 (FAILED) ■ If <OPS_RESULT>: 1 ■ <SSID>: The SSID is surrounded by single quotation marks. ■ <IP_ADDRESS>: Assigned IP address and format is xxx.xxx.xxx.xxx. ■ If <OPS_RESULT>: 0 ■ <REASON>: Well-known reason in text ■ <REASON_CODE>: If <REASON> is OTHER, this shows the reason code. For details about <REASON> or <REASON_CODE>, see Appendix E Reason Code for Wi-Fi Connection Failure or Disconnection. Note: ■ The host should wait for both command responses **OK** or **ERROR** and **Operation Result;** wait for OK and +WFJAP:1,'<SSID>',<IP Address> for successful connection. ■ Depending on the network conditions, it might take more time to get an Operation Result because of internal connection retry. ■ No system reboot is required after running this command. ■ The AP configuration parameters (AP Profile) are stored in NVRAM. ■ If channel list is specified, connection scanning is limited to the specified channels. ■ In TIN/Combo, '\' character is used as delimiter for hexa/octal values. If the '\' character is used as a standalone character in the input string (not as a delimiter), it must be entered together with an additional delimiter. For example: abcdefg\12345678 → should be entered as abcdefg\\12345678.

Command	Parameters	Description
	?	Get the AP provisioning information (SSID and Passphrase only). ■ Operation Results: ■ If Wi-Fi connection is successful: +WFJAPA:'<SSID>','<Passphrase>' ■ If Wi-Fi connection fails: ERROR: 5243401 (No SSID found)
	(none)	
	Example AT+WFJAPA=MY_AP_SSID // Open security OK +WFJAP:1,'MY_AP_SSID',192.168.43.32 AT+WFJAPA=MY_AP_SSID,1 // Open security + hidden SSID OK +WFJAP:1,'MY_AP_SSID',192.168.43.32 AT+WFJAPA=MY_AP_SSID,N12345678 // WPA2 security OK +WFJAP:1,'MY_AP_SSID',192.168.43.32 AT+WFJAPA=MY_AP_SSID,N12345678,1 // WPA2 security + hidden AP OK +WFJAP:1,'MY_AP_SSID',192.168.43.32 AT+WFJAPA=? +WFJAPA:'MY_AP_SSID','N12345678' OK AT+WFJAPA=MY_AP_SSID,12345678,'ch=1,6,11' //WPA2 security + channel specified OK +WFJAP:1,'MY_AP_SSID',10.103.233.52	
AT+WFJAPMK	<ssid>,<auth>,<pmk> [,<hidden>] [,'ch=<channel>'] (auth=2|3|4)	Connect to an AP using a pre-computed raw PMK. ■ <ssid>: AP SSID (UTF-8 / Extended ASCII supported) ■ <auth>: Security protocol 2=WPA, 3=WPA2, 4=WPA/WPA2 auto (PSK modes only) ■ <pmk>: Pre-computed PMK - exactly 64 hexadecimal characters ■ <hidden>: Optional. 1 or [not specified] (<ssid> is hidden), 0 (<ssid> is NOT hidden). ■ ch=<channel>: Optional channel hint to restrict the scan. Example: ch=6 or ch=1,6,11. Response: OK or ERROR Operation Results: ■ +WFJAP:<OPS_RESULT>['<SSID>','<IP_ADDRESS>'] ■ +WFJAP:<OPS_RESULT>,<REASON>,[<REASON_CODE>] ■ <OPS_RESULT>: 1 (SUCCESS), 0 (FAILED) ■ If <OPS_RESULT>: 1 ■ <SSID> : The SSID is surrounded by single quotation marks ■ <IP_ADDRESS>: Assigned IP address and format is xxx.xxx.xxx.xxx ■ If <OPS_RESULT>: 0 ■ <REASON> : Well-known reason in text ■ <REASON_CODE>: if <REASON> is OTHER, this shows the reason code For details about <REASON> or <REASON_CODE>, see Appendix E Reason Code for Wi-Fi Connection Failure or Disconnection. Note:

Command	Parameters	Description
		■ The host should wait for both command responses (OK or ERROR) and the Operation Result. Wait for OK and +WFJAP:1,<SSID>,<IP Address> for a successful connection. ■ Depending on the network conditions, it may take more time to get an Operation Result because of internal connection retry. ■ No system reboot is required after running this command. ■ The AP configuration parameters (AP Profile) are stored in NVRAM. ■ This command bypasses the PBKDF2 derivation step by accepting the raw PMK directly, reducing CPU load and connection latency. ■ This command supports WPA-PSK/WPA2-PSK only. WPA3-SAE, WEP, and Enterprise modes are not supported. ■ Only valid in Station mode or Station + Soft-AP mode. ■ Query form (AT+WFJAPMK=?) is NOT supported because the raw PMK cannot be read back for security reasons.
	Example AT+WFJAPMK=MY_AP_ SSID,3,b5b6290fb5128907de20efaa05b5806779d973fc7513e957f0ab9725555fb6a6//WPA2-PSK connect using a pre-computed raw PMK OK +WFJAP:1,'MY_AP_SSID',192.168.43.32 AT+WFJAPMK=MY_AP_ SSID,4,b5b6290fb5128907de20efaa05b5806779d973fc7513e957f0ab9725555fb6a6//WPA/WPA2 auto-negotiation connect using a pre-computed raw PMK OK +WFJAP:1,'MY_AP_SSID',192.168.43.32 AT+WFJAPMK=MY_AP_ SSID,3,b5b6290fb5128907de20efaa05b5806779d973fc7513e957f0ab9725555fb6a6//Auto-reconnect with stored PMK after restart OK +WFJAP:1,'MY_AP_SSID',192.168.43.32 AT+RESTART OK +INIT:DONE,0 +WFJAP:1,'MY_AP_SSID',192.168.43.32 AT+WFJAPMK=MY_AP_ SSID,3,b5b6290fb5128907de20efaa05b5806779d973fc7513e957f0ab9725555fb6a6//Disconnect, then reconnect using stored PMK OK +WFJAP:1,'MY_AP_SSID',192.168.43.32 AT+WFDAP OK AT+WFJAPMK=MY_AP_ SSID,3,b5b6290fb5128907de20efaa05b5806779d973fc7513e957f0ab9725555fb6a6 OK +WFJAP:1,'MY_AP_SSID',192.168.43.32 AT+WFJAPMK=MY_AP_ SSID,3,b5b6290fb5128907de20efaa05b5806779d973fc7513e957f0ab9725555fb6a6//Connection status check after PMK connect	

Command	Parameters	Description
	OK +WFJAP:1,'MY_AP_SSID',192.168.43.32 AT+WFSTAT +WFSTAT:Interface 0: SSID_LENGTH:10 SSID:MY_AP_SSID BSSID:52:8f:0e:41:d3:9f SECURITY:3(WPA2 Security) CHANNEL:149 WIFI GENERATION:5 OK AT+WFJAPMK=MY_AP_ SSID,3,ZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ //ERROR - Invalid PMK (non-hex characters) ERROR:0x5001D6 (5243350) AT+WFJAPMK=MY_AP_ SSID,3,deadbeefdeadbeefdeadbeefdeadbeefdeadbeefdeadbeefdeadbeefdeadbeef//ERROR - Wrong PMK (valid hex format, wrong value) ERROR:0x5001F7 (5243383)	
AT+WFCAP	(none)	Connect to an AP with the current WLAN0 interface configuration. Response: OK or ERROR Prerequisite ■ AP profile parameters should be in NVRAM. Note: ■ An AP profile can be stored in NVRAM by issuing the AT+WFJAPA or AT+WFJAP command. ■ If there is no AP profile found, the RA6W1 returns an error (0x5001F7). ■ If the RA6W1 is already in connection with an AP, it returns an error (0x5001CC).

	Example
	AT+WFCAP
	OK
	+WFJAP:1,'MY_AP_SSID',192.168.0.7
	
	AT+WFCAP
	ERROR:0x5001F7 (5243383) // Failed to connect to AP (for example, AP profile is not found).
	
	AT+WFCAP
	ERROR:0x5001CC (5243340) // Already connected	

AT+WFQAP	(none)	Disconnect from the currently associated AP. Response: OK or ERROR Prerequisite ■ The RA6W1 should be connected to AP. Note: No error returns if it is already disconnected from an AP.
	Example AT+WFQAP +WFDAP:0,DEAUTH OK	
AT+WFSTA	(none)	Check Wi-Fi connection. Response: +WFSTA:<status> <status> 1 (Connected), 0 (disconnected) Prerequisite ■ Station mode. Note: If the RA6W1 runs the command in Soft AP mode, it

Command	Parameters	Description
		returns an error (0x500064).
	Example AT+WFSTA +WFSTA:0 OK AT+WFSTA +WFSTA:1 OK	
AT+WFDIS	<disabled>	Set the Wi-Fi STA profile unused. If set to 1, the RA6W1 does not start connecting to the configured AP when rebooting. <disabled>: 1 (Unused), 0 (Used) Response: OK or ERROR Note: ■ The "unused" flag is stored in the NVRAM. ■ The flag affects RA6W1 during boot-up procedure. ■ Restart the system to apply the changes.
	?	Get the status of the Wi-Fi profile. Response: +WFDIS:<disabled>
	(none)	
	Example AT+WFDIS=1 OK AT+WFDIS=? +WFDIS:1 OK	
AT+WFSAP	<ssid>,<sec>,<ch>,<code> (sec=0|5)	Set up Soft AP interface. <ssid>: AP SSID. Max 32 characters are allowed <sec>: Security protocol. 0 (OPEN), 2 (WPA), 3 (WPA2), 4 (WPA+WPA2)), 5 (WPA3 OWE), 6 (WPA3 SAE), 7 (WPA2 RSN & WPA3 SAE) <enc>: Encryption. 0 (TKIP), 1 (AES), 2 (TKIP+AES) <key>: Passphrase. 8 ~ 63 characters are allowed. <ch>: Operating channel (optional). Default is 1 or use the current channel if Soft AP is operating. <code>: Country code (optional). If exists, <ch> is essential. Response: OK or ERROR Note: ■ The Soft AP configuration parameters are stored in NVRAM. ■ If the command is issued in Station mode, reboot the system to start in Soft AP mode. (If the command is issued in Soft AP mode, then no system restart is required). ■ The "," (comma) is included in the SSID string and encloses the SSID with single quotation marks. ■ See the example. ■ If <sec> is set to 6 (WPA3 SAE) or 7 (WPA2 RSN & WPA3 SAE), 1 (AES) is only valid as <enc> because WPA3 SAE allows only CCMP. ■ In TIN/Combo, '\' character is used as delimiter for hexa/octal values. If the '\' character is used as a standalone character in the input string (not as a delimiter), it must be entered together with an additional delimiter. For example: abcdefg\12345678 → should be entered as abcdefg\\12345678.
	<ssid>,<sec>,<enc>,<key>,<ch>,<code> (sec=2|3|4|6|7)	

Command	Parameters	Description
	?	Get the Soft AP interface configuration. ▪ Response: +WFSAP:'<ssid>',<auth>,<enc>,'<key>',<ch>,<code> Operation Result: +WFSAP:<ssid> is printed on success.
	(none)	
	Example AT+WFSAP=RA6W1_MY_SSID,0,1,KR // Open mode +WFSAP:RA6W1_MY_SSID OK AT+WFSAP=? +WFSAP:'RA6W1_MY_SSID',0,1,KR OK AT+WFSAP=RA6W1_MY_SSID,3,1,12345678,1,KR // WPA2-AES +WFSAP:RA6W1_MY_SSID OK AT+WFSAP=? +WFSAP:'RA6W1_MY_SSID',3,1,'12345678',1,KR OK AT+WFSAP='RA6W1,MY_SSID',3,2,'12345678',1,KR // WPA2-AES +WFSAP:RA6W1,MY_SSID OK AT+WFSAP=? +WFSAP:'RA6W1,MY_SSID',3,1,'12345678',1,KR OK	
AT+WFOAP	(none)	Operate Soft AP interface. Response: OK or ERROR Prerequisite A Soft AP profile is stored in NVRAM. Note: Run this command in Soft AP mode. If there is no profile in NVRAM, it returns an error (0x5000BC). The RA6W1 returns an error (0x50020A) if it already operates as Soft AP.
	Example AT+WFOAP OK	
AT+WFTAP	(none)	Stop the Soft AP interface. Response: OK or ERROR Prerequisite Soft AP mode. Note: This command is valid while the RA6W1 is running in Soft AP mode.
	Example AT+WFTAP OK	
Additional notes for AT+WFSAP, AT+WFOAP, and AT+WFTAP: Example: In STA mode, in factory reset state Set up Soft AP: AT+WFSAP=RA6W1_OPEN,0 Reboot to start in the configured Soft AP mode: AT+RESTART DUT starts as Soft AP Stop Soft AP if required: AT+WFTAP Start Soft AP if required: AT+WFOAP		
AT+WFRAP	(none)	Restart the Soft AP interface.

Command	Parameters	Description
		Response: OK or ERROR Prerequisite ■ A profile for Soft AP should be stored in NVRAM. Note: ■ This command is valid in Soft AP mode. ■ If it runs in Station mode, the RA6W1 returns an error (0x500064).
	Example AT+WFRAP OK	
AT+WFLCST	(none)	Get connected station information. Response: +WFLCST:<mac><LF><flags><LF><var>… Note: If no station is connected, then the RA6W1 returns +WFLCST:NOT_FOUND.
	Example AT+WFLCST +WFLCST:a6:f2:7c:d4:53:1c flags=[AUTH][ASSOC][AUTHORIZED][SHORT_PREAMBLE][WMM][MAYBE_WPS][HT] aid=1 capability=0x421 listen_interval=10 wifi_mode=802.11n timeout_next=NULLFUNC POLL rx_packets=290 tx_packets=4 rx_bytes=29625 tx_bytes=10658 inact_cnt=0 connected_time=20 sta_count=1 OK AT+WFLCST +WFLCST:NOT_FOUND OK	
AT+WFAPWM	<mode>	Set IEEE 802.11 Wi-Fi mode of Soft AP interface. <mode>: 0 (B/G/N), 1 (G/N), 2 (B/G), 3 (N 2 GHz only), 4 (G), 5 (B), 6 (AN), 7 (A), 8 (N 5 GHz only) Response: OK or ERROR Note: ■ The configuration is stored in NVRAM. ■ Restart the system to apply the changes.
	?	Get IEEE 802.11 Wi-Fi mode of Soft AP interface. Response: +WFAPWM:<mode>
	(none)	
	Example AT+WFAPWM=0 OK AT+WFAPWM=1 OK AT+WFAPWM=? +WFAPWM:1	

Command	Parameters	Description
	OK	
AT+WFAPCH	<ch>	Set the operating channel number for the Soft AP interface. <ch>: Operating channel (0 is auto) Response: OK or ERROR Note: ■ The configuration is stored in NVRAM. ■ Restart the system to apply the changes.
	?	Get the operating channel number for the Soft AP interface. Response: +WFAPCH:<ch>
	(none)	
	Example AT+WFAPCH=5 OK AT+WFAPCH=? +WFAPCH:5 OK	
AT+WFAPCHLIST	<country_code>	List channels that can be used as operating channels for SoftAP mode. <country_code>: country code Response: +WFAPCHLIST:<list of channels> OK or ERROR
	Example AT+WFAPCHLIST=KR +WFAPCHLIST:1-13,36,40,44,48,149,153,157,161,165 OK AT+WFAPCHLIST=US +WFAPCHLIST:1-11,36,40,44,48,149,153,157,161,165 OK	
AT+WFAPBI	<interval>	Set the AP beacon interval. <interval>: Beacon interval (ms) Response: OK or ERROR Note: ■ The configuration is stored in NVRAM. ■ Restart the system to apply the changes.
	?	Get the AP beacon interval. Response: +WFAPBI:<interval>
	(none)	
	Example AT+WFAPBI=200 OK AT+WFAPBI=? +WFAPBI:200 OK	
AT+WFAPUI	<timeout>	Set station disconnection timeout in Soft AP mode. <timeout>: Disconnection timeout (seconds) (from 30 to 86400, step = 10) If 0, the default value (300 s) is used. Response: OK or ERROR Note: ■ Within the specified time, if an STA does not send any frame, Soft AP sends a NULL frame after the timeout is expired to check STA's inactivity. If no ACK is received from the STA, Soft AP removes the STA.

Command	Parameters	Description
		■ The configuration is stored in NVRAM. ■ Restart the system to apply the changes.
	?	Get station disconnection timeout in Soft AP mode. Response: +WFAPUI:<timeout>
	(none)	
	Example AT+WFAPUI=60 OK AT+WFAPUI=? +WFAPUI:60 OK	
AT+WFAPRT	<threshold>	Set the AP RTS threshold (octets). <threshold>: RTS threshold (from 1 to 2347) Response: OK or ERROR Note: ■ When sending a frame that is bigger than the RTS threshold specified, RTS/CTS frames are sent first to avoid collision in the air. By default, the RTS threshold is 2347. ■ The configuration is stored in NVRAM. ■ Restart the system to apply the changes.
	?	Get the AP RTS threshold. Response: +WFAPRT:<threshold>
	(none)	
	Example AT+WFAPRT=2100 OK AT+WFAPRT=? +WFAPRT:2100 OK	
AT+WFAPDE	<mac>	Send deauthentication frame to the connected station. <mac>: MAC address of the connected station Response: OK or ERROR Note: ■ Use this command in Soft AP mode. ■ Check the MAC address of an STA that needs to send deauthentication frame by using the command AT+WFLCST. ■ If the operation is not successful (for example, a wrong MAC address is specified), then there is no operation result.
	Prerequisite The RA6W1 should be connected to AP. Example AT+WFAPDE=E6:0D:E5:A5:5D:B3 +WFDST:e6:0d:e5:a5:5d:b3 OK	
AT+WFAPDI	<mac>	Send the disassociation frame to the connected station. <mac>: MAC address of the connected station Response: OK or ERROR Note: ■ Use this command in Soft AP mode. ■ Check the MAC address of an STA that needs to send disassociation frame by using the command AT+WFLCST. ■ If the operation is not successful (for example, a wrong MAC address is specified), then there is no operation result.

Command	Parameters	Description
	Prerequisite The RA6W1 should be connected to AP. Example AT+WFAPDI=E6:0D:E5:A5:5D:B3 +WFDST:e6:0d:e5:a5:5d:b3 OK	
AT+WFWMM	<wmm>	Set WMM on/off. <wmm>: 0 (off), 1 (on) Response: OK or ERROR Prerequisite ■ Soft AP mode. Note: ■ WMM is enabled by default. If WMM is enabled, Beacon/Probe Rsp/Assoc frames have WMM information. WMM enables QoS on the AC category. ■ The configuration is stored in NVRAM.
	?	Get the WMM status. Response: +WFWMM:<wmm>
	(none)	
	Example AT+WFWMM=1 OK AT+WFWMM=? +WFWMM:1 OK	
AT+WFSMSAVE	<run_mode>	Save Switching system run-mode <run_mode>: 0 (STA), 1(SoftAP) Response: OK or ERROR Prerequisite ■ Concurrent mode. Note: The configuration is stored in NVRAM.
	?	Get the run mode. Response: +WFSMSAVE: <run_mode>
	(none)	
	Example AT+WFSMSAVE=0 OK AT+WFSMSAVE=2 ERROR:0x50006F (5242991) AT+WFSMSAVE=? +WFSMSAVE:0 OK	
AT+WFMODESWTCH	(none)	Switch system run-mode Response: OK or ERROR Prerequisite ■ Concurrent mode. ■ <run_mode> should be stored. Note: ▪ Return ERROR:0x5001CD (5243341) when there is no profile information
	Example AT+WFMODESWTCH OK AT+WFMODESWTCH ERROR:0x5001CD (5243341)	

Command	Parameters	Description
	AT+WFMODESWTCH OK +INIT:DONE,<run_mode>	
AT+WFWMP	<wmmps>	Set WMM-PS (WMM Power Save) on/off. <wmmps>: 0 (off), 1 (on) Response: OK or ERROR Prerequisite ■ Soft AP mode. Note: ■ By default, WMM-PS is disabled. If WMM-PS is enabled, Beacon/Probe Rsp/Assoc Rsp frames sent from Soft AP have a U-APSD flag set. For WMM and WMM-PS to properly work, the STA should also have WMM and WMM-PS certified. ■ The configuration is stored in NVRAM.
	?	Get the WMM-PS status. Response: +WFWMP:<wmmps>
	Example AT+WFWMP=0 OK AT+WFWMP=? +WFWMP:0 OK	
AT+WFINIT	(none)	Initialize WLAN. Note: WLAN is initialized at boot time by default, but if the current WLAN init mode is 0 (do not initialize WLAN at boot), running AT+WFINIT starts WLAN initialization. See AT+WFINITMODE.
	?	Get WLAN initialization status. +WFINIT:1 (WLAN initialized)/0 (WLAN not initialized)
	Example AT+WFINIT OK AT+WFINIT=? +WFINIT:1 OK	
AT+WFINITMODE	<flag>	Set WLAN initialization mode. <flag>: 0 (No WLAN initialization at boot), 1 (WLAN initialization at boot) Note: WLAN is initialized by default at boot time, but if the current WLAN init mode is 0 (WLAN not initialized yet), running AT+WFINIT starts WLAN initialization. See AT+WFINITMODE.
	?	Query WLAN initialization mode. +WFINITMODE:<flag>
	(none)	
	Example AT+WFINITMODE=?// Query the current mode +WFINITMODE:1// WLAN initialization at boot OK AT+WFINITMODE=0// Not to set WLAN initialization at boot OK AT+WFINITMODE=?// Query the current mode	

Command	Parameters	Description
	+WFINITMODE:0 OK AT+RESTART// Reboot the system OK +INIT:DONE,0 ATE Echo on OK AT+WFINIT=? +WFINIT:0// WLAN init is not done yet OK AT+WFINIT// Start WLAN initialization OK	
AT+WFSETBAND	<band>	Set bandwidth. <band>: 0 (AUTO), 2 (2 GHz only), 5 (5 GHz only) Prerequisite ■ __SUPPORT_SETBAND_5GHZ__ should be enabled to use this command. Note: ■ The configuration is stored in NVRAM. ■ In Soft AP mode, <band> allows only 2 or 5.
	?	Get the current bandwidth set value. +WFSETBAND:<band>
	Example AT+WFSETBAND=5 OK AT+ WFSETBAND=? +WFSETBAND:5 OK	

Table 6. Wi-Fi function response list

Response	Parameters	Description
+WFJAP	<result>,<ssid>,<ip> <result>,<well-known-reason>[,<reason_code>]	The result of AP connection in STA mode (The result of AT+WFJAP or AT+WFJAPA or AT+WFCAP). <result>: 0 (failed), 1 (succeeded) For <result>: 1 ■ <ssid>: SSID of the AP when succeeded. ■ <ip>: IP address of the station when succeeded. For <result>: 0 <well-known-reason>: reason for connection attempt failure in text format, TIMEOUT/WRONGPWD/ACCESSLIMIT/OTHER ■ TIMEOUT: connection attempt failed after continuous connection attempts. ■ WRONGPWD: WPA 4-Way Handshake failed, pre-shared key (password) might be incorrect. ■ ACCESSLIMIT: disconnected because the authorized access number limit is reached. ■ OTHER: other reasons <reason_code>: if <well-known-reason> is OTHER, this field shows what caused the connection attempt failure. See Appendix E Reason Code for Wi-Fi Connection Failure or Disconnection. Example: +WFJAP:0,TIMEOUT

Response	Parameters	Description
		+WFJAP:1,'ap_test',192.168.0.10 // The Wi-Fi connection is established, and the assigned IP address is 192.168.0.10.
+WFDAP	<reserved>, <well-known-reason> [,<reason_code>]	Disconnected from the AP. <reserved>: 0 <well-known-reason>: disconnection reason in text format, AUTH_NOT_VALID/DEAUTH/INACTIVITY/APBUSY/OTHER ■ AUTH_NOT_VALID: Previous authentication no longer valid. ■ DEAUTH: Deauthenticated as STA is leaving. ■ INACTIVITY: Disassociated because of inactivity. ■ APBUSY: Disassociated because AP is unable to handle all currently associated STAs. <reason_code>: If <well-known-reason> is OTHER, this field shows what caused the disconnection. See Appendix E Reason Code for Wi-Fi Connection Failure or Disconnection. Example: +WFDAP:0,INACTIVITY +WFDAP:0,DEAUTH +WFDAP:0,OTHER,8 à WLAN_REASON_CLASS2_FRAME_FROM_NONAUTH_STA (8)
+WFCST	<mac>	A Wi-Fi station connected in Soft AP mode. <mac>: MAC address of the connected station
+WFDST	<mac>	Wi-Fi station disconnected in Soft AP mode. <mac>: MAC address of the disconnected station.

2.4 Wi-Fi Function Commands for WPA3

You can configure the RA6W1 as WPA3 STA or WPA3 Soft AP. WPA3 Personal is enabled by default. Syntax of all the Wi-Fi function commands is the same as described in Table 7, except the following commands which must specify WPA3 specific parameters.

NOTE
For special characters input in <ssid> or <key>, see Appendix I Special Characters Support in SSID or PSK.

Table 7. List of WPA3-relevant Wi-Fi function commands

Command	Parameters	Description
AT+WFJAP	See AT+WFJAP	
	Example AT+WFJAP=MY_AP_SSID,5// WPA3 OWE OK +WFJAP:1,'MY_WPA3_AP_SSID',192.168.0.7 AT+WFJAP=MY_AP_SSID,5,1// WPA3 OWE + hidden SSID OK +WFJAP:1,'MY_AP_SSID',192.168.43.32 AT+WFJAP=MY_AP_SSID,6,1,N12345678// WPA3 SAE security OK +WFJAP:1,'MY_WPA3_AP_SSID',192.168.0.7 AT+WFJAP=MY_AP_SSID,6,1,12345678,1 // WPA3 SAE + hidden AP OK +WFJAP:1,'MY_AP_SSID',192.168.0.7 AT+WFJAP=MY_AP_SSID,7,1,N12345678// WPA2(RSN)+WPA3 SAE security OK +WFJAP:1,'MY_WPA3_AP_SSID',192.168.0.7 AT+WFJAP=? +WFJAP:'MY_AP_SSID',6,1,'N12345678' OK	

AT+WFJAPA3	`<wpa3_flag>,<ssid>`
	`[,<key>]`
	`[,<hidden>]`
	`[,'ch=<channel1>`
	`[,<channel2>...]']`
		Connect to an AP which includes WPA3 type.
		■ `<wpa3_flag>`: WPA2/WPA3 AP-type
		■ If 1, WPA3-AP.
		■ If 0, WPA/WPA2-AP.
		■ If `<key>` exists, security protocol is WPA+WPA2 and encryption is TKIP+AES.
		■ If `<key>` is omitted,
		● When <wpa3_flag> is 0, the security protocol is OPEN.
		● When <wpa3_flag> is 1, the security protocol is OWE.
		■ `<hidden>`: 1 or [not specified] (`<ssid>` is hidden), 0 (`<ssid>` is NOT hidden)
		■ If `<hidden>` is omitted, `<ssid>` is not hidden.
		■ `<ssid>`: AP SSID
		■ `<key>`: Passphrase. 8 ~ 63 characters are allowed.
		■ `ch=<channel1>[,<channel2>...]`: Optional channel list for scan during connection.
		■ Channel range: `1-14` (2.4 GHz), `36-165` (5 GHz).
		■ Multiple channels are comma-separated.
		■ Maximum channel entries in one command: 20
		■ `ch=` prefix is case-insensitive.
		■ Response: OK or ERROR
		■ Operation Results:
		■ +WFJAP:<OPS_RESULT>['<SSID>','<IP_ADDRESS>']
		■ +WFJAP:<OPS_RESULT>,<REASON>,[<REASON_CODE>]
		■ <OPS_RESULT>: 1 (SUCCESS), 0 (FAILED)
		■ If <OPS_RESULT>: 1
		■ <SSID>: The SSID is surrounded by single quotation marks
		■ <IP_ADDRESS>: Assigned IP address and format is xxx.xxx.xxx.xxx
		■ If <OPS_RESULT>: 0
		■ <REASON>: well-known reason in text
		■ <REASON_CODE>: if < REASON > is OTHER, this shows the reason code.
		For details about <REASON> or <REASON_CODE>, see 2.3.
		Note:
		■ The host should wait for both command responses **OK** or **ERROR** and **Operation Result**; wait for OK and +WFJAPA:1,'<SSID>',<IP Address> for successful

<table>
<tr><th>Command</th><th>Parameters</th><th>Description</th></tr>
<tr><td></td><td></td><td>connection.
■ Depending on the network conditions, it might take more time to get an Operation Result because of internal connection retry.
■ No system reboot is required after running this command.
■ The AP configuration parameters (AP Profile) are stored in NVRAM.
■ If channel list is provided, connection is limited to those channels.
■ In TIN/Combo, '\' character is used as delimiter for hexa/octal values. If the '\' character is used as a standalone character in the input string (not as a delimiter), it must be entered together with an additional delimiter. For example: abcdefg\12345678 → should be entered as abcdefg\\12345678.</td></tr>
<tr><td></td><td>?</td><td rowspan="2">Get the AP profile information (SSID and Passphrase only)
■ Operation Results:
■ If Wi-Fi connection is successful:
+WFJAP:'<SSID>','<Passphrase>'
■ If Wi-Fi connection fails:
ERROR: 5243401 (No SSID found)</td></tr>
<tr><td></td><td>(none)</td></tr>
<tr><td></td><td colspan="2">Example
AT+WFJAPA3=0,WPA2_AP_SSID// Open mode
OK
+WFJAP:1,'WPA2_AP_SSID',192.168.0.2

AT+WFJAPA3=0,WPA2_AP_SSID,1// Open mode + hidden SSID
OK
+WFJAP:1,'WPA2_AP_SSID',192.168.0.2

AT+WFJAPA3=0,WPA2_AP_SSID,N12345678// WPA2 security
OK
+WFJAP:1,'WPA2_AP_SSID',192.168.0.2

AT+WFJAPA3=0,WPA2_AP_SSID,N12345678,1 // WPA2 security + hidden AP
OK
+WFJAP:1,'WPA2_AP_SSID',192.168.0.2

AT+WFJAPA3=1,WPA3_AP_SSID// WPA3-OWE
OK
+WFJAP:1,'WPA3_AP_SSID',192.168.0.2

AT+WFJAPA3=1,WPA3_AP_SSID,N12345678 // WPA3-SAE security
OK
+WFJAP:1,'WPA3_AP_SSID',192.168.0.2

AT+WFJAPA3=1,WPA3_AP_SSID,N12345678,1 // WPA3-SAE + hidden AP
OK
+WFJAP:1,'WPA3_AP_SSID',192.168.0.2

AT+WFJAPA3=?
+WFJAPA3:'MY_AP_SSID','N12345678'
OK

AT+WFJAPA3=1,MY_AP_SSID,12345678,'ch=1,6,11' // WPA3-SAE security + channel specified
OK
+WFJAP:1,'MY_AP_SSID',10.103.233.52</td></tr>
</table>

Command	Parameters	Description
AT+WFSAP	See AT+WFSAP.	
	Example AT+WFSAP=RA6W1_MY_SSID,5,1,KR// WPA3 OWE +WFSAP:RA6W1_MY_SSID OK AT+WFSAP=RA6W1_MY_SSID,7,1,12345678,1,KR // WPA2 RSN & WPA3 SAE, AES +WFSAP:RA6W1_MY_SSID OK AT+WFSAP=? +WFSAP:'RA6W1_MY_SSID',7,1,'12345678',1,KR OK	

2.5 Wi-Fi Function Commands for WPA-Enterprise

AT commands of the RA6W1 provide Wi-Fi commands that can be used as STA in WPA-Enterprise environment. To connect the WPA-Enterprise AP, the RA6W1 must have profile information for the WPA-Enterprise AP and user account information.

NOTE
For special characters input in <ssid> or <key>, see Appendix I Special Characters Support in SSID or PSK.

Table 8. WPA-enterprise Wi-Fi function commands

Command	Parameters	Description
AT+WFENTAP	<ssid>,<auth>,<enc>, <phase1>,<phase2> [,<hidden>] [,'ch=<channel1> [,<channel2>...]'] (phase1=0|1|2|4)	Create Enterprise profile to NVRAM. ■ <ssid>: Enterprise AP SSID ■ <auth>: Authentication mode for WAP-Enterprise. 8 (WPA-EAP), 9 (WPA2-EAP), 10 (WPA/WPA2-EAP),11 (WPA3-EAP), 12(WPA3-EAP-192B), 13(WPA2/WPA3-EAP). ■ <enc>: Encryption Type. 0 (TKIP), 1 (AES), 2 (TKIP+AES), 3 (GCMP-256) ■ <phase1>: Phase #1 EAP type. 0 (Mixed), 1 (PEAP0), 2 (PEAP1), 3 (FAST), 4 (TTLS), 5 (TLS) ■ <pahse2>: Phase #2 EAP type. 0 (Mixed), 1 (MSCHAPV2), 2 (GTC), 3 (TLS) ■ <hidden>: 1 or [not specified] (<ssid> is hidden), 0 (<ssid> is NOT hidden) ■ ch=<channel1>[,<channel2>...]: Optional channel hint/list for scan during Enterprise connection. ■ Channel range: 1 to 14 (2.4 GHz), 36 to 165 (5 GHz). ■ Multiple channels are comma-separated. ■ Maximum channel entries in one command: 20. ■ ch= prefix is case-insensitive Response: OK or ERROR Operation Results: +WFENTAP:<SSID> Note: ■ The WPA-Enterprise profile is stored in NVRAM. ■ If <phase1> is set to 3 (FAST) or 5 (TLS), <phase2> is not allowed. ■ Need user account to connect to WPA-Enterprise AP. See AT+WFENTLI command. ■ Restart the system to apply the changes. ■ If channel list is specified, scan/connect is limited to the listed channels. ■ To add the certificates for TLS, see Table 4.
	<ssid>,<auth>,<enc>, <phase1>[,<hidden>] [,'ch=<channel1> [,<channel2>...]'] (phase1=3|5)	
	?	Get the WPA-Enterprise configuration. Response: +WFENTAP:<ssid>,<auth>,<enc>,<phase1>,<pahse2>
	(none)	
	Example AT+WFENTAP=MY_AP_SSID,10,2,0 // Phase#1 Mixed mode	

Command	Parameters	Description
	OK +WFENTAP:'MY_AP_SSID' AT+WFENTAP=MY_AP_SSID,10,2,0,0 // Phase#1, #2 Mixed mode OK +WFENTAP:'MY_AP_SSID' AT+WFENTAP=MY_AP_SSID,10,2,0,0,1 // Phase#1, #2 Mixed mode OK AT+WFENTAP=SSID_Your_AP,9,1,2,3 // PEAP-TLS AT+WFENTAP=SSID_Your_AP,9,1,4,3 // TTLS-TLS	
AT+WFENTLI	<id>[,<pw>]	Set User-ID/Password for WPA-Enterprise user account. ■ <id>: Login-ID for WPA-Enterprise user account ■ <pw>: Login-password for WPA-Enterprise user account Response: OK or ERROR Note: ■ User account ID and password are stored in the NVRAM. ■ Restart the system to apply the changes.
	?	Get currently saved User-ID/Password for WPA-Enterprise user account. Response: OK or ERROR Operation Result: +WFENTLI:<id>,<pwd>
	(none)	
	Example AT+WFENTLI='USER_ACCOUNT_ID','USER_ACCOUNT_PWD' OK AT+WFENTLI +WFENTLI='USER_ACCOUNT_ID','USER_ACCOUNT_PWD' AT+WFENTLI=? +WFENTLI='USER_ACCOUNT_ID','USER_ACCOUNT_PWD'	

2.5.1 WPA-Enterprise Connection Example

To start Wi-Fi connection, create WPA-Enterprise profile and restart the RA6W1. For all cases, WPA-Enterprise user account information is needed.
Case #1: Mixed mode for EAP-type.
In this case, Encryption-type is configured as Mixed mode. EAP-type and Encryption type are selected automatically.

```
AT+WFENTAP='WPA-Ent-AP-SSID',10,2,0
AT+WFENTLI='WPA-Ent_User_ID','WPA-Ent_PWD'
AT+RESTART
```

Case #2: Mixed mode for EAP-type and Encryption type.
EAP-type and Encryption type are selected automatically.

```
AT+WFENTAP='WPA-Ent-AP-SSID',10,2,0,0
AT+WFENTLI='WPA-Ent_User_ID','WPA-Ent_PWD'
AT+RESTART
```

Case #3: in case of PEAP0 and MSCHAPV2 for WPA-Enterprise.

```
AT+WFENTAP='WPA-Ent-AP-SSID',10,2,1,1
AT+WFENTLI='WPA-Ent_User_ID','WPA-Ent_PWD'
AT+RESTART
```

2.6 Advanced Function Commands

2.6.1 MQTT Commands

Table 9 shows commands for configuring MQTT client parameters. After running the commands, restart the MQTT client for applying the configuration.

Table 9. MQTT configuration command list

Command	Parameters	Description
AT+NWMQBR	<host_name>,<port>	Set the host name (or IP address) and the port number of the MQTT broker. ■ <host_name>: Broker's domain name, or IP address ■ <port>: Broker's port number Response: OK or ERROR Prerequisite ■ The MQTT client should be disabled (+NWMQCL:0). Note: ■ The broker host name (or IP address) and port configured are stored in the NVRAM. ■ Restart the MQTT to apply the new configuration.
	?	Get the host name or IP address and the port number of the MQTT broker. Response: +NWMQBR:<host_name>,<port>
	(none)	
	Example AT+NWMQBR=192.168.0.65,1884 OK AT+NWMQBR=? +NWMQBR:192.168.0.65,1884 OK	
AT+NWMQQOS	<qos>	Set the MQTT QoS level. <qos>: 0 (at most once), 1 (at least once), 2 (exactly once) Response: OK or ERROR Prerequisite ■ The MQTT client should be disabled (+NWMQCL:0). Note: Restart the MQTT to apply the new configuration.
	?	Get the MQTT QoS level. Response: +NWMQQOS:<qos>
	(none)	
	Example AT+NWMQQOS=1 OK	

Command	Parameters	Description
	AT+NWMQQOS +NWMQQOS:1 OK	
AT+NWMQTLS	<tls>	Enable/disable the MQTT TLS function. <tls>: 1 (enable), 0 (disable) Response: OK or ERROR Prerequisite ■ Certificates should be stored. See Table 4. ■ The MQTT client should be disabled (+NWMQCL:0). Note: Restart MQTT to apply the new configuration.
	?	Get MQTT TLS status. Response: +NWMQTLS:<tls>
	(none)	
	Example AT+NWMQTLS=1 OK AT+NWMQTLS +NWMQQOS:1 OK	
AT+NWMQCS	<clean_session>	Set clean session mode. <clean_session>: 1(session cleared), 0(session retained) Response: OK or ERROR Prerequisite ■ The MQTT client should be disabled (+NWMQCL:0). Note: ■ To disable/enable this feature, use __MQTT_CLEAN_SESSION_MODE_SUPPORT__ definition. ■ If __MQTT_CLEAN_SESSION_MODE_SUPPORT__ is not defined, the MQTT client always connects to a MQTT broker in CleanSession=1 mode. ■ Reconnect the MQTT to apply the new configuration. ■ See Section 2.6.1.3 MQTT Example: Using CleanSession=0.
	?	Get clean session status. Response: +NWMQCS:<clean_session>
	(none)	
	Example AT+NWMQCS=1 OK AT+NWMQCS=? +NWMQCS:1 OK	
AT+NWMQTS	<num>,<topic#1>, <topic#2>, …	Set the topic(s) of the MQTT subscriber. ■ <num>: Number of topics. The maximum subscriber topic number is 4. ■ <topic#n>: MQTT subscriber topic(s). Max topic length = 64 Response: OK or ERROR Prerequisite ■ The MQTT client should be disabled (+NWMQCL:0). Note: ■ Return "ERROR:0x50028E when there is no subscriber topic set. ■ After running the command, the previously configured subscriber topic (s) is(are) cleared and set to new one(s). ■ Restart the MQTT to apply the new configuration.

Command	Parameters	Description
	?	Get the MQTT subscriber topic(s). Response: +NWMQTS:<num>,<topic#1>,<topic#2>…
	(none)	
	Example AT+NWMQTS=? ERROR:0x50028E AT+NWMQTS=1,rrq61x_sub OK AT+NWMQTS=? +NWMQTS:1,”rrq61x_sub” OK	
AT+NWMQATS	<topic>	Add the specified MQTT Subscriber topic to MQTT configuration. Prerequisite ■ The MQTT client should be disabled (+NWMQCL:0). Note: Query command (AT+NWMQATS=?) is not supported. If AT+NWMQATS=? is running, "?" is added as a topic.
	Example AT+NWMQATS=ABCD OK AT+NWMQTS=? +NWMQTS:1,"ABCD" OK	
AT+NWMQDTS	<topic>	Delete the specified topic from MQTT configuration. Prerequisite ■ The MQTT client should be disabled (+NWMQCL:0).
	Example AT+NWMQTS=? +NWMQTS:2,"ABCD",”EFGH” OK AT+NWMQDTS=ABCD OK AT+NWMQTS=? +NWMQTS:1,”EFGH” OK	
AT+NWMQTP	<topic>	Set the default topic of the MQTT publisher. <topic>: MQTT publisher topic Response: OK or ERROR Prerequisite ■ The MQTT client should be disabled (+NWMQCL:0). Note: ■ ERROR: 5243542 means No Publish topic exists. ■ This default Publisher topic is used when sending a message (see Table 10 for AT+NWMQMSG) without an explicit topic specified. ■ Restart the MQTT to apply the new configuration.
	?	Get the MQTT publisher topic. Response: +NWMQTP:<topic>
	(none)	
	Example AT+NWMQTP=? ERROR:0x500296 AT+NWMQTP=rrq61x_pub	

Command	Parameters	Description
	OK AT+NWMQTP=? +NWMQTP:rrq61x_pub OK	
AT+NWMQMSGFMVER	<format_version>	Specify message format version that is used for received PUBLISH message (+NWMQMSG) <format_version>: 0 (default), 1 (new) 0 (default) : +NWMQMSG:<message>,<topic>,<length> 1 (new) : +NWMQMSG:<topic>,<length>,<message> Note: Restart the MQTT client to apply the new configuration.
	?	Show the message format version currently set.
	(none)	
	Example AT+NWMQMSGFMVER=? +NWMQMSGFMVER:0 OK AT+NWMQMSGFMVER=1 OK AT+NWMQMSGFMVER =? +NWMQMSGFMVER:1 OK	
AT+NWMQV311	<use_v311>	Use MQTT protocol v3.1.1. The default is v3.1. <use_v311>: 1 (v3.1.1)/0 (v3.1) Prerequisite ■ The MQTT client should be disabled (+NWMQCL:0). Note: Restart the MQTT to apply the new configuration.
	?	Show the MQTT protocol version currently set.
	Example AT+NWMQV311=? +NWMQV311:0 OK AT+NWMQV311=1 OK AT+NWMQV311=? +NWMQV311:1 OK	
AT+NWMQPING	<period>	Set MQTT ping period. <period>: Ping period (second) Response: OK or ERROR Prerequisite ■ The MQTT client should be disabled (+NWMQCL:0). Note: Restart the MQTT to apply the new configuration.
	?	Get the current MQTT ping period. Response: +NWMQPING:<period>
	(none)	
	Example AT+NWMQPING=? +NWMQPING:600 OK AT+NWMQPING=300 OK	

Command	Parameters	Description
	AT+NWMQPING +NWMQPING:300 OK	
AT+NWMQCID	<client_id>	Set the MQTT Client ID. <client_id>: Client ID Response: OK or ERROR Prerequisite ■ The MQTT client should be disabled (+NWMQCL:0). Note: Restart the MQTT to apply the new configuration.
	?	Get the current MQTT Client ID. Response: +NWMQCID:<client_id>
	(none)	
	Example AT+NWMQCID=? +NWMQCID:rrq61k_cca4 // A default CID is used if CID is not stored in NVRAM. AT+NWMQCID=client-1 OK AT+NWMQCID +NWMQCID:client-1 OK	
AT+NWMQLI	<name>,<pw>	MQTT login information. <name>: ID <pw>: Password Response: OK or ERROR Prerequisite ■ The MQTT client should be disabled (+NWMQCL:0). Note: ■ ERROR: 5243543 means No username exists. ■ Restart the MQTT to apply the new configuration.
	?	Get the MQTT login information. Response: +NWMQLI:<name>,<pw>
	(none)	
	Example AT+NWMQLI=? ERROR:0x5002A1 AT+NWMQLI=rrq61x_user,12345678 OK AT+NWMQLI +NWMQLI:rrq61x_user,12345678 OK	
AT+NWMQAUTO	<auto>	Enable/Disable auto-start of the MQTT client at reboot. <auto>: 1 (Enable), 0 (Disable) Prerequisite ■ The MQTT client should be disabled (+NWMQCL:0). Note: ■ The default is 0 (disable). ■ Restart the MQTT to apply the new configuration.
	?	Get the MQTT client's auto-start configuration status. Response: +NWMQAUTO:<auto>
	(none)	
	Example AT+NWMQAUTO=?	

Command	Parameters	Description
	+NWMQAUTO:0 OK AT+NWMQAUTO=1 OK AT+NWMQAUTO +NWMQAUTO:1 OK	
AT+NWMQWILL	<topic>,<msg>,<qos>	Set the MQTT Will message. <topic>: Will topic <msg>: Will message <qos>: Will QoS. 0 (at most once), 1 (at least once), 2 (exactly once) Response: OK or ERROR Prerequisite ■ The MQTT client should be disabled (+NWMQCL:0). Note: ■ The MQTT Will message is not retained. ■ ERROR: 5243544 or 5243545 means topic or message is missing. ■ Restart the MQTT to apply the new configuration.
	?	Get the MQTT Will message. Response: +NWMQWILL:<topic>,<msg>,<qos>
	(none)	
	Example AT+NWMQWILL=? ERROR:0x500298 Or ERROR:0x500299 AT+NWMQWILL=rrq61x_will,bye,0 OK AT+NWMQWILL +NWMQWILL:rrq61x_will,bye,0 OK	
AT+NWMQDEL	(none)	Reset the MQTT configurations. Response: OK or ERROR Prerequisite ■ The MQTT client should be disabled (+NWMQCL:0). Note: ■ This command resets all MQTT configurations. ■ If the MQTT client is running, execute this command after the MQTT client is disabled by AT+NWMQCL=0.
	Example AT+NWMQDEL OK	
AT+NWMQTLSVER	<tls_ver>	Set MQTT TLS version. <tls_ver>: 0 (v1.2), 1 (v1.3), 2 (v1.2 and v1.3) Response: OK or ERROR Prerequisite ■ The MQTT client should be disabled (+NWMQCL:0). Note: ■ This command sets the TLS version used in the MQTT client. For example, if the Broker server supports only TLS v1.3, you can run AT+NWMQTLSVER=1 or AT+NWMQTLSVER=2. ■ If the MQTT client is running, execute this command after the MQTT

Command	Parameters	Description
		client is disabled by AT+NWMQCL=0.
	?	Query MQTT TLS version status. +NWMQTLSVER:<tls_ver>
	(none)	
	Example AT+NWMQTLSVER +NWMQTLSVER:0 OK AT+NWMQTLSVER=1 OK AT+NWMQTLSVER +NWMQTLSVER:1 OK	
AT+NWMQTLSBUFIN	<size>	Set MQTT TLS INCOMING buffer size. <size>: size in bytes Response: OK or ERROR Prerequisite ■ The MQTT client should be disabled (+NWMQCL:0). Note: ■ This command sets MQTT TLS incoming buffer size. TLS incoming buffer is used in decoding incoming TLS encrypted messages. If TLS incoming message size is bigger than MQTT TLS incoming buffer size, an error occurs. In this case, you can adjust MQTT TLS incoming buffer size using this command. ■ If the MQTT client is running, execute this command after the MQTT client is disabled by AT+NWMQCL=0.
	?	Query MQTT TLS version status. +NWMQTLSBUFIN:<size>
	(none)	
	Example AT+NWMQTLSBUFIN +NWMQTLSBUFIN:6144 OK AT+NWMQTLSBUFIN=8192 OK AT+NWMQTLSBUFIN=? +NWMQTLSBUFIN:8192 OK	
AT+NWMQTLSBUFOUT	<size>	Set MQTT TLS OUTGOING buffer size. <size>: size in bytes Response: OK or ERROR Prerequisite ■ The MQTT client should be disabled (+NWMQCL:0). Note: ■ This command sets MQTT TLS outgoing buffer size. TLS outgoing buffer is used in encrypting outgoing messages. If TLS outgoing message size is bigger than MQTT TLS outgoing buffer size, an error occurs. In this case, you can adjust MQTT TLS outgoing buffer size using this command. ■ If the MQTT client is running, execute this command after the MQTT client is disabled by AT+NWMQCL=0.

Command	Parameters	Description
	?	Query MQTT TLS version status. +NWMQTLSBUFOUT:<size>
	(none)	
	Example AT+NWMQTLSBUFOUT +NWMQTLSBUFOUT:4096 OK AT+NWMQTLSBUFOUT=5120 OK AT+NWMQTLSBUFOUT=? +NWMQTLSBUFOUT:5120 OK	
AT+NWMQTLSAUTH	<authmode>	Set the MQTT TLS Auth mode. <authmode>: ■ 0: Peer certification is not verified. This is the default setting. ■ 1: Peer certification is verified – optional. Cert verification result is decided – TLS handshake success or failure – by MQTT client. ■ 2: Peer certification is verified – mandatory, if cert verification fails, TLS handshake fails. Response: OK or ERROR Prerequisite ■ The MQTT client should be disabled (+NWMQCL:0). Note: ■ This command is applied only for TLS v1.2. ■ If the MQTT client is running, execute this command after the MQTT client is disabled by AT+NWMQCL=0.
	Example AT+NWMQTLSAUTH +NWMQTLSAUTH:0 OK AT+NWMQTLSAUTH=1 OK AT+NWMQTLSAUTH=? +NWMQTLSAUTH:1 OK	

Table 10. MQTT operation command list

Command	Parameters	Description
AT+NWMQCL	<mqtt_client>	Enable/disable the MQTT client. <mqtt_client>: 0 (disable), 1 (enable) Response: OK or ERROR Prerequisite ■ The RA6W1 should be connected to AP. Note: ■ If the system restarts, then the MQTT client is not started automatically because this command is for start/stop the MQTT client. ■ Set MQTT configuration parameters such as MQTT broker IP, port number, and subscriber topic, to complete before issuing this command. ■ After OK, the following operation result response message appear: ● +NWMQCL:1 – indicates connection successful. ● +NWMQCL:0 – indicates connection not successful. ● +NWMQCL:0,IN_RETRY – indicates MQTT client is retrying connection to Broker.

Command	Parameters	Description
	? (none)	Get the MQTT client status. Response: +NWMQCL:<mqtt_client>
	Example AT+NWMQCL=1 OK +NWMQCL:1 AT+NWMQCL +NWMQCL:1 OK AT+NWMQCL=0 OK +NWMQCL:0 AT+NWMQCL=1 OK +NWMQCL:0,IN_RETRY +NWMQCL:0,IN_RETRY +NWMQCL:1	
AT+NWMQMSG	<msg>[,<topic>]	Publish an MQTT message. ■ <msg>: Message to be published ■ <topic>: MQTT topic (optional) ■ Response: OK or ERROR ■ Operation Results: ■ Send Success: +NWMQMSGSND:1 ■ Send Failure: +NWMQMSGSND:0,<err_code> Prerequisite ■ The MQTT client should be enabled (+NWMQCL:1). Note: ■ The MQTT message is not retained. ■ If a single quotation is used in a message, it should be surrounded by double quotation marks. ■ In the default AT command image, the maximum total combined string length allowed for <msg> + <topic> should be less than or equal to 4114. So, if it needs to send a max length <msg> (4096 bytes long) with an explicit <topic> specified, the <topic> length should be 18 characters long or less. If it needs to send a message with the maximum length topic allowed (which is 128), send 3986 bytes <msg> in maximum. ■ Operation Results: +NWMQMSGSND:1 or +NWMQMSGSND:0,<err_code>. ■ Message publishing transactions (QoS 0, 1, 2) might take some time if network condition is not stable. ■ A new async response +NWMQMSGSND:1 or +NWMQMSGSND:0 that comes after OK indicates either completion of publish transaction or failure. ■ In CleanSession=1 mode, if the MQTT is disconnected, the host can immediately get +NWMQMSGSND:0, but in CleanSession=0 mode, +NWMQMSGSND:0 is not sent but instead the transaction resumes when the MQTT client re-connects. See Section 2.6.1.3 MQTT Example: Using CleanSession=0.
	Example AT+NWMQMSG=Hello world !!! OK +NWMQMSGSND:1 AT+NWMQMSG='{"car":"red", "type":"bus"}' OK +NWMQMSGSND:1 AT+NWMQMSG=Hello OK +NWMQMSGSND:0,-6 // Send failed because MQTT is not in connected state.	

Command	Parameters	Description
AT+NWMQMSGBIN	<is_default_topic>, <topic_len>, <topic>, <data_len>, <data>	Publish an MQTT message in binary format. <is_default_topic>: ■ 1 (default topic is used). ■ 0 (default topic is not used, instead, the next parameter specifies the topic). <topic_len>: String length of <topic>. ■ 0 if <is_default_topic> is 1. <topic>: Topic string. ■ 0 if <is_default_topic> is 1 <data_len>: length of <data> <data>: binary data
	Example: ; To use this command, make sure msg format version is 1 AT+NWMQMSGFMVER=1 OK ; Publish binary data (the length is 4) with the default topic AT+NWMQMSGBIN=1,0,0,4,<bin_data> OK +NWMQMSGSND:1 ; Publish binary data (length 4) with the topic “mytopic” AT+NWMQMSGBIN=0,7,mytopic,4,<bin_data> OK +NWMQMSGSND:1	
AT+NWMQUTS	<topic>	Unsubscribe from the specified topic. Prerequisite The MQTT client should be enabled (+NWMQCL:1). Note: ■ Enabled by default in the SDK. ■ This command should be run while the MQTT client is in a connected state with Broker.
	Example AT+NWMQUTS=ABCD OK	
AT+NWMQTT	<host_name>,<port>, <sub_topic>, <pub_topic>, <qos>,<tls>, <username>, <password>	Run the MQTT Client with options. After entering this command, the system reboots automatically. At reboot, the RA6W1 tries to connect to the MQTT broker after the Wi-Fi connection is successfully established. ■ <host_name>: Broker's domain name or IP address, ■ <port>: Broker's port number ■ <sub_topic>: MQTT subscriber topic ■ <pub_topic>: MQTT publisher topic ■ <qos>: MQTT QoS level ■ <tls>: Enable/disable MQTT TLS. 1 (enable), 0 (disable) ■ <username>: Login ID (optional) ■ <password>: Login password (optional) Response: OK or ERROR Prerequisite ■ The MQTT client should be disabled (+NWMQCL:0). Note: After the system reboot, operation result is sent, see +NWMQCL response.
	Example AT+NWMQTT=192.168.0.65,1884,rrq61x_sub,rrq61x_pub,0,0 //The following are logs after the RA6W1 reboot. +INIT:DONE,0 +WFJAP:1,'test_ap_ssid',192.168.0.88 +NWMQCL:1	

Table 11 shows optional MQTT configuration commands for the MQTT brokers that require TLS ALPN, SNI, or Cipher Suite information from the MQTT Client at the connection stage.

Table 11. MQTT optional configuration commands

Command	Parameters	Description
AT+NWMQALPN	<num>, <alpn#1>, <alpn#2>, <alpn#3>	Set the TLS ALPN protocol name for the MQTT. ■ <num>: Number of ALPNs. The maximum number of ALPN is three. ■ <alpn#n>: TLS ALPN protocol name. The maximum length of each ALPN protocol name is 24. Response: OK or ERROR Prerequisite ■ The MQTT client should be disabled (+NWMQCL:0). Note: ■ If __MQTT_TLS_OPTIONAL_CONFIG__ is enabled in the SDK, the command is enabled. ■ ERROR: 5243524 means No ALPN is set.
	?	Get the TLS ALPN(s) that are set. Response: +NWMQALPN:<num>,<alpn#1>,<alpn#2>,<alpn#3>
	Example AT+NWMQALPN=? ERROR: 5243524 AT+NWMQALPN=2,alpn-protrol-name-an,alpn-protocol-name-ax OK AT+NWMQALPN +NWMQALPN:2,"alpn-protrol-name-an","alpn-protocol-name-ax" OK	
AT+NWMQSNI	<sni>	Set TLS SNI for the MQTT. <sni>: Server Name Indication. The maximum length of SNI is 64. Response: OK or ERROR Prerequisite ■ The MQTT client should be disabled (+NWMQCL:0). Note: ■ If __MQTT_TLS_OPTIONAL_CONFIG__ is enabled in the SDK, the command is enabled. ■ ERROR: 5243528 means No SNI is set.
	?	Get the TLS SNI that is set. Response: +NWMQSNI:<sni>
	Example AT+NWMQSNI=? ERROR: 5243528 AT+NWMQSNI=a38a9rhiu3roqb-ats.myserver.com OK AT+NWMQSNI +NWMQSNI: a38a9rhiu3roqb-ats.myserver.com OK	
AT+NWMQCSUIT	<cipher suite 1>, <cipher suite 2>, …	Set TLS Cipher suites. <cipher suite>: A hex decimal value of cipher suite. See Appendix D RA6W1 Cipher Suites. The maximum number of cipher suites is 17. Response: OK or ERROR Prerequisite ■ The MQTT client should be disabled (+NWMQCL:0). Note: ■ If __MQTT_TLS_OPTIONAL_CONFIG__ is enabled in the SDK, the command is enabled.

Command	Parameters	Description
		■ ERROR:5243530 or 5243531 means No CSUIT info is set. ■ The hex pre-fix "0x" should be removed when one is typed. ■ The RA6W1 does not support all the cipher suites because of memory limitation. Contact Renesas Electronics for using other cipher suites that are not specified in Appendix D RA6W1 Cipher Suites.
	?	Get TLS cipher suites that are set. Response: +NWMQSNI:<number of cipher suites>,<cipher suite 1>,<cipher suite 2>…
	Example AT+NWMQCSUIT=? ERROR: 5243530 or ERROR: 5243531 AT+NWMQCSUIT=c024,c023,c00a,c009,c00d,c032 OK AT+NWMQCSUIT +NWMQCSUIT:6,c024,c023,c00a,c009,c00d,c032 OK	

Table 12. MQTT response list

Response	Parameters	Description
+NWMQCL	<result> [,TOO_LONG_MSG_RX] [,IN_RETRY]	The result of the MQTT client connection. ■ <result>: 0 (disconnected), 1 (connected) Example: ■ +NWMQCL:1 If MQTT connection to the MQTT broker is successfully established ■ +NWMQCL:0 If the MQTT connection is NOT successfully established ■ +NWMQCL:0,IN_RETRY If the MQTT client is in connection retrial state ■ +NWMQCL:0,TOO_LONG_MSG_RX Can be sent when the MQTT is disconnected by unsupported message length only if the current MQTT connection is with clean_session=0 and QoS greater than or equal to 1.

	Example
	// When MQTT connection to the MQTT broker is successfully established
	+NWMQCL:1
	// When MQTT broker is down
	+NWMQCL:0
	Note:
	■ The RA6W1 debug console log (UART1).
	■ When MQTT connection to the MQTT broker is successfully established, the RA6W1 sends +NWMQCL:1 message to MCU (or AT command console). At this moment, the following log appears:
	>>> MQTT Client connection OK
	■ When the MQTT broker is down, the RA6W1 sends +NWMQCL:0 message to MCU (or AT command console) after retrying connection. In the console log, the following logs appear:
	Failed to receive pkt. (0x38)
	Failed to read pkt(0x7880)
	MQTT Client disconnectedi ... (state=6)
	[SUB] REQ mqtt_restart (count=1)
	Connecting FAIL (0x38)
	Unable to connect (The connection was refused.)
	…	

Response	Parameters	Description

[SUB] REQ mqtt_restart (count=5)
Connecting FAIL (0x38)
Unable to connect (The connection was refused.)
[SUB] MAX Retry (Retry Cnt=6).

- To get **Operation Result**, it can take more time if the RA6W1connection reattempt occurs depending on the test network condition.
- This message is also sent after AT+NWMQTT is run or if any MQTT configuration command is run and then the system is restarted.
  - The RA6W1 restarts if the AT command format (for example, AT+NWMQTT) is OK.
    - +INIT:DONE,0 message is sent as the RA6W1 boots up.
    - If usage of the AT command (for example, AT+NWMQTT) is not valid, the RA6W1 sends an **ERROR** message without restarting.
  - TheRA6W1 tries to connect to the AP after the reboot.
    - +WFJAP:0,<reason> or +WFJAP:1,'<SSID>',<IP Address> as result of the Wi-Fi connection.
    - If the Wi-Fi connection information such as SSID or key is NOT stored correctly in the RA6W11 NVRAM, +WFJAP:x response is NOT sent and the MQTT connection is NOT attempted. Because the MQTT connection needs a successful Wi-Fi connection first.
  - The RA6W1 tries to connect to the MQTT broker after the Wi-Fi connection is established. The MQTT broker information is stored in NVRAM. Connection result – +NWMQCL:0 or +NWMQCL:1 – is sent over UART2 as a result.
- +NWMQCL:0,IN_RETRY
  - If the 1st trial of connecting to Broker is failed, MQTT client retries the connection attempt. Every time the connection attempt fails, +NWMQCL:0,IN_RETRY comes. If DPM is not used, MQTT client tries connection retry up to six consequtive times. If DPM is used, MQTT client tries connection retry up to 3 consequtive times and then use wakeup-sleep cycle (“sleep -> wakeup -> try MQTT connection -> sleep”) up to 6 times (the interval between sleep is 5 seconds). At each wakeup, if connection attempt fails, +NWMQCL:0 is sent to ATCMD host.
- +NWMQCL:0,TOO_LONG_MSG_RX
  - If the current mqtt_client connection with Broker is configured with **clean_session=0** and **QoS is greater than or equal to 1**, +NWMQCL:0,TOO_LONG_MSG_RX can be sent to AT command host (exceptional case). This message indicates that mqtt_client is disconnected by receiving a message that exceeds the message length limit (2048) of RA6W1 MQTT client. What AT command host should do, in this situation, is configuring clean_session to 1 and connect to Broker to delete the message (in the MQTT broker) and then disconnect from Broker and reconnect with clean_session=0 again to start over (a kind of Recovery). According to MQTT Spec of clean_session=0, Broker keeps sending a message that is not ACKed by the client. In this case, the long message (valid for Broker perspective, but not valid for RA6W1 MQTT client perspective) can repeatedly be sent to RA6W1 MQTT client unless connection with clean_session=1 is made from RA6W1 MQTT client.
  - Example recovery flow on receipt of +NWMQCL:0,TOO_LONG_MSG_RX.

```
...
// MQTT client is disconnected by receiving a message with unsupported length
+NWMQCL:0,TOO_LONG_MSG_RX
AT+NWMQCS=1 // set clean_session=1
OK
// connect to Broker (to clear the long message in the server)
AT+NWMQCL=1
OK

+NWMQCL:1
AT+NWMQCL=0 // Disconnect from Broker
OK
+NWMQCL:0
```

Response	Parameters	Description
	AT+NWMQCS=0 // Set clean_session=0 OK AT+NWMQCL=1 // Connect to Broker with clean_session=0 OK +NWMQCL:1	
+NWMQMSG	<msg>,<topic>,<length>	Received the MQTT message. ■ <msg>: Message data ■ <topic>: Received topic ■ <length>: Message length When the RA6W1 receives a message from the MQTT publisher, the following message is sent from the RA6W1 to AT command console: +NWMQMSG:Hello world!!!!,rrq61x_sub,15 Note: The MQTT client is in a connected state with the broker (+NWMQCL:1).

2.6.1.1 MQTT Client Connection Example

Configure the parameters and start the MQTT Client (after Wi-Fi connection):

```
AT+NWMQBR=172.16.0.1,1884
AT+NWMQTS=1,rrq61x_sub
AT+NWMQTP=rrq61x_pub
AT+NWMQAUTO=1
AT+NWMQCL=1
```

If the connection is successful, the following is shown:

```
+NWMQCL:1
```

If RA6W1receives a PUBLISH from a broker, the following is shown:

```
+NWMQMSG:Hello World,rrq61x_sub,11
```

RA6W1 can send a PUBLISH to a broker. Type the following command:

```
AT+NWMQMSG='Hello I'm RRQ61X'
```

2.6.1.2 MQTT TLS Connection Example

To Configure the MQTT parameters:

```
AT+NWMQBR=172.16.0.1,1884
AT+NWMQTS=1,rrq61x_sub
AT+NWMQTP=rrq61x_pub
AT+NWMQAUTO=1
AT+NWMQCL=1
```

To check the validity of a certificate, RA6W1 should set the exact current time:

```
AT+TIME=yyyy-mm-dd,hh:mm:ss
```

And save the certificate and private key if needed. (See <ESC>C in Table 4)
After all settings are made, start the MQTT client:

```
AT+NWMQCL=1
```

2.6.1.3 MQTT Example: Using CleanSession=0

2.6.1.3.1 CleanSession=0 Mode

When an MQTT Client (or MQTTC) establishes connection with an MQTT broker (Broker onward), there are two types of session: CleanSession=1 and CleanSession=0.
CleanSession=1: default session type. When Broker gets a connect request from an MQTTC that tries to connect with an option "CleanSession=1" (which is default config on the RA6W1), Broker treats the connection as a "new" session. If there is any existing session associated with the same client_id found, Broker clears that previous session and creates a new one with the client_id.
CleanSession=0: when Broker gets a connect request from an MQTTC that tries to connect with an option CleanSession=0, Broker tries to find a session (session data) with the same client_id first. If it finds one, it keeps using that session for the new MQTTC.
While MQTTC is in operation with Broker, there might be times when the TCP connection gets unstable and disconnected (for example, MQTT ping failed) which might cause some messages that are published to Broker at that specific disconnected time cannot be delivered to a subscriber. If new messages (with QoS > 0) are published to Broker and for sessions that are configured in CleanSession=0, Broker retains and re-send them when the MQTTC is re-connected. The MQTTC (if CleanSession=0 is enabled) also should retain the state of the unfinished/unacked messages until reconnection.

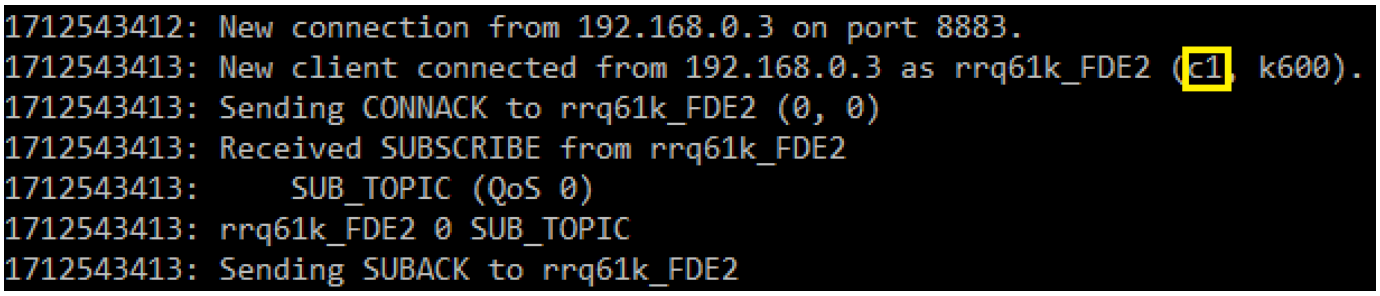


Figure 1. Broker console – CleanSession=1 connection

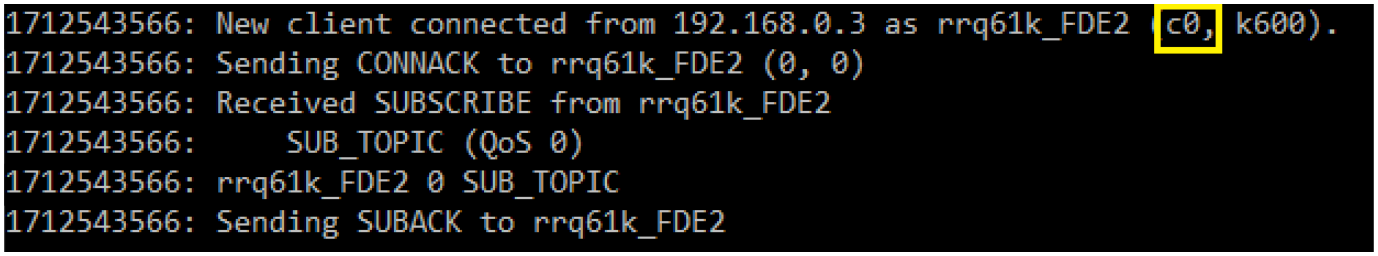


Figure 2. Broker console – CleanSession=0 connection

Even with CleanSession=0 connection, Broker does not maintain session data if MQTT is disconnected in the following cases.

- If a new message is published with QoS 0 after MQTT is disconnected.
- If MQTTC connection QoS is 0.

The RA6W1 supports CleanSession=0 mode in the following way:

- CleanSession=0 feature is enabled.
- If a customer application decides that **QoS 1 or Qos 2 and CleanSession=0** is used in their application, the message (payload) size (both TX and RX) should be predetermined. By default, 100 bytes are defined.
  #define MQTT_MSG_TBL_PRESVD_MAX_PLAYLOAD_LEN 100
- Depending on the application's expected maximum payload size while operation, other values can be defined.
- The default configuration (payload_len: 100, max_count: 10) allocates about 1.9 KB.
- Search the following compiler options in custom_config_sdk.h.
  //max payload length of a preserved message
  #define MQTT_MSG_TBL_PRESVD_MAX_PLAYLOAD_LEN 100
  // max number of preserved messages
  #define MQTT_MSG_TBL_PRESVD_MAX_MSG_CNT 10
- ▪ Supported command to set CleanSession mode: AT+NWMQCS=<1|0>

CleanSession and QoS matrix table for PUBLISH RX

Table 13. CleanSession and QoS matrix in message RX

Subscriber			Unacked message delivery (After MQTT reconnection)	QoS (Effective actual)	Publisher message's QoS
Case	Clean session	QoS			
1	1	0	X	0	0
2	1	1	X	0	0
3	1	2	X	0	0
4	1	0	X	0	1
5	1	1	X	1	1
6	1	2	X	1	1
7	1	0	X	0	2
8	1	1	X	1	2
9	1	2	X	2	2
10	0	0	X	0	0
11	0	1	X	0	0
12	0	2	X	0	0
13	0	0	X	0	1
14	0	1	O	1	1
15	0	2	O	1	1
16	0	0	X	0	2
17	0	1	O	1	2
18	0	2	O	2	2

With CleanSession=1, no unacked message delivery occurs when MQTT reconnects happen (marked as x).
With CleanSession=0, only cases of 14, 15, 17, and 18 make message redeliver for messages that were delivered to Broker while the MQTTC was offline (marked as O).

CleanSession and QoS matrix table for PUBLISH TX

- Expectation 1 – the application assumes that it failed to send a message and waits until MQTT gets re-connected.
- Behavior 1 – the application sends messages again.
- Expectation 2 – the application assumes that it failed to send a message but resumed sending the message when

MQTT reconnected.

- Behavior 2 – the application simply waits as MQTT sends the message automatically.

Table 14. CleanSession and QoS matrix in message TX

Publisher			Expectation if MQTT gets disconnected (while QoS 1/2 message is not fully acked or QoS 0 send is being sent)	Behavior expected when MQTT client re-connected
Case	Clean session	QoS		
1	1	0	Expectation 1	Behavior 1
2	1	1	Expectation 1	Behavior 1
3	1	2	Expectation 1	Behavior 1
4	0	0	Expectation 1	Behavior 1
5	0	1	Expectation 2	Behavior 2
6	0	2	Expectation 2	Behavior 2

When publishing a message from RA6W1, the application's expectation and action/behavior might be different if CleanSession=0 and QoS 1 or 2 are used in some specific cases.
In normal network conditions, there is no difference in message send behavior between CleanSession=0 and CleanSession=1.
In some abnormal cases where QoS 1/2's ACK message (PUBACK, PUBREC, PUBREL, or PUBCOMP) get lost because of some bad network conditions (which can cause MQTTC re-connection), CleanSession=0 can recover the previous message state and resume the communication with Broker.
However, if CleanSession=1 is used when MQTT Client is disconnected, it can safely re-transmit the message when MQTT Client reconnects. Depending on use cases of applications/host applications, either approach (CleanSession=0 or CleanSession=1) can be used.

2.6.1.3.2 Connect with CleanSession=0

To activate **CleanSession=0 support mode** in the RA6W1, QoS should be 1 or 2 and CleanSession option should be set to 0. If either option (CleanSession and QoS) is not set as above, CleanSession=0 support mode is disabled.

```
AT+NWMQQOS=2
OK
AT+NWMQCS=0
OK
AT+NWMQCL=1
OK

+NWMQCL:1
```

2.6.1.3.3 Restart CleanSession=0 test

If it needs to re-test (fresh new test) with CleanSession=0 mode, depending on the previous session type, it might need Broker to clear the previous session.
The reason is because an MQTTC connects with CleanSession=0, Broker does not delete the session data until the MQTT Client re-connects with CleanSession=1.
Case 1: Previous session is CleanSession=1 and must restart a new CleanSession=0 test.

```
AT+NWMQCL=0
OK
AT+NWMQCS=0
OK
AT+NWMQCL=1
OK
```

```
+NWMQCL:1
```

Case 2: Previous session is CleanSession=0 and needs to re-test another CleanSession=0 test run.

```
AT+NWMQCL=0
+NWMQCL:0

OK
AT+NWMQCS=1
OK
AT+NWMQCL=1
OK

+NWMQCL:1
AT+NWMQCL=0
+NWMQCL:0

OK
AT+NWMQCS=0
OK
AT+NWMQCL=1
OK

+NWMQCL:1
```

2.6.1.3.4 PUBLISH RX Test Steps

The test steps are:

1. RA6W1: connect to Broker.
2. Publisher: send one or two messages.
3. RA6W1: check if the messages are received.
4. RA6W1: disconnect from Broker.
5. Publisher: send one or two messages (for example, msg_A).
6. RA6W1: reconnect to Broker.
7. RA6W1: check if msg_A (sent while the RA6W1 is offline) is received.

NOTE

- Mosquitto broker (Broker), Mosquitto publisher (Publisher), and RA6W1 (Subscriber) are used for the test.
- Message length from publisher should be less than or equal to 100. If messages are no longer sent, they cannot be restored properly when MQTT is reconnected.

2.6.1.3.5 PUBLISH RX Test Steps – Example 1

This is the test step for case 15, see Table 13.
[RA6W1] connect MQTT Client with CleanSession=0 and QoS 2.

```
AT+NWMQQOS=2
OK
AT+NWMQCS=0
OK
AT+NWMQCL=1
OK

+NWMQCL:1
```

[Other Publisher] publish messages.

```
C:\mosquitto>mosquitto_pub -h 192.168.0.230 -p 8883 --cafile cas.pem --cert wifiuser.pem --key wifiuser.key --tls-version tlsv1 --insecure -q 2 -t SUB_TOPIC -m "Hello_q2" C:\mosquitto>mosquitto_pub -h 192.168.0.230 -p 8883 --cafile cas.pem --cert wifiuser.pem --key wifiuser.key --tls-version tlsv1 --insecure -q 2 -t SUB_TOPIC -m "Hello_q2_2"
```

[RA6W1] check whether the messages are successfully received.

```
+NWMQMSG:Hello_q2,SUB_TOPIC,8

+NWMQMSG:Hello_q2_2,SUB_TOPIC,10
```

[RA6W1] disconnect from Broker.

```
AT+NWMQCL=0
+NWMQCL:0

OK
```

[Other Publisher] publish two messages (while the RA6W1 is in disconnected state).

```
C:\mosquitto>mosquitto_pub -h 192.168.0.230 -p 8883 --cafile cas.pem --cert wifiuser.pem --key wifiuser.key --tls-version tlsv1 --insecure -q 2 -t SUB_TOPIC -m "Hello_q2_3" C:\mosquitto>mosquitto_pub -h 192.168.0.230 -p 8883 --cafile cas.pem --cert wifiuser.pem --key wifiuser.key --tls-version tlsv1 --insecure -q 2 -t SUB_TOPIC -m "Hello_q2_4"
```

[RA6W1] reconnect to Broker and check if the two messages that are published while the RA6W1 is in disconnected state are received successfully.

```
AT+NWMQCL=1
OK

+NWMQCL:1

+NWMQMSG:Hello_q2_3,SUB_TOPIC,10

+NWMQMSG:Hello_q2_4,SUB_TOPIC,10
```

2.6.1.3.6 PUBLISH TX Test Steps

The test steps are:

1. RA6W1: connect to Broker.
2. RA6W1: send a message.
3. RA6W1: check if the message is sent successfully.

NOTE

Message length fromRA6W1 should be less than or equal to 100 bytes for case 5 and 6 configuration. Sending longer messages returns failure. For cases other than case 5 or 6, message length limit is 2048 bytes.

2.6.1.3.7 PUBLISH TX Test Steps – Example

This is the test step for case 6.

```
AT+NWMQQOS=2
OK
AT+NWMQCS=0
OK
AT+NWMQCL=1
OK

+NWMQCL:1
AT+NWMQMSG=hello_q2
OK

+NWMQMSGSND:1
```

2.6.2 HTTP-Client Commands

Table 15. HTTP-client command list

Command	Parameters	Description
AT+NWHTC	<url>,<method> (,<body>)	Start the HTTP client with options. ■ <url>: HTTP server address ■ <method>: GET, POST or PUT ■ <body>: Body for POST and PUT methods, omitted for other methods. For JSON type, enclose the message with the single quotation - <'body'> Prerequisite ■ The RA6W1 should be connected to AP.

	Example 1
	AT+NWHTC=http://httpbin.org/get,get
	OK
	+NWHTCDATA:295,{
	"args": {},…
	Example 2
	AT+NWHTC=http://httpbin.org/post,post,HTTP-Client POST method sample test!
	OK
	+NWHTCDATA:424,{
	"args": {},
	"data": "HTTP-Client POST method sample test!",
	…
	For JSON type,
	AT+NWHTC=http://httpbin.org/post,post,'{ username: "aaa", password: "1234"}'
	OK
	+NWHTCDATA:432,{
	"args": {},
	"data": "{ username: \"aaa\", password: "1234\"}",…	

	<url>,message, <'header+body'>	You can directly input header and body as plain text. Line feeds and carriage returns are inserted as \r\n. <url>: HTTP server address message: Use the message as a fixed option (not the http method) <'header+body'>: Enter a plain text string in the form of 'header+body' Prerequisite

Command	Parameters	Description
		■ The RA6W1 should be connected to AP.

	Example 1: GET method request (header)
	AT+NWHTC=http://httpbin.org/get,message,'GET /get HTTP/1.1\r\nHost: httpbin.org\r\nConnection: Close\r\n\r\n'
	OK
	+NWHTCDATA:197,{
	"args": {},
	"headers": {…
	Example 2: POST method request (header+body)
	AT+NWHTC=http://httpbin.org/post,message,'POST /post HTTP/1.1\r\nHost: httpbin.org\r\nAccept: */*\r\nContent-Length: 10\r\nConnection: Close\r\n\r\nHelloWorld\r\n'
	OK
	+NWHTCDATA:322,{
	"args": {},
	"data": "HelloWorld",
	…
	For JSON type,
	AT+NWHTC=http://httpbin.org/post,message,'POST /post HTTP/1.1\r\nHost: httpbin.org\r\nContent-Type: application/json\r\nContent-Length: 40\r\nConnection: Close\r\n\r\n{ username: "aaa", password: "1234"}\r\n'
	OK
	+NWHTCDATA:375,{
	"args": {},
	"data": "{ username: \"aaa\", password: "1234\"}",…	

AT+NWHTCSTLSVER	<tls_ver>	Set the TLS version. tls_ver: 0 (v1.2), 1 (v1.3), 2 (v1.2 and v1.3) Note: It must be set up before connecting to the server.
	Example AT+NWHTCSTLSVER 0 OK AT+NWHTCSTLSVER 1 OK AT+NWHTCSTLSVER 2 OK	
AT+NWHTCSNI	<sni>	Set the server name indication. <sni>: Server name Note: It must be set up before connecting to the server.
	Example AT+NWHTCSNI=httpbin.org OK	
AT+NWHTCALPN	<alpn_number>,<alpn1>, <alpn2>,<alpn3>	Set the application layer protocol negotiation. ■ <alpn_number>: Number of alps ■ <alpn1>: First alpn ■ <alpn2>: Second alpn ■ <alpn3>: Third alpn Note: It must be set up before connecting to the server.
	Example AT+NWHTCALPN=1,http/1.1 OK	

Command	Parameters	Description
	AT+NWHTCALPN=2,http/1.1,h2 OK AT+NWHTCALPN=3,http/1.0,h2,h2c OK	
AT+NWHTCSNIDEL	(none)	Delete the saved SNI. Note: It must be set up before connecting to the server.
	Example AT+NWHTCSNIDEL OK	
AT+NWHTCALPNDEL	(none)	Delete all saved ALPNs. Note: It must be set up before connecting to the server.
	Example AT+NWHTCALPNDEL OK	
AT+NWHTCTLSAUTH	<tls_auth_mode>	Set the certificate verification mode. ■ #define MBEDTLS_SSL_VERIFY_NONE 0 ■ #define MBEDTLS_SSL_VERIFY_ OPTIONAL 1 ■ #define MBEDTLS_SSL_VERIFY_ REQUIRED 2 Note: It must be set up before connecting to the server.
	Example AT+NWHTCTLSAUTH=0 OK AT+NWHTCTLSAUTH=1 OK AT+NWHTCTLSAUTH=2 OK	

Table 16. HTTP-client response list

Response	Parameters	Description
+ NWHTCSTATUS	<status>	Return status along with the received payload according to the requested method. <status>: 0 is successful See Appendix B HTTP Client Result Codes. Example: +NWHTCSTATUS:0
+NWHTCDATA	<data size,>	Insert the size information of data received only from AT+NWHTC command. An integer data size and a comma are inserted, and the actual received data is after that. Example: **+NWHTCDATA:426,**HTTP/1.1 200 OK

2.6.2.1 HTTP-Client Connection Example

2.6.2.1.1 GET Method Request

```
AT+NWHTC=http://httpbin.org/get,get

OK
+NWHTCDATA:295,{
  "args": {},
  "headers": {
    "Accept": "*/*",
    "Host": "httpbin.org",
    "User-Agent": "lwIP/2.1.3 (http://savannah.nongnu.org/projects/lwip)",
    "X-Amzn-Trace-Id": "Root=1-673d6a68-5e62f214521796db3e7c4164"
  },
  "origin": "61.35.35.173",
  "url": "http://httpbin.org/get"
}

+NWHTCSTATUS:0
```

2.6.2.1.2 POST Method Request

```
AT+NWHTC=http://httpbin.org/post,post,HTTP-Client POST method sample test!

OK
+NWHTCDATA:424,{
  "args": {},
  "data": "HTTP-Client POST method sample test!",
  "files": {},
  "form": {},
  "headers": {
    "Accept": "*/*",
    "Content-Length": "36",
    "Host": "httpbin.org",
    "User-Agent": "lwIP/2.1.3 (http://savannah.nongnu.org/projects/lwip)",
    "X-Amzn-Trace-Id": "Root=1-673d6a7f-794f708b37d31bf67556cc7c"
  },
  "json": null,
  "origin": "61.35.35.173",
  "url": "http://httpbin.org/post"
}

+NWHTCSTATUS:0
```

2.6.2.1.3 GET/POST Method Request Using Message Option

```
AT+NWHTC=http://httpbin.org/get,message,'GET /get HTTP/1.1\r\nHost: httpbin.org\r\nConnection:
Close\r\n\r\n'

OK
+NWHTCDATA:197,{
  "args": {},
```

```
  "headers": {
    "Host": "httpbin.org",
    "X-Amzn-Trace-Id": "Root=1-673d6a98-5fd80f47311b2dc106878a7c"
  },
  "origin": "61.35.35.173",
  "url": "http://httpbin.org/get"
}

+NWHTCSTATUS:0

AT+NWHTC=http://httpbin.org/post,message,'POST /post HTTP/1.1\r\nHost: httpbin.org\r\nAccept:
*/*\r\nContent-Length: 10\r\nConnection: Close\r\n\r\nHelloWorld\r\n'

OK
+NWHTCDATA:322,{
  "args": {},
  "data": "HelloWorld",
  "files": {},
  "form": {},
  "headers": {
    "Accept": "*/*",
    "Content-Length": "10",
    "Host": "httpbin.org",
    "X-Amzn-Trace-Id": "Root=1-673d6b0d-0455ec727ed2a59e26ab9905"
  },
  "json": null,
  "origin": "61.35.35.173",
  "url": "http://httpbin.org/post"
}

+NWHTCSTATUS:0
```

2.6.3 HTTP-Server Commands

Table 17. HTTP-server command list

Command	Parameters	Description
AT+NWHTS	<flag>	Start or stop the HTTP(S) server depending on the option. <start>: 1 (start), 0 (stop) Response: OK or ERROR Prerequisite ■ The RA6W1 should be connected to AP.
	Example AT+NWHTS=1 OK	

2.6.3.1 HTTP/HTTPS-Server Start Example

```
AT+NWHTS=1
OK
```

2.6.4 WebSocket-Client Commands

Table 18. WebSocket-client command list

Command	Parameters	Description
AT+NWWSC	<operation>,<uri> (<msg>)	Start the WebSocket client with options. ■ <operation>: connect, send, or disconnect ■ <uri>: WebSocket server address ■ <msg>: Request message Prerequisite ■ The RA6W1 should be connected to AP.
	Example 1 AT+NWWSC=connect,ws://192.168.86.182:8080 +NWWSC:1 Example 2 AT+NWWSC=connect,ws://[fd96:8dfc:9995::60a]:8080 +NWWSC:1 Example 3 AT+NWWSC=send,Send Message Test OK Example 4 AT+NWWSC=disconnect +NWWSC:0	

Table 19. WebSocket-client response list

Response	Parameters	Description
+NWWSC	<status>(<opcode>, <received msg length>, <received msg>)	Return status along with the received payload. <status> ■ 0 is disconnected. ■ 1 is connected. <opcode> ■ Continuation Frame: 0x00 ■ Text Frame: 0x01 ■ Binary Frame: 0x02 ■ Close Frame: 0x08 ■ Ping Frame: 0x09 ■ Pong Frame: 0x0a Example 1: +NWWSC:1 Example 2: +NWWSC:0 Example 3: +NWWSC:1,1,12,**Test Message**

2.6.5 OTA Commands

NOTE
When DPM mode is enabled and OTA update is in progress (firmware download is in progress), it does not enter DPM Sleep because SFlash write operation occurs. After downloading the firmware, the RA6W1 resumes to enter DPM Sleep mode.

Table 20. OTA command list

Command	Parameters	Description
AT+NWOTADW START	<fw_type>,<uri> [,<fw_name>]	Start downloading firmware from an OTA server. ■ <fw_type> : Set the firmware type: RTOS, BLE_ FW, MCU_FW, or CERT_KEY. ■ <uri>: Server address where the firmware is located. ■ <fw_name>: Optional. The maximum input size of fw_type is 7 bytes. MCU_FW is stored by default if not specified. (Only for MCU firmware). Response: +NWOTADWSTART:0x00 Prerequisite

Command	Parameters	Description
		■ The RA6W1/RA6W2RA6W2 should be connected to AP. Note: The parameter, fw_type should be lowercase.

	Example
	// RTOS download
	AT+NWOTADWSTART=rtos,https://server/RA6W1-xxxxxxxxxx-xxxxxxxxxx.img
	OK
	+NWOTADWSTART:0x00
	
	// Bluetooth firmware download (RA6W2 only)
	AT+NWOTADWSTART=ble_fw,https://server/ble_firmware.img
	OK
	+NWOTADWSTART:0x00
	
	// MCU firmware download
	AT+NWOTADWSTART=mcu_fw,https://server/mcu_firmware.img
	OK
	+NWOTADWSTART:0x00
	
	// MCU firmware download
	AT+NWOTADWSTART=mcu_fw,https://server/mcu_firmware.img
	OK
	+NWOTADWSTART:0x00
	
	// MCU firmware download (Input the name of MCU firmware within 8 characters. The default is "MCU_FW")
	AT+NWOTADWSTART=mcu_fw,https://server/mcu_firmware.img,MCU_FW
	OK
	+NWOTADWSTART:0x00
	
	// Cert Key download:
	AT+NWOTADWSTART=cert_key,https://server/ca.pem
	OK
	+NWOTADWSTART:0x00	

AT+NWOTARENEW	(none)	If the new downloaded firmware is good, it is applied to the system and reboot. Prerequisite ■ Download RTOS or Bluetooth images. Note: ■ The boot index should be changed automatically. ■ Reboot automatically after renewing is completed.
	Example AT+NWOTARENEW +NWOTARENEW:0x00	
AT+NWOTADWPROG	<fw_type>	Firmware download progress. <fw_type>: Set the firmware type: RTOS, BLE_FW, MCU_FW, or CERT_KEY. Response: +NWOTADWPROG:100

	Example
	// RTOS download progress:
	AT+NWOTADWPROG=rtos
	+NWOTADWPROG:100
	OK
	
	// MCU firmware download progress:
	AT+NWOTADWPROG=mcu_fw
	+NWOTADWPROG:100
	OK
	
	// Bluetooth firmware download progress (RA6W2 only):	

Command	Parameters	Description
	AT+NWOTADWPROG=ble_fw +NWOTADWPROG:100 OK // Cert Key download progress: AT+NWOTADWPROG=cert_key +NWOTADWPROG:100 OK	
AT+NWOTADWRESUME	<fw_type>,<uri> [,<fw_name>]	During an OTA firmware download, a power loss or Wi-Fi drop forces the legacy AT+NWOTADWSTART flow to discard everything and download the full image again. The resume command help to keep the downloaded portion in the flash and the transfer continues from where it stopped when you execute the command again. Currently RTOS firmware support is added.
	Example AT+NWOTADWRESUME =rtos,https://server/RA6W1-xxxxxxxxxx-xxxxxxxxxx.img OK +NWOTADWSTART:0x00	
AT+NWOTADWSTOP	(none)	Stop while downloading firmware.
	Example AT+NWOTADWSTOP OK	
AT+NWOTAFWNAME	(none)	Read a name in the header of the MCU firmware (Only for MCU firmware).
	Example AT+NWOTAFWNAME +NWOTAFWNAME:MCU OK	
AT+NWOTAFWSIZE	(none)	Read a size in the header of the MCU firmware (Only for MCU firmware).
	Example AT+NWOTAFWSIZE +NWOTAFWSIZE:4128 OK	
AT+NWOTAFWCRC	(none)	Read a CRC in the header of the MCU firmware (Only for MCU firmware).
	Example AT+NWOTAFWCRC +NWOTAFWCRC:0x580813b1OK	
AT+NWOTAREADFW	<read addr>, <read_size>	Read the MCU firmware as much as the read_size from the read_addr and transmit it (Only for MCU firmware). ■ <read_addr>: Hexadecimal without "0x" prefix ■ <read_size>: Decimal MCU_FW default address: ■ RA6W1: 0x700000 ■ RA6W2: 0x720000
	Example AT+NWOTAREADFW=700000,128 TESTFMCUÿÿÿÿ12345678901234561234567890123456123456789012345612345678901234561234567890123456123456789012345612345678901234561234567890123456 +NWOTAREADFW:COMPLETE OK	

Command	Parameters	Description
AT+NWOTATRANSFW	(none)	Transmit the downloaded MCU firmware to the MCU. Transmission failed if no header (16 bytes) information exists (Only for MCU firmware).
	Example AT+NWOTATRANSFW MCU TESTFMCUÿÿÿÿ12345678901234561234567890123456123456789012345612345678901234561234567890123456123456789012345612345678901234561234567890123456123456789012345612345678901234561234567890123456 …… +NWOTATRANSFW:COMPLETE OK	
AT+NWOTAERASEFW	(none)	Erase the MCU firmware stored in a serial flash of the RA6W1/RA6W2 (Only for MCU firmware).
	Example AT+NWOTAERASEFW +NWOTAERASEFW:COMPLETE OK	
AT+NWOTASETADDR	<sflash_addr>	Designate an address where data can be downloaded within the range of User Area and TLS Certificate Key in the SFlash area. MCU_FW/CERT_KEY default address: ■ RA6W1: 0x700000 ■ RA6W2: 0x720000 CERT_KEY should be copied to the operating area if downloaded to the user area, which is the default address. CERT_KEY area address: ■ RA6W1/RA6W2: 0x00350000
	Example AT+NWOTASETADDR=700000 +NWOTASETADDR:0x00 OK	
AT+NWOTAGETADDR	<fw_type>	Return the value set with NWOTASETADDR. MCU_FW/CERT_KEY default address: ■ RA6W1: 0x700000 ■ RA6W2: 0x720000
	Example AT+NWOTAGETADDR=mcu_fw +NWOTAGETADDR:0x700000 OK AT+NWOTAGETADDR=cert_key +NWOTAGETADDR:0x700000 OK	
AT+NWOTAREADFLASH	<sflash_addr>,<size>	Read as much as size from sflash_addr. MCU_FW default address: ■ RA6W1: 0x700000 ■ RA6W2: 0x720000
	Example AT+NWOTAREADFLASH=700000,128 MCU_FW TESTFMCUÿÿÿÿ12345678901234561234567890123456123456789012345612345678901234561234567890123456123456789012345612345678901234561234567890123456 OK	
AT+NWOTAERASEFLASH	<sflash_addr>,<size>	Delete as much as size from sflash_addr. MCU_FW default address: ■ RA6W1: 0x700000

Command	Parameters	Description
		■ RA6W2: 0x720000
	Example AT+NWOTAERASEFLASH=700000,1000 +NWOTAERASEFLASH:COMPLETE OK Note: It is erased in 4 kB increments.	
AT+NWOTACOPYFLASH	<dest_sflash_addr>,<src_sflash_addr>,<size>	Copy as much as size from src_sflash_addr to dest_sflash_addr. MCU_FW default address: ■ RA6W1: 0x700000 ■ RA6W2: 0x720000 Note: It is copied in 4 kB increments.
	Example AT+NWOTACOPYFLASH=720000,700000,1000 +NWOTACOPYFLASH:COMPLETE OK	
AT+NWOTATLSAUTH	<tls_auth_mode>	Set the certificate verification mode. ■ #define MBEDTLS_SSL_VERIFY_NONE 0 ■ #define MBEDTLS_SSL_VERIFY_OPTIONAL 1 ■ #define MBEDTLS_SSL_VERIFY_REQUIRED 2
	Example AT+NWOTATLSAUTH=0 OK AT+NWOTATLSAUTH=1 OK AT+NWOTATLSAUTH=2 OK	
AT+NWOTAALPN	<alpn_index>,<alpn>	Set the application layer protocol negotiation. Up to 3 can be set.
	Example AT+NWHTCALPN=1,http/1.1 OK AT+NWHTCALPN=2,http/1.1,h2 OK AT+NWHTCALPN=3,http/1.1,h2,h2c OK	
AT+NWOTAALPNDEL	(none)	Delete all set ALPNs.
	Example AT+NWHTCALPNDEL OK	
AT+NWOTASNI	<sni>	Set the server name indication.
	Example AT+NWHTCSNI=httpbin.org OK	
AT+NWOTASNIDEL	(none)	Delete the set SNI.
	Example AT+NWHTCSNIDEL OK	
AT+NWOTATLSVER	<tls_ver>	Set the TLS version. tls_ver: 0 (v1.2), 1 (v1.3), 2 (v1.2 and v1.3)

Command	Parameters	Description
	Example AT+NWOTATLSVER=0 OK AT+NWOTATLSVER=1 OK AT+NWOTATLSVER=2 OK	
AT+NWOTASETBIDX	<boot_index>	Set the boot index to boot after a reboot. Boot_index: 0 (0x0000_2000) 1(0x0040_0000) Note: ■ This command should be used very carefully. If there is no RTOS in the selected index or an incorrect RTOS exists, serious damage to the system might occur. ■ The boot index is automatically changed when you execute the AT+NWOTARENEW command. Therefore, do not use this command unless it is for special purposes.
	Example AT+NWOTASETBIDX=0 OK AT+NWOTASETBIDX=1 OK	
AT+NWOTAGETBIDX	(none)	Get the boot index that boots after reboot.
	Example AT+NWOTAGETBIDX +NWOTAGETBIDX:0 OK	
AT+NWOTABYMCU	rtos,<full_size>	Transmit the RTOS stored in the MCU to the RA6W1/RA6W2 when there is no network access. If the AT+NWOTABYMCU= rtos,<full_size> command is OK, RTOS is transmitted as much as the partial size with tx_size=<partial_size>,<binary data>. Every transmission sends "OK" as a response unless there is an error. If an error occurs or transmission is complete, it responds with +NWOTABYMCU:0x00 including status. Note that only RTOS can be downloaded.
	Example AT+NWOTABYMCU=rtos,1335408 OK tx_size=4096,4643394BDA4F27840000000000000000… OK … tx_size=112,00000000000000000000000001000000… +NWOTABYMCU:0x00	

NOTE
When DPM mode is enabled and OTA update is in progress (firmware download is in progress), it does not enter DPM Sleep because of SFlash write operation. After downloading the firmware, the RA6W1 resumes to enter DPM Sleep mode.

Table 21. OTA response list

Response	Parameters	Description
+NWOTADWSTART	<status>	Return the status of firmware download. <status>: 0x00 is successful. See Table 22 for other status value. Example: +NWOTADWSTART:0x00
+NWOTARENEW	<status>	Return the status for firmware RENEW. <status>: 0x00 is successful. See OTA Response Code List for others. Example: +NWOTARENEW:0x00
+NWOTADWPROG	<progress>	Return the percentage value (%) of the firmware download progress. <progress>: Print download progress in percentage. Example: +NWOTADWPROG:100
+NWOTADWSTOP	<status>	Return the status of firmware download stop. <status>: 0x00 is successful. See Table 22 for other status values. Example: +NWOTADWSTOP:0x00
+NWOTATRANSFW	COMPLETE or FAIL	Return result of MCU firmware transmission. (Only for MCU firmware). Example: +NWOTATRANSFW:COMPLETE
+NWOTAFWNAME	<name>	String entered by a user (The default is MCU_FW). Returns "(NULL)" if there is no MCU firmware. (Only for MCU firmware)
+NWOTAFWSIZE	<size>	Downloaded MCU firmware size. It returns 0 if there is no MCU firmware. (Only for MCU firmware)
+NWOTAFWCRC	<crc>	Downloaded MCU FW CRC. It returns 0 if there is no MCU firmware. (Only for MCU firmware)
+NWOTAREADFW	COMPLETE or FAIL	Success: COMPLETE Failure: FAIL (Only for MCU firmware)
+NWOTAERASEFW	COMPLETE or FAIL	Success: COMPLETE Failure: FAIL (Only for MCU firmware)
+NWOTASETADDR	<status>	<status>: 0x00 is successful. See Table 22 for other status values.
+NWOTAGETADDR	<sflash_addr>	Return the value of sflash_addr.
(AT+NWOTAREADFLASH)	(Binary)	Return binary data as much as entered SFlash address and size.
+NWOTAERASEFLASH	COMPLETE or FAIL	Success: COMPLETE Failure: FAIL
+NWOTACOPYFLASH	COMPLETE or FAIL	Success: COMPLETE Failure: FAIL
+NWOTABYMCU	<status>	<status>: 0x00 is successful. See Table 22 for other status values.

Table 22. OTA response code list

Return value	Description
0x00	Return success.
0x01	Return fail.
0x02	SFlash address is wrong.
0x03	Firmware type is unknown.
0x04	Server URL is unknown.
0x05	The firmware size is too big.
0x06	CRC is not correct.

Return value	Description
0x07	Firmware version is unknown.
0x08	The firmware version is incompatible.
0x09	Firmware not found on the server.
0x0A	Failed to connect to the server.
0x0B	Not all new firmware is downloaded.
0x0C	Failed to allocate memory.
0xA1	The Bluetooth firmware version is unknown.

2.6.5.1 OTA Download Example

RTOS download:

```
AT+NWOTADWSTART=rtos, https://server/RA6W1-xxxxxxxxxx-xxxxxxxxxx.img
```

Bluetooth firmware download: (RA6W2 only):

```
AT+NWOTADWSTART=ble_fw,https://server/ble_firmware.img
```

MCU firmware download:

```
AT+NWOTADWSTART=mcu_fw,https://server/mcu_firmware.img
AT+NWOTADWSTART=mcu_fw,https://server/mcu_firmware.img,ver01
```

Cert Key download:

```
AT+NWOTADWSTART=cert_key,https://server/ca.pem
```

2.6.5.2 OTA Download Progress Example

RTOS download progress:

```
AT+NWOTADWPROG=rtos
```

Bluetooth firmware download progress: (RA6W2 only):

```
AT+NWOTADWPROG=ble_fw
```

MCU firmware download progress:

```
AT+NWOTADWPROG=mcu_fw
```

Cert Key download progress:

```
AT+NWOTADWPROG=cert_key
```

2.6.5.3 OTA Renew Example

Renew Firmware (reboot with updated firmware):

```
AT+NWOTARENEW
```

2.6.5.4 MCU Firmware Transport Example

MCU firmware transmission:

```
AT+NWOTATRANSFW
```

Get MCU firmware name:

```
AT+NWOTAFWNAME
```

Get MCU firmware size:

```
AT+NWOTAFWSIZE
```

Get MCU firmware CRC:

```
AT+NWOTAFWCRC
```

Read MCU firmware as much as specified size:

```
AT+NWOTAREADFW=700000,128
```

Delete MCU firmware stored in the RA6W1/RA6W2 SFlash:

```
AT+NWOTAERASEFW
```

2.6.5.5 SFlash User Area Address Setting Example

Set ADDR:

```
AT+NWOTASETADDR=700000
```

Get ADDR:

```
AT+NWOTAGETADDR=mcu_fw
AT+NWOTAGETADDR=cert_key
```

2.6.5.6 SFlash READ/COPY/ERASE Example

SFLASH Read:

```
AT+NWOTAREADFLASH=700000,128
```

SFLASH Copy:

```
AT+NWOTACOPYFLASH=720000,0x700000,128
```

SFLASH Erase:

```
AT+NWOTAERASEFLASH=0x700000,128
```

2.6.5.7 TLS Certificate Verification Mode Setting Example

Set MBEDTLS_SSL_VERIFY_NONE:

```
AT+NWOTATLSAUTH=0
```

Set MBEDTLS_SSL_VERIFY_OPTIONAL:

```
AT+NWOTATLSAUTH=1
```

Set MBEDTLS_SSL_VERIFY_REQUIRED:

```
AT+NWOTATLSAUTH=2
```

2.6.5.8 RTOS by MCU Download Example

Initialization:

```
AT+NWOTABYMCU=rtos,1335408
```

Data transmission:

```
tx_size=4096,4643394BDA4F27840000000000000000…
```

2.6.6 Transfer Function Commands

2.6.6.1 Socket Commands

Table 23. Socket command list

Command	Parameters	Description
AT+TRTS	<ip_type>, <local_port>[,<max allowed connection>]	Open a TCP server socket. <ip_type>: IP version. 0 (IPv4), 1 (IPv6) <local_port>: Local port number of the socket. <max allowed connection>: It is optional. Set maximum allowed TCP session. Response: OK (with '+TRCTS:*** ') See Table 24 or ERROR. Async message: CID(+TRTS:<Assigned CID>) Prerequisite ■ The RA6W1 should be connected to AP. Note:

Command	Parameters	Description
		■ CID number 0 (TCP server), 1 (TCP client), 2 (UDP) are pre-assigned numbers. A maximum of four TCP sockets can be created starting with CID 3. ■ A total of four sessions can be created for the transfer function. But it depends onRA6W1 SDK configuration. Basically, the RA6W1 can have up to four TCP sockets.

	Example
	// Open first TCP server
	AT+TRTS=0,10194
	+TRTS:0
	OK
	
	// Open second TCP server
	AT+TRTS=0,10195
	+TRTS:3
	OK	

AT+TRTC	<server_ip>, <server_port> [,<local_port>]	Open a TCP client socket and connect to a TCP server. ■ <server_ip>: IP address of TCP server to be accessed ■ <server_port>: Port number of TCP server ■ <local_port>: Local port number of the socket (optional, 0: auto) Response: OK or ERROR Async message: CID(+TRTC:<Assigned CID>) Prerequisite ■ The RA6W1 should be connected to AP. Note: ■ CID number 0 (TCP server), 1 (TCP client), 2 (UDP) are pre-assigned numbers. A maximum of four TCP sockets can be created starting with CID 3. ■ A total of four sessions can be created for the transfer function. But it depends on RA6W1 SDK configuration. Basically, the RA6W1 can have up to four TCP sockets.
	Example AT+TRTC=192.168.0.18,1025,1024 +TRTC:1 OK AT+TRTC=192.168.0.18,1025,1025 +TRTC:3 OK	
AT+TRUSE	<ip_type>, <local_port>	Open a UDP socket. ■ <ip_type>: IP version. 0 (IPv4), 1 (IPv6) ■ <local_port>: Local port number of the socket Response: OK or ERROR Async message: CID(+TRUSE:<Assigned CID>) Note: ■ CID number 0 (TCP server), 1 (TCP client), 2 (UDP) are pre-assigned numbers. A maximum of four TCP sockets can be created starting with CID 3. ■ A total of four sessions can be created for the transfer function, but it depends on RA6W1 SDK configuration. Basically, the RA6W1 can have up to four UDP sockets.
	Example AT+TRTALL (optional, run this first if ERROR is responded) AT+TRUSE=0,10195 +TRUSE:2 OK	

Command	Parameters	Description
	AT+TRUSE=0,10196 +TRUSE:3 OK	
AT+TRUR	<remote_ip>, <remote_port> [,<local_port>]	Open a UDP socket with remote IP and port of the UDP socket. ■ <remote_ip>: Remote IP address ■ <remote_port>: Remote port number ■ <local_port> : Local port (Optional) Response: OK or ERROR Async message: CID(+TRUR:2) Note: It is only for the CID 2.
	Example AT+TRUR=192.168.0.18,1027 +TRUR:2 OK	
AT+TRPRT	<cid>	Get session information by CID. <cid>: Assigned CID Response: <cid>,[TCP|UDP],<remote_ip>,<remote_port>, <local_port> Prerequisite ■ A UDP socket should be opened (AT+TRUSE). Note: CID number 0 (TCP server), 1 (TCP client), and 2 (UDP) are pre-assigned numbers. A maximum of four TCP sockets can be created starting with CID 3.
	Example AT+TRPRT=2 +TRPRT:2,UDP,192.168.0.18,10194,10195 OK	
AT+TRPALL	(none)	Get all session information. Response: <cid>,[TCP|UDP],<remote_ip>,<remote_port>, <local_port><LF>… Prerequisite ■ The target system should be connected to any UDP or TCP server.
	Example AT+TRPALL +TRPALL:2,UDP,192.168.0.18,10194,10195 OK	
AT+TRTRM	<cid> [,<remote_ip> ,<remote_port>]	Close (terminate) a session by CID. If CID is 0 (TCP server), remote_ip, and remote_port are input, the session with the specific remote is closed. ■ <cid>: Assigned CID ■ <remote_ip>: Remote IP address connected to TCP server. It is only allowed in TCP server ■ <remote_port>: Remote port number connected to TCP server. It is only allowed in TCP server Response: OK or ERROR Prerequisite ■ The target system should be connected to any UDP or TCP server.
	Example AT+TRTRM=2 OK AT+TRTRM=0,192.168.0.18,10194 OK	
AT+TRTALL	(none)	Close (terminate) all sessions.

Command	Parameters	Description
		Response: OK or ERROR
	Example AT+TRTALL OK	
AT+TRSAVE	(none)	Save status of all sessions to NVRAM. Response: OK or ERROR
	Example AT+TRSAVE OK	
AT+TCPDATAMODE	<mode>	Set the mode of the received TCP data. <mode> ■ 0: text mode (default) ■ 1: hex string mode In text mode, data is returned as an ascii string: "0123ABCD" In hex mode, the data is returned as a hex encoded text string "3031323341424344". Response: OK or ERROR
	Example AT+TCPDATAMODE=1 OK	

Table 24. Socket connection response list

Response	Parameters	Description
+TRCTS	<cid>, <remote_ip>, <remote_port>	When sending the AT command (AT+TRTS=40000), receive this response if there is no error. ■ <cid>: Assigned CID for TCP server ■ <remote_ip>: TCP client IP address ■ <remote_port>: TCP client port number
	Example +TRCTS:0,192.168.0.18,41014	
+TRXTS	<cid>, <remote_ip>, <remote_port>	A remote TCP client is disconnected from the TCP server that was opened by AT+TRTS. ■ <cid>: Assigned CID for TCP server ■ <remote_ip>: TCP client IP address ■ <remote_port>: TCP client port number
	Example // When a remote peer is disconnected +TRXTS:0,192.168.0.18,41014	
+TRXTC	<cid>, <remote_ip>, <remote_port>	The TCP client socket that was opened by AT+TRTC is disconnected. ■ <cid>: Assigned CID for TCP client ■ <remote_ip>: TCP server IP address ■ <remote_port>: TCP server port number
	Example // When the TCP client socket is disconnected +TRXTC:1,192.168.0.18,1025	

2.6.6.2 Data Transfer Commands

Table 25. Data transmission command

Escape sequence	Parameters	Description
<ESC>M	<cid>,<length>, <remote_ip >, <remote_port >, [<mode>,]<data>	Transmit data through a socket with the CID specified. ■ <ESC>M: To enter data input mode, type in <ESC>(0x1B) and M key together ■ <cid>: Assigned CID ■ <length>: Data length. Data length can be 0 in only text mode. If this is 0, data is read

Escape sequence	Parameters	Description
		until "\r" or "\n" is met. In raw mode, data is read until the length. ■ <remote_ip>: Remote IP address ■ <remote_port>: Remote port number For TCP Server, <remote_ip> and <remote_port> of a TCP Client should be given. For TCP Client, 0, 0 is given (as the destination is the server). For UDP, if 0,0 is given, the data is sent to the destination that AT+TRUR has specified. if non-0 <remote_ip> and <remote_port> are given, UDP temporarily sends to the destination <remote_ip> and <remote_port> specified. ■ <mode>: Mode to transmit data in raw or text mode. It is optional. If there is no option, data should be transmitted in text mode. This option is allowed only for UART communication. ■ r: The raw mode is active. In raw mode, Data is read until data length. The data length is specified in <length> parameter ■ t: The text mode is active. In text mode, the data can be affected if it has unprintable control codes like backspace(0x08) Response: OK or ERROR Prerequisite ■ The target system should be connected to any UDP or TCP server/client. Note: Recommended to use <ESC>H command if UART baud rate is over 230400 bps. There might be data loss during the RA6W1 parses this AT command.
	Example1 – To send data to TCP client <ESC>M0,10,192.168.0.18,43110,abcde12345 OK Example2 – To send data to TCP server <ESC>M1,10,192.168.0.18,1025,abcde12345 OK Example3 – To send data to TCP server with '0, 0' as the destination/server <ESC>M1,10,0,0,abcde12345 OK Example4 – To send data to UDP receiver <ESC>M2,10,192.168.0.18,1024,abcde12345 OK	
<ESC>H	<cid>,<length>, <remote_ip >, <remote_port >	Transmit data through a socket with the CID specified. The host must send data after getting OK response. ■ <ESC>H: To enter data input mode, type in <ESC>(0x1B) and H key together. ■ <cid>: Assigned CID. ■ <length>: Data length. Data is read until the length after getting OK response. ■ <remote_ip>: Remote IP address. ■ <remote_port>: Remote port number. For TCP Server, <remote_ip> and <remote_port> of a TCP Client should be given. For TCP Client, 0, 0 is given (as the destination is the server). For UDP: if 0,0 is given, the data is sent to the destination that AT+TRUR has specified. if non-0 <remote_ip> and <remote_port> are given, UDP temporarily sends to the destination <remote_ip> and <remote_port> specified. Response: OK or ERROR Prerequisite ■ The target system should be connected to any UDP or TCP server/client.
	Example1 – To send data to TCP client <ESC>H0,10,192.168.0.18,43110 OK abcde12345 OK Example2 – To send data to TCP server <ESC>H1,10,192.168.0.18,1025 OK abcde12345	

Escape sequence	Parameters	Description
	OK Example3 – To send data to TCP server with '0, 0' as the destination/server <ESC>H1,10,0,0 OK abcde12345 OK Example4 – To send data to UDP receiver <ESC>H2,10,192.168.0.18,1024 OK abcde12345 OK	

Table 26. Data reception responses

Response	Parameters	Description
+TRDTS	<cid>, <src_ip>,<src_port>, <length>,<data>	Receive data through TCP server socket. ■ <cid>: Assigned CID ■ <src_ip>: Source IP address ■ <src_port>: Source port number ■ <length>: Data length ■ <data>: Received data
	Example // When data is sent from a TCP client +TRDTC:1,192.168.0.18,1025,4,test	
+TRDTC	<cid>, <src_ip>,<src_port>, <length>,<data>	Receive data through TCP client socket. ■ <cid>: Assigned CID ■ <src_ip>: Source IP address ■ <src_port>: Source port number ■ <length>: Data length ■ <data>: Received data
	Example // When TCP client receives data +TRDTC:1,192.168.0.18,1025,4,test	
+TRDUS	<cid>, <src_ip>,<src_port>, <length>,<data>	Receive data through UDP socket. ■ <cid>: Assigned CID ■ <src_ip>: Source IP address ■ <src_port>: Source port number ■ <length>: Data length ■ <data>: Received data
	Example // When UDP session receives data +TRDUS:2,192.168.0.18,10194,4,test	

2.6.6.3 Secure Socket Commands

Table 27. Secure socket command list

Command	Parameters	Description
AT+TRSSLINIT	<Role>	Initialize the SSL module. The RA6W1 allows you to create a module of TLS client. <Role>: The role of SSL, 1 – Client.
	Example AT+TRSSLINIT=1 +TRSSLINIT:0 OK	
AT+TRSSLCFG	<CID>,<Configuration	Configure SSL connection.

Command	Parameters	Description
	ID>,<Configuration value>	<CID>: The CID obtained after issuing the AT+TRSSLINIT command. <Configuration ID>: The configuration ID available in the following list: ■ 0: Invalid configuration parameter ■ 1: To ser SSL Protocol Version ■ 2: To set SSL CA Certificate ■ 3: To set SSL Certificate ■ 6: To set the SNI ■ 9: To enable/disable server validation ■ 10: To set the Incoming buffer length ■ 11: To set the Outgoing buffer length <Configuration value>: Value to the configuration provided in configuration ID CONF_ID:CONF_VAL ■ 0: Invalid ■ 1: SSL Protocol Version ● 0: TLS Version 1.2 (Default) ● 1: TLS Version 1.3 ● 2: Compatibility Mode (TLS 1.2/1.3) ■ 2: SSL CA Certificate Name ■ 3: SSL Certificate Name ● This parameter specifies the name of the SSL certificate used for client authentication. The SSL certificate and its corresponding private key are stored using the AT+TRSSLCERTSTORE command. ● Because RA6W1/RA6W2 requires the same name to be used for both the SSL certificate and the private key, a separate configuration parameter for the private key name is not required. ■ 6: To Set the SNI (supported only for TLS client) ■ 9: To enable/disable server validation ● 0: Disables server validation (Default) ● 1: Enables server validation ■ 10: To set the incoming buffer length ● These parameters define the buffer sizes used by the internal TLS stack. If the TLS packet size exceeds the configured incoming or outgoing buffer length, data encryption or decryption may fail. ● The valid range and maximum supported value are as follows: ○ Valid range: 1,024 to 17,408 bytes ○ Maximum supported value: 17,408 bytes. ■ 11: To set the outgoing buffer length ● Same buffer size constraints as Incoming buffer length - Valid range: 1,024 to 17,408 bytes; Maximum supported value: 17,408 bytes. Prerequisite ■ CID should be obtained (AT+TRSSLINT). ■ SSL CA certificate and SSL certificate should be set up.
	Example AT+TRSSLCFG=0,2,CA_CERT OK AT+TRSSLCFG=0,3,CERT OK AT+TRSSLCFG=0,6,RA6W1	

Command	Parameters	Description
	OK AT+TRSSLCFG=0,9,0 OK AT+TRSSLCFG=0,10,6144 OK AT+TRSSLCFG=0,11,6144 OK	
AT+TRSSLCO	<CID>,<Server IP Address>,<Server Port number>	Connect to an SSL server. ■ <CID>: The CID obtained after issuing the AT+TRSSLINIT command. ■ <Server IP Address>: The IP Address of the server to connect. Only supported IPv4 address. ■ <Server Port>: The port number of the SSL server to connect. Prerequisite ■ CID should be obtained (AT+TRSSLINT).
	Example AT+TRSSLCO=0,192.168.0.11,30000 OK	
AT+TRSSLWR	<CID>,[<Server IP Address>,<Server Port number>,<mode>,]<Data length>,<Data>	Send the data to the SSL server that is already established. ■ <CID>: The CID obtained after issuing the AT+TRSSLINIT command. ■ <Server IP Address>: The IP Address of the SSL server is already established. If there is no input, the IP address is internally used to the SSL server IP address. ■ <Server Port number>: The port number of the SSL server is already established. If there is no input, the Port number is internally used to the SSL server port number. ■ <mode>: Transmit data in raw or text mode. It is optional. If there is no option, data is transmitted in text mode. ● r: The raw mode is active. In raw mode, Data is read until data length. The data length is specified in <length> parameter. ● t: The text mode is active. In text mode, the data can be affected if it has unprintable control codes like backspace (0x08). ■ <Data length>: The length of data to send. ■ <Data>: The data to send. The input can be closed by <Ctrl>+C or reaching data length. Prerequisite ■ CID should be obtained (AT+TRSSLINT).
AT+TRSSLPRT	[<CID>]	Get TLS session information. ■ <CID>: The CID obtained after issuing AT+TRSSLINIT command. Response: <cid>,<role>,<status>,<remote ip>,<remote port>,<local port><LF>… Note ■ <cid>: The CID of the TLS session. ■ <role>: SSL role, 1 - Client. ■ <status>: Connected status, 1 - Connected, 2 - Not connected. ■ <remote ip>: Remote IP address if TLS session connected. ■ <remote port>: Remoted Port number if TLS session connected. ■ <local port>: Local Port number if TLS session

Command	Parameters	Description
		connected.
	Example AT+TRSSLPRT ERROR:0x5002FA (5243642) // Not found CID obtained. AT+TRSSLPRT +TRSSLPRT:0,1,0,0,0,0 // Not connected TLS session. AT+TRSSLPRT +TRSSLPRT:0,1,1,192.168.1.138,10000,50905 // Connected TLS session.	
AT+TRSSLCL	<CID>	Close the SSL connection. <CID>: The CID obtained after issuing AT+TRSSLINIT command. Prerequisite ■ CID should be obtained (AT+TRSSLINT).
	Example AT+TRSSLCL=0 OK	
AT+TRSSLCERTLIST	<Certificate Type>	Show a list of certificates or a list of CA data available in SFlash memory. <Certificate Type>: The value of the certificate. 0 – CA Certificates 1 – Client/Server Certificates
	Example AT+TRSSLCERTLIST=0 +TRSSLCERTLIST=0,CA_CERT	
AT+TRSSLCERTSTORE	<Certificate Type>, <Sequence>, <Format>, <Name>, [<Data length>,]<Data>	Store a certificate and CA list data in SFlash memory. ■ <Certificate Type>: The value of the certificate. 0 – CA. Certificates 1 – Client/Server Certificates ■ <Sequence>: Specifies the position of a certificate within a certificate chain that shares the same certificate name. This parameter ensures that multiple certificates belonging to the same logical group (chain) can be stored and referenced correctly ■ The valid range is 0–5, and it must start from 0. ■ If Certificate Type = 0 (CA Certificates): Up to 6 CA certificates (sequence values 0 through 5) can be stored as part of a single chain under the same name. ■ If the certificate type is 1 (Client/Server certificate), then several certificates in a sequence are 1-SSL cert or 2-SSL key. ■ <Format>: The value of the CA/Certificate/Key0 – DER, 1 – PEM. ■ <Name>: The name of the certificate. While loading certificate and key file separately, the same name should be used in both commands. ■ <Data length>: The length of certificate data. If the certificate is DER format, data length parameter is mandatory. ■ <Data>: The certificate data to be stored. Note: ■ If it's not entered within 3 seconds, an error code(0x500004) is returned.
	Example AT+TRSSLCERTSTORE=0,1,1,CA_CERT, -----BEGIN CERTIFICATE----- …	

Command	Parameters	Description
	-----END CERTIFICATE-----<Ctrl>+C OK	
AT+TRSSLCERTDELETE	<Certificate Type>,<Name>	Delete a certificate or CA list data in SFlash memory. ■ <Certificate Type>: The type of certificates. 0 – CA Certificates 1 – Client/Server Certificates ■ <Name>: The name of the certificate.
	Example AT+TRSSLCERTDELETE=0,CA_CERT OK	
AT+TRSSLSAVE	(none)	Store the current SSL module's configuration in NVRAM.
	Example AT+TRSSLSAVE OK	
AT+TRSSLDELETE	(none)	Delete the stored SSL module's configuration in NVRAM.
	Example AT+TRSSLDELETE OK	

Table 28. Secure socket response list

Response	Parameters	Description
+TRSSLDTC	<CID>, <remote_ip>, <local_port>, <length>, <data>	It sends the response when receiving data from SSL server. <CID>: The CID obtained after issuing the AT+TRSSLINIT command. <remote_ip>: SSL server IP address. <local_port>: Local port number of the secure socket. <length>: Data length. <data>: Received data.
	Example // When SSL client received data from secure server +TRSSLDTC:0,192.168.0.3,31200,5,Hello	
+TRSSLXTC	<CID>, <remote_ip>, <local_port>	It sends the response when secure socket connection is closed. <CID>: The CID obtained after issuing the AT+TRSSLINIT command. <remote_ip>: SSL server IP address. <local_port>: Local port number of the secure socket.
	Example // When secure socket connection is closed +TRSSLXTC:0,192.168.0.3,31200	

2.6.7 Power Manager Commands

Table 29. Power manager command list

Command	Parameters	Description
AT+PMGRWAKESRC	<action>,<wake_source>	Set/Clear the PMGR wake-up source to wake up the RA6W1. <action> ■ 1 (Set the wake-up source) ■ 2 (Clear the wake-up source) <wake_source> ■ 1 (RTC) ■ 2 (GPT) ■ 3 (GPIO) ■ 4 (ADC) ■ 5 (Wi-Fi) ■ 6 (Bluetooth) Response: OK or ERROR

Command	Parameters	Description
	?	Query the status of wake-up source. Response: +PMGRWAKESRC:<RTC>,<GPT>,<GPIO>,<ADC>,<Wi-Fi >,<Bluetooth>
	(none)	

	Example
	// Set Wi-Fi as a wake-up source
	AT+PMGRWAKESRC=1,5
	OK
	// Query the status of the wake-up source
	AT+PMGRWAKESRC
	+PMGRWAKESRC:0,0,0,0,1,0
	OK
	// Clear Wi-Fi from the wake-up source
	AT+PMGRWAKESRC=2,5
	OK
	// Query the status of the wake-up source
	AT+PMGRWAKESRC=?
	+PMGRWAKESRC:0,0,0,0,0,0
	OK	

AT+WFPSMODE	<0/1>	Enable or disable power save (sleep 4)

	Example
	//Get current PS setting
	AT+WFPSMODE=?
	+WFPSMODE:0OK
	//Enable sleep4
	AT+WFPSMODE=1
	OK	

AT+GPIOSET	`<Port Num>,<Pin Num>,<mode>,<val>`	Set the GPIO status to High or Low. ■ `<Port Num>`: GPIO port number ■ `<Pin Num>`: GPIO pin number within the selected port ■ `<mode>`: Pin mode configuration ■ `<val>`: Pin value(high or low)
	Example //Set port 0 pin 6 to high (P0_6) AT+GPIOSET=0,6,3,1 +GPIOSET:0 OK	
AT+GPIOGET	`<Port Num>,<Pin Num>`	Get the GPIO status, it should be hight(1) or low(0). ■ `<Port Num>`: GPIO port number ■ `<Pin Num>`: GPIO pin number within the selected port
	Example //Get port 0 pin 6 value (P0_6 low) AT+GPIOGET=0,6 +GPIOGET:0,6,0 OK	

AT+SETCONFIG	`<action>,<wake_source>,<port>,<pin>[,<edge_type>]`	Set/Clear the wake-up source to wake up the RA6W1 with specific pin and port.
		Sets the specified GPIO pin as a edge type (active high or active low) for the wakeup source (optional – edge_type).
		`<action>`
		■ 1 (Set the wake-up source)
		■ 2 (Clear the wake-up source)
		`<wake_source>`
		■ 1 (RTC)
		■ 2 (GPT)
		■ 3 (GPIO)
		■ 4 (ADC)
		■ 5 (Wi-Fi)
		■ 6 (Bluetooth)

Command	Parameters	Description
		<port> ■ 0 (P0) ■ 1 (P1) <pin> ■ 8 (P0_8) ■ 9 (P0_9) ■ 10 (PX_10) ■ 11 (PX_11) ■ 12 (PX_12) ■ 13 (PX_13) <edge_type> (optional only of action=1 and wake_source=3) ■ 0 ■ 1 Response: OK or ERROR
	Example //Clear pin 11 port 0(P0_11) AT+SETCONFIG=2,3,0,11 OK	
AT+GETCONFIG	(none)	Get the set pin status

	Example
	//Clear pin 11 port 0(P0_11)
	AT+SETCONFIG=2,3,0,11
	OK
	AT+GETCONFIG
	OK
	//Set pin 11 port 0 (P0_11)
	AT+SETCONFIG=1,3,0,11
	OK
	AT+GETCONFIG
	P0_11, P0_12, P0_13
	OK
	Note: AT+GETCONFIG output shows P0_11,ADC/P0_12/P0_13 ports if it is already set in the system. If ADC/P0_12/P0_13 is not already set in the system, then it shows only the port that is being set.	

AT+PMGRCONSTRAINT	<action>,<constraint>	Add or Remove constraint. <action> ■ 1 (Add) ■ 2 (Remove) <constraint> ■ 1 (RAM) ■ 2 (RETENTION) ■ 3 (MAC_HW) ■ 4 (PROHIBITED) Response: OK or ERROR
	(none)	Query the status of constraint counter. +PMGRCONSTRAINT:<RAM_counter>,<RET_counter>,<MAC_HW_counter>,<PROHIBITED_counter> Note: When "AT+PMGRCONSTRAINT=1,1" is run, the RAM-power-down sleep (Sleep mode 2, Sleep mode 3, and DPM sleep) is blocked, see the *RA6W1 PMGR DPM, Application Note*. While the RAM-power-down sleep is on hold, a job to do can start. After the job is done, run "AT+PMGRCONSTRAINT=2,1" to allow RAM-power-down sleep again.
	?	

	Example
	// Add RAM constraint
	AT+PMGRCONSTRAINT=1,1
	OK
	// Query the status of constraint counter	

Command	Parameters	Description

	AT+PMGRCONSTRAINT=?
	+PMGRCONSTRAINT:1,1,0,0
	OK
	// Add RAM constraint
	AT+PMGRCONSTRAINT=1,1
	OK
	// Query the status of constraint counter
	AT+PMGRCONSTRAINT=?
	+PMGRCONSTRAINT:2,1,0,0
	OK
	// Remove RAM constraint
	AT+PMGRCONSTRAINT=2,1
	OK
	// Query the status of constraint counter
	AT+PMGRCONSTRAINT=?
	+PMGRCONSTRAINT:1,1,0,0
	OK	

AT+PMGRFORCE	< sleep_mode >, < duration / twt action >, < neg_type / mantissa> , < min_wake_ dur>, < flow_type >, < trigger_en >, < neg_type >	Force to enter Sleep mode for the specified time. <sleep_mode> ■ 2 (Sleep mode 2) ■ 3 (Sleep mode 3) ■ 4 (DPM Sleep) ■ 5 (TWT) <duration> (when <sleep_mode> is 2, 3, or 4) Sleep duration in seconds. The range of <duration> is from 1 sec to ~24 days(2,073,600 sec). **TWT Parameters (when <sleep_mode> is 5)** AT+PMGRFORCE=5,<twt_action>,... <twt_action> = 0 > TWT Teardown Next argument: <neg_type> Negotiation type (0: Individual, 1: wake TBTT, 2: BCAST, 3: BCAST MGMT) <twt_action> = 1 > TWT Setup Next 6 arguments: <wake_int_mantissa> (TWT Wake Interval Mantissa) <wake_int_exp> (Wake interval Exponent) <min_twt_wake_dur> (Nominal Minimum TWT Wake Duration for example, 3) <flow_type> (for example, 0 = Announced, 1 = Unannounced) <trigger> (0 = disabled, 1 = enabled) <neg_type> (0: Individual, 1: wake TBTT, 2: BCAST, 3: BCAST MGMT)

	Example
	// Force to enter Sleep mode 2 for 10 seconds
	AT+PMGRFORCE=2,10
	OK
	// Force to enter Sleep mode 3 for 10 seconds
	AT+PMGRFORCE=3,10
	OK
	// Force to enter DPM Sleep for 10 seconds
	AT+PMGRFORCE=4,10
	OK
	// TWT setup with an 8192 TU interval, exponent 10, 3 TU minimum wake duration, flow type 0, trigger disabled, negotiation type 1
	AT+PMGRFORCE=5,1,8192,10,3,0,0,1
	OK
	// TWT teardown with negotiation type 1
	AT+PMGRFORCE=5,0,1
	Note:	

Command	Parameters	Description
	■ By default, PMGR manages (chooses and executes) Sleep modes based on constraint and wake-up source, but using this command forces the Sleep mode selected by the specified mode. ■ Regarding AT+PMGRFORCE=4,<sleep_time>, it works only when the following conditions are met: ● Active Wi-Fi connection in place. ● Wi-Fi is set as a PMGR wake-up source. ■ When AT+PMGRFORCE=4,<sleep_time> is run, regardless of RAM constraint counter value (currently non-zero), it forces to enter DPM sleep. After <sleep_time> is passed, the system wakes up. ● TWT Mode (5): Additional arguments are required (as described above). ● Teardown requires a negotiation type parameter. ● Setup requires 6 additional parameters specifying wake-up interval, flow type, and more.	
AT+PMGRDPMKA	<period>	Set DPM keepalive period. <period>: Keepalive period (millisecond, 0 ~ 600000) Response: OK or ERROR
	?	Get DPM keepalive period. Response: +PMGRDPMKA=<millisecond>
	(none)	
	Example AT+PMGRDPMKA +PMGRDPMKA:30000 OK AT+PMGRDPMKA=15000 OK AT+PMGRDPMKA=? +PMGRDPMKA:15000 OK Note: ▪ The configuration is stored in NVRAM. ▪ Restart the system to apply the changes.	
AT+PMGRIPCOND	<ip_condition>	Set IP Condition to enter PMGR_LLD_DPM. <ip_codition> ■ 1 (IPv4 Only) ■ 2 (IPv6 Only) ■ 3 (Both) Response: OK or ERROR
	?	Get IP Condition value. Response: +PMGRIPCOND:<ip_condition>
	(none)	
	Example AT+PMGRIPCOND +PMGRIPCOND:1 OK AT+PMGRIPCOND=2 OK AT+PMGRIPCOND =? +PMGRIPCOND:2 OK Note: ■ The configuration is stored in NVRAM. Restart the system to apply the changes.	
AT+PMGRDPMTIMWU	<count>	Set DPM TIM wake-up count. <count>: TIM wake-up count (1 ~ 6000) Response: OK or ERROR
	?	Get DPM TIM wake-up count. Response: +PMGRDPMTIMWU=<count>
	(none)	

Command	Parameters	Description
	Example AT+PMGRDPMTIMWU +PMGRDPMTIMWU:10 OK AT+PMGRDPMTIMWU=20 OK AT+PMGRDPMTIMWU=? +PMGRDPMTIMWU:20 OK Note: ■ The configuration is stored in NVRAM. ■ Restart the system to apply the changes.	
AT+PMGRDPMUSERWU	<time>	Set DPM user wake-up time. The system wakes up at the specified time interval in periodic manner. <time>: User wake-up period (millisecond, 0 ~ 86400000) Response: OK or ERROR Note: ■ The configuration is stored in NVRAM. ■ The timer set by this command is periodic. ■ To cancel the timer, run AT+PMGRDPMUSERWU=0. ■ Restart the system to apply the changes.
	?	Get DPM user wake-up time. Response: + DPMUSERWU =<millisecond>
	(none)	
	Example AT+PMGRDPMUSERWU +PMGRDPMUSERWU:0 OK AT+PMGRDPMUSERWU=10000 OK AT+PMGRDPMUSERWU=? +PMGRDPMUSERWU:10000 OK	
AT+PMGRMCUWUDONE	(none)	Notify the RA6W1 that the MCU (that is connected to RA6W1 wakes up completely. When this command is received, the RA6W1 starts sending messages to the MCU (that is, MCU should send this command immediately after executing "External wakeup"). Response: OK or ERROR Note: ■ When the RA6W1 receives the command, it starts to send messages to the MCU. Sending this command means the MCU is ready to receive a message. MCU should send this command immediately when it receives a notification like +INIT:WAKEUP,UC.
	Example AT+PMGRMCUWUDONE OK	
List of unsolicited messages	+PMGR:<sleep_mode_event>	This message is sent to host when RA6W is entering DPM sleep. <sleep_mode_event> : 1 (entering sleep mode)

2.7 Bluetooth® LE Commands

NOTE
Table 30 shows commands that are applicable only for RA6W2 codeless app.

Table 30. Bluetooth LE commands list

Command	Parameters	Description
ATI	[none]	Bluetooth LE Device information query. Return firmware version, hardware type, and unique organization identifier.
	Example ATI CodeLess DA14531 v_6.380.9.10 OK	
ATR	[none]	Trigger a platform reset.
	Example ATR OK	
AT+BDADDR	[none]	Query the Bluetooth device address.
	Example AT+BDADDR 48:23:35:F4:00:05,P OK Note: Bluetooth device addresses are commonly two types: Public address (P) and Non-Public address or Random address (R).	
AT+SLEEP	[<slp_mode>]	Use the designated mode to instruct the controller to enter sleep mode. If the command is issued without any parameters, the current applied value is returned. This command has an effect only for command mode. [<slp_mode>] - 0 = Disable Sleep [<slp_mode>] - 1 = Enable Extended Sleep [<slp_mode>] - 2 = Enable Deep Sleep [<slp_mode>] - 3 = Enable Hibernate
	Example AT+SLEEP=0 OK	
AT+DEVNAME	<device name>	Change the Bluetooth LE device name.
	[none]	Get the Bluetooth LE device name.
	Example AT+DEVNAME=RA6Wx OK AT+DEVNAME RA6Wx OK	
AT+ADVSTART	[none]	Start advertising. Return ERROR if already starts advertising
	Example AT+ADVSTART OK	
AT+ADVSTOP	[none]	Stop advertising. Return ERROR if not already advertising.
	Example AT+ADVSTOP OK	
AT+ADVDATA	[<advertise data>]	Set or query about the advertising data. Data must be provided as hex string. The content takes effect only after advertising is restarted. There are four types of

Command	Parameters	Description
		data, 0x09 specifies the complete local name of the device. Other data types are 0x01 – flags, 0x03 – UUID, and 0x16 – service data.
	Example AT+ADVSTOP OK AT+ADVDATA=04:09:43:41:54 [Length = 0x04, type = 0x09, data = 'CAT' (C=0x43, A=0x41, T=0x54), the length includes type and data] OK AT+ADVSTART OK	
AT+ADVRESP	[<advertise data>]	Set or query scan response data. Change to take effect after the restart of advertising.
	Example AT+ADVSTOP OK AT+ADVRESP=04:09:43:41:54 [Length = 0x04, type = 0x09, data = 'CAT' (C=0x43, A=0x41, T=0x54), the length includes type and data] OK AT+ADVSTART OK	
AT+CENTRAL	[none]	Set the device Bluetooth role to central role. Advertising must be stopped, and any connection must be terminated before the role change is accepted.
	Example AT+CENTRAL OK	
AT+PERIPHERAL	[none]	Set the device Bluetooth role to peripheral. Any connection must be terminated before the role change is accepted.
	Example AT+PERIPHERAL OK	
AT+GAPSTATUS	[none]	Report the Bluetooth role and connection status as X, Y where X is 0 for peripheral role and one for central role and Y is 0 for non-connected and 1 for connected.
	Example AT+GAPSTATUS 1,1 OK	
AT+GAPSCAN	[none]	Start a Bluetooth device scan. It is only accepted when a device is in central role and not connected. A scan continues for 8 seconds or until any character is received through UART.
	Example AT+GAPSCAN Scanning… ( ) FD:37:13:D0:6D:02,R, Type: ADV, RSSI:-81 ( ) FD:37:13:D0:6D:02,R, Type: RSP, RSSI:-80 ( ) 69:35:59:5C:88:DA,R, Type: ADV, RSSI:-87 ( ) 80:EA:CA:80:00:07,P, Type: ADV, RSSI:-52 ( ) 80:EA:CA:80:00:07,P, Type: RSP, RSSI:-52	

Command	Parameters	Description
	( ) 69:35:59:5C:88:DA,R, Type: RSP, RSSI:-81 ( ) F0:1B:2A:F3:C6:0E,R, Type: ADV, RSSI:-67 ( ) F1:5C:6F:77:62:AF,R, Type: ADV, RSSI:-64 ( ) F1:5C:6F:77:62:AF,R, Type: RSP, RSSI:-64 ( ) F0:1B:2A:F3:C6:0E,R, Type: RSP, RSSI:-67 Scan Completed…	
AT+GAPCONNECT	[<slave_address>,<P:public/R:random>]	Initiate a connection with a specific slave device. The local device must be in central role. The connection attempt continues until a connection has been established or until a character is received via the UART.
	Example AT+GAPCONNECT=FD:37:13:D0:6D:02,R Connecting… Connected OK	
AT+GAPDISCONNECT	[none]	Disconnect from a peer Bluetooth device. This command can be used in both central and peripheral role.
	Example AT+GAPDISCONNECT Disconnected OK	
AT+BINREQ	[none]	This command is used in conjunction to AT+BINACK to enter binary mode. It is a pass-through command to the peer host to request a switch to binary mode. This command takes no parameters and has no effect on the internal state of the device.
	Example AT+BINREQ OK	
AT+BINREQACK	[none]	This command should be used as a reply to AT+BINREQ to enter binary mode. When the Codeless parsers detect this command, switches the flow to binary mode operation through the DSPS path. This command has no parameters.
	Example AT+BINREQACK OK	
AT+BINREQEXIT	[none]	Upon issuing the escape sequence the host device switches the Codeless device into a local command mode. Then, using the AT+BINEXIT command, it may request the peer host to exit Binary mode. When issued by the host, this command is causing an escape sequence to the peer host. The peer host should reply with AT+BINEXITACK. This command takes no parameters
	Example AT+BINREQEXIT OK	
AT+BINREQEXITACK	[none]	When a host device is in binary mode upon reception of an escape sequence, it should exit binary mode and reply with an AT+BINEXITACK. This command is transferred pass-through to the peer host to indicate

Command	Parameters	Description
		the switch to full end to end command operation.
	Example AT+BINREQEXITACK OK	
AT+BINRESUME	[none]	When the host switches the Codeless device to command mode using the escape sequence, it may switch back to binary mode using this command.
	Example AT+BINRESUME OK	
AT+BINESC	[<esctime1>,<escchar>,<esctime2>]	This command is used to specify escape condition to exit binary sequence. If the command is issued without any parameters, the current applied values are returned. [<esctime1>] - A 16-bit unsigned value that defines the escape time in milliseconds that should apply without reception prior to the reception of escape characters. The default value is 1000 msec. [<escchar>] - A 32-bit integer that should specify 3 bytes of escape characters. The most significant byte is ignored. The default escape sequence is 0x002B2B2B that is equal to the escape sequence '+++'. [<esctime2>] - A 16-bit unsigned value that defines the escape time in milliseconds that should apply without reception after the reception of escape characters. The default value is 1000 msec.
	Example AT+BINESC=100,+++,100 OK	
AT+PIN	[none]	This command is only valid for the central device when pin entry is requested from the peripheral device. The pin generated is always a randomly generated number, the pin code is printed on the peripheral side during bonding and the AT+PIN should be used on the central side for entering the pin code appearing on the peripheral side.
	Example AT+PIN=123456 // printed on the peripheral side OK	
AT+CLRBNDE	<index>	Clear a bonding database entry or clear the whole bonding database. <index> - The index of the bonding database entry to clear. Valid inputs are 1, 2, 3, 4, and 5. A parameter of 0xFF erases the whole database.
	Example AT+CLRBNDE=0xFF OK	
AT+CHGBNDP	[<index>, <status>]	Change the persistence status of the bonding entry specified by index. <index> : Specifies the index of the entry whose persistence status changes. Valid inputs are 1, 2, 3, 4, and 5. In case the index is 0xFF, all entries are

Command	Parameters	Description
		changed simultaneously. <status>: 0 – make the entry non-persistent 1 – make the entry persistent.
	Example AT+CHGBNDP=1,0 OK	
AT+IEBNDE	[<index>,[<entry>]]	Import or export (print to serial port) a bonding database entry. The first argument is mandatory whereas the second argument is optional (denoted by [ ]) and is only used in the case of importing an entry to the database. ■ <index> – Specifies the index of the entry that is exported (printed to the serial port). The valid index option is 1. The index plays no role in importing an entry, but it must be provided. ■ [<entry>] – This is an optional argument. If it exists, it specifies the hexadecimal string that is imported in the database. The database index is the one found within the database string. Format of the exported entry Character Position Data 1 – 32 Long Term Key (LTK) 33 - 36 Encrypted Diversifier (EDIV) 37 - 52 Random number (RAND) 53 - 54 Key size 55 ; (comma delimiter) 56 -87 Peer Connection Signature Resolving Key (CSRK) 88 - 99 Peer Bluetooth Address 100 - 101 Address type 102 - 103 Authentication level 104 - 105 Bonding database slot 106 ; (comma delimiter) 107 - 138 Identity resolving key (IRK) 139 ; (comma delimiter) 140 -141 Persistence status 142 ; (comma delimiter) 143 - 150 Timestamp Additional notes: Please note that this command is a very powerful one, especially when importing data. The user must be very careful to ensure the validity of the data imported. Although certain validity checks are performed (string length, position of delimiters, hexadecimal characters) no check is done about the validity of the data itself. An invalid string may cause connection errors, bonding errors, erratic behavior of the software or even cause the software to enter an undefined state.
	Example AT+IEBNDE=1,1 OK	
AT+SEC	[<mode>]	The command sets the current security/pairing mode out of 4 different modes: ■ LE secure connections pairing ■ Legacy pairing with MITM protection ■ Unauthenticated No MIMT protection (Just works) ■ No security The device must not be connected for the security mode to be changed, or an error occurs. If no argument is specified, the command returns to the current configuration. ■ <mode> – The mode parameter can be one of the

Command	Parameters	Description
		following: ■ 0 = LE secure connections pairing: In this case, cryptography is used along with the Diffie - Hellman public key exchange mechanism. The passkey entry pairing method is used for MITM protection. The LTK is stored along with other parameters in the bonding database if the bonding database is available. The device prints the 6-digit pin (by default 000000) which can also be set in advance using the AT+PIN command. ■ 1 = Legacy pairing with MITM protection: The user must enter a passkey which is currently set to 6 zero characters (000000). It can be changed using the AT+PIN command. ■ 2 = Unauthenticated no MITM protection: In this case, the Just Works pairing method is used to pair the two devices. The communication is encrypted. ■ 3 = No security: In this method there is no support for authentication or encryption.
	Example AT+SEC=1 OK	
AT+ENPRMD	[none]	This command enables pairing mode. Any new device that can provide the correct PIN code can pair and are added to the bonding database.
	Example AT+ ENPRMD OK	
AT+DISPRMD	[none]	This command disables pairing mode. Any device that is not previously bonded is disconnected when trying to pair. Any device that is already in the bonding database can connect seamlessly. The pairing mode is disabled by default when the device starts.
	Example AT+DISPRMD OK	
AT+GETPRMD	[none]	Get the pairing mode status. This command prints the status of the pairing mode to the console. Either a “ENABLED” or “DISABLED” string is printed.
	Example AT+GETPRMD DISABLED OK	
AT+RSSI	[none]	Retrieve the received signal strength indication and print it in the console in dBm. This value is updated internally every two seconds. The device must be in a connected state otherwise the command returns an error.
	Example AT+RSSI -47 dBm	

Command	Parameters	Description
	OK	
AT+PRINT	<text_to_print>	Print a specified string to UART. As opposed to the pipe command, the PRINT command returns OK. The special pipe command (|) sends the following string to the connected peer and when the peer receives it, it prints it out to the local terminal. No reply is expected/generated by the pipe command. Note: The maximum length of string that can be printed is 1024 B.
	Example AT+PRINT=<text_to_print> OK	

2.8 RF Test Function Commands

Table 31. RF test command list

Command	Parameters	Description
AT+TMLMACINIT	(none)	Initialize and start the LMAC task.
	Example AT+TMLMACINIT OK	
AT+RFVER	(none)	Display RF driver version.
	Example AT+RFVER RF Driver version v2.0.24	
AT+RFTX	<freq>, <BW>, <numFrames>, <frameLen>, <txRate>, <txPower>	Start RF TX test on 5 GHz or 2.4 GHz. <freq>: Carrier frequency (2412 ~ 2484 MHz for 2.4 GHz or 5180 ~ 5825 MHz for 5 GHz) <BW>: [0]: Fixed. Carrier Bandwidth. 20 MHz fixed <numFrames>: Number of frames to transmit <frameLen>: Length of frame (bytes) <txRate>: Data rate <txPower>: TX power (0 ~ 15), 0.8 dB step For more details on the txRate and txPower see Appendix H Wi-Fi RF Parameters.
	Example AT+RFTX=2412,0,0,100,b1,0 OK AT+RFTX=5180,0,2,100,b1,1 OK	
AT+RFTXPKT	<freq>, <BW>, <txRate>, <txPower>, <timeOut>, <data-ASCII encoded>	RF TX Packet test. <freq>: Carrier frequency (2412 ~ 2484 MHz for 2.4 GHz or 5180 ~ 5825 MHz for 5 GHZ) <BW>: [0]: Fixed. Carrier Bandwidth. 20 MHz fixed <txRate>: Data rate <txPower>: TX power (0 ~ 15), 0.8 dB step <timeOut>: Timeout duration for transmission <data>: Payload in ASCII encoded format
	Example AT+RFTXPKT=2412,0,b1,01000,HELLO OK	

Command	Parameters	Description
AT+RFTXSTOP	(none)	Stop RF TX test.
	Example AT+RFTXSTOP OK	
AT+RFCWTEST	<freq>	Start CW test. <freq>: Carrier frequency (2412 ~ 2484 MHz for 2.4 GHz or 5180 ~ 5825 MHz for 5 GHz) CW is generated with +1 MHz offset to center frequency.
	Example AT+RFCWTEST=2412 OK AT+RFCWTEST=5180 OK	
AT+RFCWSTOP	(none)	Stop CW tests.
	Example AT+RFCWSTOP Continuos TX Stoped OK	
AT+RFCONTSTART	<txRate>, <txPower>, <freq>	Start RF continuous TX test. <txRate>: Data rate. See the AT+RFTX command <txPower>: TX power (0 ~ 15), 0.8 dB step <freq>: Carrier frequency (2412 ~ 2484 MHz for 2.4 GHz or 5180 ~ 5825 MHz for 5 GHz)
	Example AT+RFCONTSTART=2412,0,b1 Continuos TX Started OK AT+RFCONTSTART=5180,0,b1 Continuos TX Started OK	
AT+RFCONTSTOP	(none)	Stop RF continuous TX test.
	Example AT+RFCONTSTOP OK	
AT+RFCHANNEL	<channel>, <band>	Change RF channel frequency. <Ch>: Carrier frequency(2412 ~ 2484 MHz for 2.4 GHz or 5150 ~ 5825 MHz for 5 GHz)
	Example AT+RFCHANNEL=3,2 Set RF 2 GHz Band, Channel 3, Frequency 2422 MHz OK AT+RFCHANNEL=36,5 Set RF 5GHz Band, Channel 36, Frequency 5180 MHz OK	
AT+RFRXSTART	(none)	RF RX test start.
	Example AT+RFRXSTART OK	

Command	Parameters	Description
AT+RFRXSTATISTICSRESET	(none)	Reset PER count.
	Example AT+RFRXSTATISTICSRESET PER count reset OK (Pass)	
AT+RFRXSTATISTICS	(none)	Display PER state. Indicate the number of Valid packets, FCS Errors packets, PHY Errors packets, and Overflow Errors.
	Example AT+RFRXSTATISTICS Error rate=46 Pass 33569 / fcs_error 10004 / phy_error 18977 / overflow 0016 Error RSSI=-43 DSSS RSSI=-89 OK	
AT+RFRXSTOP	(none)	Stop RF RX test.
	Example AT+RFRXSTOP OK	

2.9 Matter Commands

NOTE
The commands listed in Table 32 and Table 33 are applicable only for Matter application.

Table 32. AT commands from MCU TO RA6W2

Command	Parameters	Description
AT+MSTATUS	(none)	Request the status of matter application.
	Example AT+MSTATUS AT+MSTATUS=20 OK Note • Responded status _Status_IDLE = -1: idle. status is not initialized (TBD) _Status_factoryreset_done = 0:RA6W2's factory reset is done _Status_boot_ready = 1: RA6W2 powered on (TBD) _Status_need_configuration = 5: need to configure for commissioning _Status_AP_mode_start = 10: RA6W2 is in Soft AP mode (TBD). _Status_commissioning_mode_start = 11: commissioning start _Status_commissioning_mode_done = 12: commissioning done _Status_network_OK = 15: network (Wi-Fi) connected _Status_network_Fail = 16: network (Wi-Fi) connection fail _Status_STA_start = 20: station (RA6W2) system started _Status_STA_done = 25: station working done. Will be entered DPM (TBD) _Status_MCUOTA = 30: entered MCU OTA mode	
AT+ MCONTROL	<module>, <command>	Trigger Bluetooth provisioning. <module>: targeted module for the command ■ Bluetooth <command> ■ start : Bluetooth advertise start ■ stop : Bluetooth advertise stop Response: OK or ERROR
	Example AT+MCONTROL=BLE,stop OK AT+MCONTROL=BLE,start OK	
AT+ MCONFIG	<parameter>,<value>	Set configurations for commissioning. <parameter>: configurable parameter ■ DISC: discriminator ■ VID: vendor ID ■ PID: product ID ■ HWVER: Hardware version ■ SPKPCNT: spake2p iteration count ■ SPKPSALT: spake2p salt ■ SPKPVF: spake2p verifier ■ PINCODE: pin code ■ DEVTYPE: matter device type <value>: data of string type ■ '?' for <value>: is responded current value of the parameter with "+MSTATUS=CFG" Response: OK or ERROR
	<parameter>,<size>,<value>	<parameter>: configurable parameter ■ CERT0: set certification declaration ■ CERT1: device attestation certification ■ CERT2: product attestation intermediate certification

Command	Parameters	Description
		■ CERT3: device attestation private key ■ CERT4: device attestation public key <size>: binary data size <value>: data of binary type Response: OK or ERROR
	Example AT+MCONFIG=DISC,3840 OK AT+MCONFIG=VID,FFF1 OK AT+MCONFIG=CERT0,0.a.H..ZIG00 ; AT+MCONFIG=DISC,? +MSTATUS=CFG,DISC,3840 OK	
AT+MATTR	<endpoint-id>, <cluster-id>, <attribute-id>, <attribute-data>, <data-type(w),data-length(r)>, <write/read>	<endpoint-id>: device endpoint id <cluster-id>: cluster id <attribute-id>: attribute id <attribute-data>: attribute data <data-type(w), data-length(r)>: data type for write, data length for read <write/read>: write or read to attribute

	Example
	//write lock to lockstate_attribute for lock cluster
	AT+MATTR=1,256,0,1,36,1
	//read 1 byte from lockstate_attribute for lock cluster
	AT+MATTR=1,256,0,0,1,0	

Table 33. AT commands from RA6W2 to MCU

Command	Parameters	Description
AT+MSTATUS	none	Request the status of matter application.
	Example AT+MSTATUS AT+MSTATUS=20 OK Note ■ Responded status: _Status_IDLE = -1: idle. status is not initialized _Status_factoryreset_done = 0: RA6W2's factory reset is done _Status_boot_ready = 1: RA6W2 powered on _Status_need_configuration = 5: need to configure for commissioning _Status_AP_mode_start = 10: RA6W2 is in Soft AP mode _Status_commissioning_mode_start = 11: commissioning start _Status_commissioning_mode_done = 12: commissioning done _Status_network_OK = 15: network (Wi-Fi) connected _Status_network_Fail = 16: network (Wi-Fi) connection fail _Status_STA_start = 20: station (RA6W2) system started _Status_STA_done = 25: station working done. Is entered DPM _Status_MCUOTA = 30: entered MCU OTA mode	
AT+MCONTROL	<module>, <command>	Trigger Bluetooth provisioning. <module>: targeted module for the command ■ Bluetooth <command> ■ start : Bluetooth advertisement start ■ stop : Bluetooth advertisement stop Response: OK or ERROR
	Example	

Command	Parameters	Description
	AT+MCONTROL=BLE,stop OK AT+MCONTROL=BLE,start OK	
AT+MCONFIG	<parameter>, <value>	Set configurations for commissioning. <parameter>: configurable parameter ■ DISC: discriminator ■ VID: vendor ID ■ PID: product ID ■ HWVER: Hardware version ■ SPKPCNT: spake2p iteration count ■ SPKPSALT: spake2p salt ■ SPKPVF: spake2p verifier ■ PINCODE: pin code ■ DEVTYPE: matter device type <value>: data of string type ■ '?' for <value>: is responded current value of the parameter with "+MSTATUS=CFG" Response: OK or ERROR
	<parameter>, <size>,<value>	<parameter>: configurable parameter ■ CERT0: set certification declaration ■ CERT1: device attestation certification ■ CERT2: product attestation intermediate certification ■ CERT3: device attestation private key ■ CERT4: device attestation public key <size>: binary data size <value>: data of binary type Response: OK or ERROR
	Example AT+MCONFIG=DISC,3840 OK AT+MCONFIG=VID,FFF1 OK AT+MCONFIG=CERT0,0.a.H..ZIG00 ; AT+MCONFIG=DISC,? +MSTATUS=CFG,DISC,3840 OK	
AT+MATTR	<endpoint-id>, <cluster-id>, <attribute-id>, <attribute-data>, <data-type(w),data-length(r)>, <write/read>	<endpoint-id>: device endpoint id <cluster-id>: cluster id <attribute-id>: attribute id <attribute-data>: attribute data <data-type(w), data-length(r)>: data type for write, data length for read <write/read>: write or read to attribute

	Example
	//write lock to lockstate_attribute for lock cluster
	AT+MATTR=1,256,0,1,36,1
	//read 1 byte from lockstate_attribute for lock cluster
	AT+MATTR=1,256,0,0,1,0	

2.10 LittleFS Commands

NOTE
The commands in Table 34 are applicable only for RA6W2 codeless app.

Table 34. LittleFS Command list

Command	Parameters	Description
AT+FSRD	<path>[,<offset>,<len>]	Reads data from a file stored in the filesystem. Supports both full file reading and partial reading with offset and length.
	Example AT+FSRD=/test.txt //Reads the full content of the file +FSRD:11, Hello World OK AT+FSRD=/test.txt,6,5 +FSRD:5,World OK	
AT+FSWR	<path>,<len>	Writes data to a file. The file is created if it does not exist. If it exists, contents are overwritten.
	Example AT+FSWR=/a.txt,5 //File created & content written 12345 OK AT+FSWR=/a.txt,3 //Overwrites files with new data xyz xyz OK	
AT+FSDEL	<path>	Deletes a file from the filesystem.
	Example AT+FSDEL=/a.txt OK	
AT+FSFMT	<none>	Formats (erases) the filesystem. All files will be lost.
	Example AT+FSFMT OK	
AT+FSLST	<none>	Lists all files present in the filesystem with their sizes.
	Example AT+FSLST +FSLST:/test.txt,11 +FSLST:/log.txt,5 OK	

3. AT Command Examples

3.1 Data Transfer Test

This section describes how to test the data transfer function commands with a terminal emulator. Some of the terminal applications to use for this purpose are:

- IO Ninja: http://ioninja.com/
  HEXA data and file transmitting function
- Socket Test: http://sockettest.sourceforge.net/
  Text data transmittable only
- Script Communicator: http://sourceforge.net/projects/scriptcommunicator
  Socket communication, UART RX/TX data color-distinguished output function and HEXA data transmission

The following sections describe test procedures for socket communication between the RA6W1 and a personal computer with IO Ninja. Run RA6W1 AT commands on a serial terminal application on the local computer. The terminal must be connected to the UART2 interface of the RA6W1.

3.1.1 TCP Server Socket Test

3.1.1.1 Data Flow from PC to RA6W1

1. At the RA6W1 AT command, to open a TCP server socket of which the port is 1234, execute the following command:

```
AT+TRTS=0,1234
```

2. On Personal computer:
   a. Select **TCP Connection Socket** (#1, Figure 3).
   b. Enter the IP address and the port number of the RA6W1 (#2, Figure 3).
   c. Click  to connect the socket (#3, Figure 3).
3. At the RA6W1 AT command, execute the following command:
   +TRCTS:0,192.168.0.5,3713 (A TCP client socket connected, and IP address is 192.168.0.5 and port is 3713.)
4. On Personal computer, send data (#4, Figure 3).
5. At the RA6W1 AT command, execute the following command:
   `+TRDTS:0,192.168.0.5,3713,10,RRQ_AT_TCP` (Received 10 bytes of data RRQ_AT_TCP)

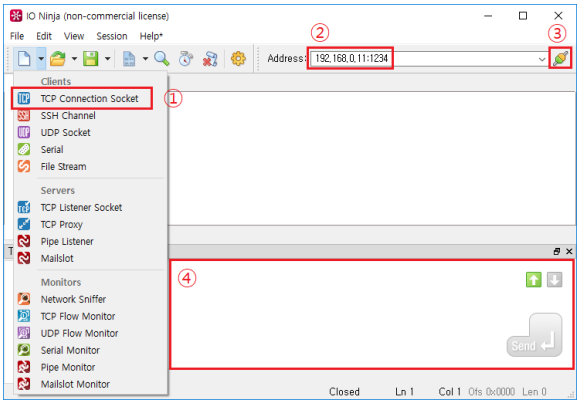


Figure 3. IO Ninja – TCP client socket setting

3.1.1.2 Data Flow from RA6W1 to PC

1. RA6W1 AT command:
   `AT+TRTS=0,1234` – Open a TCP server socket of which the port is 1234.
2. Personal computer:
   a. Select **TCP Connection Socket** (#1, Figure 3).
   b. Enter the IP address and the port number of the RA6W1 (#2, Figure 3).
   c. Click  to connect the socket (#3, Figure 3).
3. RA6W1 AT command:
   `<ESC>M0,5,192.168.0.100,51106,HELLO` (RA6W1 sent 5 bytes of data "HELLO" to the TCP client at IP 192.168.0.100 and port 51106)

3.1.2 TCP Client Socket Test

1. On Personal computer:
   a. Select **TCP Listener Socket** (#1, Figure 4).
   b. Enter the port number to be used (#2, Figure 4).
   c. Click  to start to listen (#3, Figure 4).
2. At the RA6W1 AT commands, execute the following commands to:
   a. Open a TCP client socket and set the server IP (192.168.0.5), port (1234), and the local port (2300): AT+TRTC=192.168.0.5,1234,2300.
   b. Send 8 bytes of data 12345678: <ESC>M1,8,0,0,12345678.
3. On Personal computer:
   a. Received data.
   b. Send data (#4, Figure 4).
4. At the RA6W1 AT command, execute the following command:
   +TRDTC:1,192.168.0.5,1234,10,RRQ_AT_TCP (Received 10 bytes of data RRQ_AT_TCP).

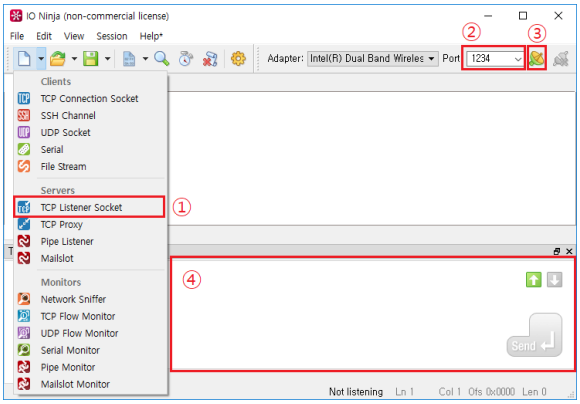


Figure 4. IO Ninja – TCP server socket setting

3.1.3 UDP Socket Test

1. On Personal computer:
   a. Select **UDP Socket** (#1, Figure 5).
   b. Enter the port number to be used and click  to open the socket (#2, Figure 5).
   c. Enter the IP address and port of the counterpart's UDP socket, click  and get ready for data transmission (#3, Figure 5).
   d. Enter data and click **Send** to transmit (#4, Figure 5).
2. At the RA6W1 AT commands:
   a. Open a UDP socket and set the local port (4567): AT+TRUSE=0,4567.
   b. Set the remote IP (192.168.0.5) and port (1234): AT+TRUR=192.168.0.5,1234.

c. Send 10 bytes of data 1234567890: <ESC>M2,10,0,0,1234567890.
d. Received 10 bytes of data RRQ_AT_UDP: +TRDTC:0,10,RRQ_AT_UDP.

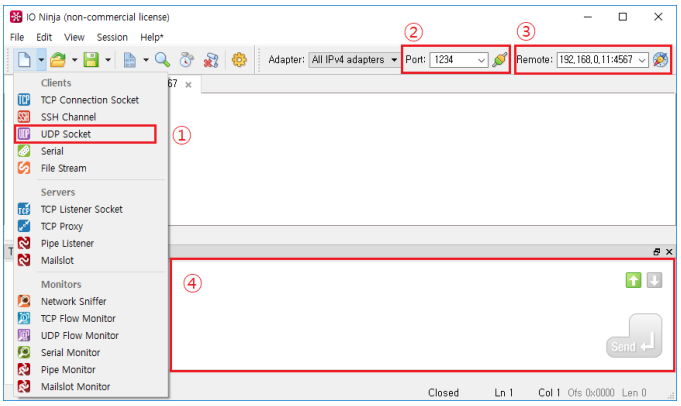


Figure 5. IO Ninja – UDP socket setting

Appendix A License Information

Mosquitto1.4.14 License
Eclipse Distribution License 1.0
Copyright (c) 2007, Eclipse Foundation, Inc. and its licensors.
All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the Eclipse Foundation, Inc.

Nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

UMAC GPL License
Linux kernel 3.9.0 rc3 version (backport 4.2.6-1)

Appendix B HTTP Client Result Codes

Table 35 shows client result codes as defined by HTTP.

Table 35. HTTP client result codes

Define	Value
HTTPC_RESULT_OK	0
HTTPC_RESULT_ERR_UNKNOWN	1
HTTPC_RESULT_ERR_CONNECT	2
HTTPC_RESULT_ERR_HOSTNAME	3
HTTPC_RESULT_ERR_CLOSED	4
HTTPC_RESULT_ERR_TIMEOUT	5
HTTPC_RESULT_ERR_SVR_RESP	6
HTTPC_RESULT_ERR_MEM	7
HTTPC_RESULT_LOCAL_ABORT	8
HTTPC_RESULT_ERR_CONTENT_LEN	9

Appendix C Fast-Reconnect on Sleep Mode 2

When Wi-Fi STA tries to connect to an AP after a power-on by power-switch or RTC timer wake-up on Sleep mode 2, it requires some time to make a Wi-Fi connection.
To reduce this Wi-Fi connection time between Wi-Fi AP and STA, the RA6W1 provides the Fast-connection function.
In AT command of the RA6W1, this function is enabled by default.

C.1 Technical Overview

C.1.1 Direct Probe Request for Wi-Fi Scan

During the Wi-Fi Setup processing after factory status, associated channel number is saved in NVRAM automatically after success Wi-Fi connect.
After saving the connected channel number to NVRAM, when reconnecting to Wi-Fi is attempted, the total Wi-Fi scan time to connect is reduced because only the registered channel number is scanned without performing full-channel scan for Wi-Fi connection.

C.1.2 Network Address without DHCP Client Procedure

The RA6W1 obtains an IP address by DHCP client procedure when the first Wi-Fi connection is completed after a factory-reset. The DHCP client operation can take a long time in some cases.
To reduce DHCP client procedure time, the RA6W1 saves the IP address, subnet mask, gateway address, and DNS address information in NVRAM after a successful DHCP client procedure, and changes to STATIC IP mode internally.
STATIC IP mode removes DHCP processing time and improves connection speed.

Appendix D RA6W1 Cipher Suites

Table 36. RA6W1 cipher suites

No.	Cipher suite supported by the RA6W1	Hex code
1	TLS_RSA_WITH_AES_128_CBC_SHA	2F
2	TLS_RSA_WITH_AES_256_CBC_SHA	35
3	TLS_RSA_WITH_AES_128_CBC_SHA256	3C
4	TLS_RSA_WITH_AES_256_CBC_SHA256	3D
5	TLS_RSA_WITH_AES_128_GCM_SHA256	9C
6	TLS_RSA_WITH_AES_256_GCM_SHA384	9D
7	TLS_RSA_WITH_AES_128_CCM	C09C
8	TLS_RSA_WITH_AES_256_CCM	C09D
9	TLS_RSA_WITH_AES_128_CCM_8	C0A0
10	TLS_RSA_WITH_AES_256_CCM_8	C0A1
11	TLS_RSA_WITH_DES_CBC_SHA	9
12	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	33
13	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	39
14	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	67
15	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	6B
16	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	9E
17	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	9F
18	TLS_DHE_RSA_WITH_AES_128_CCM	C09E
19	TLS_DHE_RSA_WITH_AES_256_CCM	C09F
20	TLS_DHE_RSA_WITH_AES_128_CCM_8	C0A2
21	TLS_DHE_RSA_WITH_AES_256_CCM_8	C0A3
22	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	16
23	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	C011
24	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	C014
25	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	C027
26	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	C028
27	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	C02F
28	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	C030
29	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	C012
30	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	C00E
31	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	C00F
32	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256	C029
33	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384	C02A
34	TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256	C031
35	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384	C032
36	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	C00D
37	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	C009
38	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	C00A
39	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	C023

No.	Cipher suite supported by the RA6W1	Hex code
40	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	C024
41	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	C02B
42	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	C02C
43	TLS_ECDHE_ECDSA_WITH_AES_128_CCM	C0AC
44	TLS_ECDHE_ECDSA_WITH_AES_256_CCM	C0AD
45	TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8	C0AE
46	TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8	C0AF
47	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	C008
48	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	C004
49	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	C005
50	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256	C025
51	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384	C026
52	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256	C02D
53	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384	C02E
54	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	C003

Appendix E Reason Code for Wi-Fi Connection Failure or Disconnection

SDK v6.0.0.0: sdk/interfaces/wifi/stack/supplicant/src/common/ieee802_11_defs.h.

```
/* Reason codes (IEEE Std 802.11-2016, 9.4.1.7, Table 9-45) */
#define WLAN_REASON_UNSPECIFIED                             1
#define WLAN_REASON_PREV_AUTH_NOT_VALID                     2
#define WLAN_REASON_DEAUTH_LEAVING                          3
#define WLAN_REASON_DISASSOC_DUE_TO_INACTIVITY                 4
#define WLAN_REASON_DISASSOC_AP_BUSY                        5
#define WLAN_REASON_CLASS2_FRAME_FROM_NONAUTH_STA                6
#define WLAN_REASON_CLASS3_FRAME_FROM_NONASSOC_STA                7
#define WLAN_REASON_DISASSOC_STA_HAS_LEFT                   8
#define WLAN_REASON_STA_REQ_ASSOC_WITHOUT_AUTH              9
/* IEEE 802.11h */
#define WLAN_REASON_PWR_CAPABILITY_NOT_VALID                   10
#define WLAN_REASON_SUPPORTED_CHANNEL_NOT_VALID                11
#define WLAN_REASON_BSS_TRANSITION_DISASSOC                    12
/* IEEE 802.11i */
#define WLAN_REASON_INVALID_IE                              13
#define WLAN_REASON_MICHAEL_MIC_FAILURE                     14
#define WLAN_REASON_4WAY_HANDSHAKE_TIMEOUT                     15
#define WLAN_REASON_GROUP_KEY_UPDATE_TIMEOUT                   16
#define WLAN_REASON_IE_IN_4WAY_DIFFERS                         17
#define WLAN_REASON_GROUP_CIPHER_NOT_VALID                     18
#define WLAN_REASON_PAIRWISE_CIPHER_NOT_VALID                     19
#define WLAN_REASON_AKMP_NOT_VALID                          20
#define WLAN_REASON_UNSUPPORTED_RSN_IE_VERSION                 21
#define WLAN_REASON_INVALID_RSN_IE_CAPAB                    22
#define WLAN_REASON_IEEE_802_1X_AUTH_FAILED                    23
#define WLAN_REASON_CIPHER_SUITE_REJECTED                   24
#define WLAN_REASON_TDLS_TEARDOWN_UNREACHABLE                  25
#define WLAN_REASON_TDLS_TEARDOWN_UNSPECIFIED                  26
#define WLAN_REASON_SSP_REQUESTED_DISASSOC                     27
#define WLAN_REASON_NO_SSP_ROAMING_AGREEMENT                   28
#define WLAN_REASON_BAD_CIPHER_OR_AKM                       29
#define WLAN_REASON_NOT_AUTHORIZED_THIS_LOCATION               30
#define WLAN_REASON_SERVICE_CHANGE_PRECLUDES_TS                31
#define WLAN_REASON_UNSPECIFIED_QOS_REASON                     32
#define WLAN_REASON_NOT_ENOUGH_BANDWIDTH                    33
/* IEEE 802.11e */
#define WLAN_REASON_DISASSOC_LOW_ACK                           34
#define WLAN_REASON_EXCEEDED_TXOP                          35
#define WLAN_REASON_STA_LEAVING                             36
#define WLAN_REASON_END_TS_BA_DLS                          37
#define WLAN_REASON_UNKNOWN_TS_BA                          38
#define WLAN_REASON_TIMEOUT                                39
#define WLAN_REASON_PEERKEY_MISMATCH                          45
#define WLAN_REASON_AUTHORIZED_ACCESS_LIMIT_REACHED                46
#define WLAN_REASON_EXTERNAL_SERVICE_REQUIREMENTS              47
#define WLAN_REASON_INVALID_FT_ACTION_FRAME_COUNT              48
#define WLAN_REASON_INVALID_PMKID                          49
#define WLAN_REASON_INVALID_MDE                             50
#define WLAN_REASON_INVALID_FTE                             51
#define WLAN_REASON_MESH_PEERING_CANCELLED                     52
#define WLAN_REASON_MESH_MAX_PEERS                          53
#define WLAN_REASON_MESH_CONFIG_POLICY_VIOLATION               54
#define WLAN_REASON_MESH_CLOSE_RCVD                         55
#define WLAN_REASON_MESH_MAX_RETRIES                        56
```

```
#define WLAN_REASON_MESH_CONFIRM_TIMEOUT                    57
#define WLAN_REASON_MESH_INVALID_GTK                        58
#define WLAN_REASON_MESH_INCONSISTENT_PARAMS                    59
#define WLAN_REASON_MESH_INVALID_SECURITY_CAP                    60
#define WLAN_REASON_MESH_PATH_ERROR_NO_PROXY_INFO                61
#define WLAN_REASON_MESH_PATH_ERROR_NO_FORWARDING_INFO            62
#define WLAN_REASON_MESH_PATH_ERROR_DEST_UNREACHABLE                63
#define WLAN_REASON_MAC_ADDRESS_ALREADY_EXISTS_IN_MBSS            64
#define WLAN_REASON_MESH_CHANNEL_SWITCH_REGULATORY_REQ            65
#define WLAN_REASON_MESH_CHANNEL_SWITCH_UNSPECIFIED                66
```

Appendix F Detailed Error Codes for AT Commands

Table 37. Common AT command error codes

Error No	Error Code	Description
0X500001	FSP_ERR_AT_CMD_ERR_UNKNOWN_CMD	Unknown command
0X500002	FSP_ERR_AT_CMD_ERR_INSUFFICENT_ARGS	Insufficient parameter
0X500003	FSP_ERR_AT_CMD_ERR_TOO_MANY_ARGS	Too many parameters
0X500004	FSP_ERR_AT_CMD_ERR_WRONG_ARGUMENTS	Wrong parameter value
0X500005	FSP_ERR_AT_CMD_ERR_NOT_SUPPORTED	Unsupported function
0X500006	FSP_ERR_AT_CMD_ERR_NOT_CONNECTED	Not connected to an AP
0X500007	FSP_ERR_AT_CMD_ERR_NO_RESULT	No result
0X500008	FSP_ERR_AT_CMD_ERR_TOO_LONG_RESULT	Response buffer overflow
0X500009	FSP_ERR_AT_CMD_ERR_INSUFFICENT_CONFIG	Function is not configured
0X50000A	FSP_ERR_AT_CMD_ERR_TIMEOUT	Command timeout
0X50000B	FSP_ERR_AT_CMD_ERR_NVR_WRITE	NVRAM write failure
0X50000C	FSP_ERR_AT_CMD_ERR_RTM_WRITE	Retention memory write failure
0X50000D	FSP_ERR_AT_CMD_ERR_SYS_BUSY	System busy
0X50000E	FSP_ERR_AT_CMD_ERR_MEM_ALLOC	Memory allocation failure
0X50000F	FSP_ERR_AT_CMD_ERR_CMD_OK	OK, No Error
0X500014	FSP_ERR_AT_CMD_ERR_DATA_TX	Data TX failure
0X500016	FSP_ERR_AT_CMD_ERR_IP_ADDRESS	IP address get failure
0X500017	FSP_ERR_AT_CMD_ERR_CMD_OK_WO_PRINT	OK, No response
0X500064	FSP_ERR_AT_CMD_ERR_COMMON_SYS_MODE	Wrong system running mode
0X50006E	FSP_ERR_AT_CMD_ERR_COMMON_ARG_TYPE	Wrong argument type
0X50006F	FSP_ERR_AT_CMD_ERR_COMMON_ARG_RANGE	Argument int-value range error
0X500070	FSP_ERR_AT_CMD_ERR_COMMON_ARG_LEN	Argument value length error
0X500071	FSP_ERR_AT_CMD_ERR_COMMON_WRONG_CC	Wrong country-code
0X500072	FSP_ERR_AT_CMD_ERR_COMMON_WRONG_MAC_ADDR	Wrong MAC address

Table 38. Flash AT command error codes

Error No	Error code	Description
0X5000AA	FSP_ERR_AT_CMD_ERR_SFLASH_READ	SFlash driver read failure
0X5000AB	FSP_ERR_AT_CMD_ERR_SFLASH_WRITE	SFlash drive write failure
0X5000AC	FSP_ERR_AT_CMD_ERR_SFLASH_ERASE	SFlash driver erase failure
0X5000AD	FSP_ERR_AT_CMD_ERR_SFLASH_ACCESS	SFlash driver access failure

Table 39. NVRAM AT command error codes

Error No	Error code	Description
0X5000B4	FSP_ERR_AT_CMD_ERR_NVRAM_READ	NVRAM driver read failure
0X5000B5	FSP_ERR_AT_CMD_ERR_NVRAM_WRITE	NVRAM driver write failure
0X5000B6	FSP_ERR_AT_CMD_ERR_NVRAM_ERASE	NVRAM driver erase failure
0X5000BC	FSP_ERR_AT_CMD_ERR_NVRAM_NOT_SAVED_VALUE	Not exist value in NVRAM

Table 40. Basic AT command error codes

Error No	Error code	Description
0X5000C8	FSP_ERR_AT_CMD_ERR_BASIC_ARG_NULL_PTR	Not used in AT command module
0X5000C9	FSP_ERR_AT_CMD_ERR_BASIC_ARG_DATE	Argument Date format failure
0X5000CA	FSP_ERR_AT_CMD_ERR_BASIC_ARG_TIME	Argument Time format failure
0X5000CB	FSP_ERR_AT_CMD_ERR_BASIC_ARG_TIME_ETC	Argument Time value failure

Table 41. UART AT command error codes

Error No	Error code	Description
0X5000DC	FSP_ERR_AT_CMD_ERR_UART_INTERFACE	Not defined UART type
0X5000DD	FSP_ERR_AT_CMD_ERR_UART_BAUDRATE	Argument BaudRate failure
0X5000DE	FSP_ERR_AT_CMD_ERR_UART_DATABITS	Argument DataBits failure
0X5000DF	FSP_ERR_AT_CMD_ERR_UART_PARITY	Argument Parity failure
0X5000E0	FSP_ERR_AT_CMD_ERR_UART_STOPBIT	Argument StopBits failure
0X5000E1	FSP_ERR_AT_CMD_ERR_UART_FLOWCTRL	Argument FlowCtrl failure
0X5000E2	FSP_ERR_AT_CMD_ERR_UART_BAUDRATE_NV_WR	NVRAM Write failure - Baudrate
0X5000E3	FSP_ERR_AT_CMD_ERR_UART_DATABITS_NV_WR	NVRAM Write failure - DataBits
0X5000E4	FSP_ERR_AT_CMD_ERR_UART_PARITY_NV_WR	NVRAM Write failure - Parity
0X5000E5	FSP_ERR_AT_CMD_ERR_UART_STOPBIT_NV_WR	NVRAM Write failure - StopBit
0X5000E6	FSP_ERR_AT_CMD_ERR_UART_FLOWCTRL_NV_WR	NVRAM Write failure - FlowCtrl

Table 42. PMGR AT command error codes

Error No	Error code	Description
0X50012C	FSP_ERR_AT_CMD_ERR_PMGR_UNSUPPORTED_SYS_MODE	Current sys mode is not supported
0X50012D	FSP_ERR_AT_CMD_ERR_PMGR_NO_WIFI_CONN	Wi-Fi is in disconnected state
0X50012E	FSP_ERR_AT_CMD_ERR_PMGR_CONSTR_RETENTION_NOT_SET	PMGR_CONSTRAINT_POWER_RETENTION is not set
0X50012F	FSP_ERR_AT_CMD_ERR_PMGR_DPM_MODE_ENABLED	DPM mode enabled
0X500130	FSP_ERR_AT_CMD_ERR_PMGR_DPM_MODE_DISABLED	DPM mode disabled
0X500131	FSP_ERR_AT_CMD_ERR_PMGR_DPM_ABN_ARG	Wrong argument type: DPM_ABN arg
0X500132	FSP_ERR_AT_CMD_ERR_PMGR_SLEEP_STARTED	DPM power-down started
0X500133	FSP_ERR_AT_CMD_ERR_PMGR_WAKE_SRC_WIFI_NOT_SET	PMGR_WAKE_SOURCE_WIFI is not set.

Table 43. Wi-Fi AT command error codes

Error No	Error code	Description
0X500190	FSP_ERR_AT_CMD_ERR_WIFI_NOT_CONNECTED	Not connected to AP
0X500191	FSP_ERR_AT_CMD_ERR_WIFI_RUN_MODE_TYPE	Wrong argument type
0X500192	FSP_ERR_AT_CMD_ERR_WIFI_RUN_MODE_RANGE	Wrong argument value range
0X500193	FSP_ERR_AT_CMD_ERR_WIFI_MAC_ADDR	Wrong string type for MAC address
0X500194	FSP_ERR_AT_CMD_ERR_WIFI_WPS_PIN_NUM	Wrong PIN number for WPS connection
0X500196	FSP_ERR_AT_CMD_ERR_WIFI_SCAN_UNSUPPORTED	Scan command not supported
0X500197	FSP_ERR_AT_CMD_ERR_WIFI_PSCAN_FREQ_RANGE	Wrong argument value range: Frequency
0X500198	FSP_ERR_AT_CMD_ERR_WIFI_PSCAN_CMAX_RANGE	Wrong argument value: Max RSSI threshold

Error No	Error code	Description
0X500199	FSP_ERR_AT_CMD_ERR_WIFI_PSCAN_CMIN_RANGE	Wrong argument value: Min RSSI threshold
0X50019A	FSP_ERR_AT_CMD_ERR_WIFI_JAP_SSID_NO_VALUE	SSID information not found in NVRAM
0X50019B	FSP_ERR_AT_CMD_ERR_WIFI_JAP_SSID_LEN	Too long SSID string
0X50019C	FSP_ERR_AT_CMD_ERR_WIFI_JAP_SECU_ARG_TYPE	Wrong argument type: Auth
0X50019D	FSP_ERR_AT_CMD_ERR_WIFI_JAP_SECU_ARG_RANGE	Wrong argument value range: Auth
0X50019E	FSP_ERR_AT_CMD_ERR_WIFI_JAP_OPEN_TOO_MANY_ ARG	Too many arguments for Open mode
0X50019F	FSP_ERR_AT_CMD_ERR_WIFI_JAP_OPEN_HIDDEN_ TYPE	Wrong argument type (OPEN): Hidden flag
0X500200	FSP_ERR_AT_CMD_ERR_WIFI_JAP_OPEN_HIDDEN_ RANGE	Wrong argument value (OPEN): Hidden flag
0X500201	FSP_ERR_AT_CMD_ERR_WIFI_JAP_SECU_HIDDEN_ TYPE	Wrong argument type (Security): Hidden flag
0X500202	FSP_ERR_AT_CMD_ERR_WIFI_JAP_SECU_HIDDEN_ RANGE	Wrong argument value (Security): Hidden flag
0X500203	FSP_ERR_AT_CMD_ERR_WIFI_JAP_WEP_IDX_TYPE	Wrong argument type: WEP Index
0X500204	FSP_ERR_AT_CMD_ERR_WIFI_JAP_WEP_IDX_RANGE	Wrong argument value range: WEP Index
0X500205	FSP_ERR_AT_CMD_ERR_WIFI_JAP_WEP_KEY_LEN	Wrong argument: WEP key length
0X500206	FSP_ERR_AT_CMD_ERR_WIFI_JAP_WPA_MODE_TYPE	Wrong argument type: Encrypt
0X500207	FSP_ERR_AT_CMD_ERR_WIFI_JAP_WPA_MODE_RANGE	Wrong argument value range: Encrypt
0X500208	FSP_ERR_AT_CMD_ERR_WIFI_JAP_WPA_KEY_LEN	Wrong argument: WPA PSK length
0X500209	FSP_ERR_AT_CMD_ERR_WIFI_JAPA_SSID_NO_VALUE	SSID information not found in NVRAM
0X50020A	FSP_ERR_AT_CMD_ERR_WIFI_JAPA_SSID_LEN	Too long SSID string
0X50020B	FSP_ERR_AT_CMD_ERR_WIFI_JAPA_PSK_LEN	Wrong argument: WPA PSK length
0X50020C	FSP_ERR_AT_CMD_ERR_WIFI_JAPA_WEP_NOT_ SUPPORT	Not supported security mode: WEP-mode
0X50020D	FSP_ERR_AT_CMD_ERR_WIFI_JAPA_HIDDEN_TYPE	Wrong argument type: Hidden flag
0X50020E	FSP_ERR_AT_CMD_ERR_WIFI_JAPA_HIDDEN_RANGE	Wrong argument value range: Hidden flag
0X50020F	FSP_ERR_AT_CMD_ERR_WIFI_JAPA_WPA3_MODE_ TYPE	Wrong argument type: WPA3 flag
0X500210	FSP_ERR_AT_CMD_ERR_WIFI_JAPA_WPA3_MODE_ RANGE	Wrong argument value range: WPA3 flag
0X500211	FSP_ERR_AT_CMD_ERR_WIFI_JAPA_WPA3_HIDDEN_ TYPE	Wrong argument type: Hidden flag
0X500212	FSP_ERR_AT_CMD_ERR_WIFI_JAPA_WPA3_HIDDEN_ RANGE	Wrong argument value range: Hidden flag
0X500213	FSP_ERR_AT_CMD_ERR_WIFI_ROAP_ROAM_TYPE	Wrong argument type
0X500214	FSP_ERR_AT_CMD_ERR_WIFI_ROAP_ROAM_RANGE	Wrong argument value range
0X500215	FSP_ERR_AT_CMD_ERR_WIFI_ENTAP_SSID_NO_VALUE	SSID information not found in NVRAM
0X500216	FSP_ERR_AT_CMD_ERR_WIFI_ENTAP_SSID_LEN	Too long SSID string
0X500217	FSP_ERR_AT_CMD_ERR_WIFI_ENTAP_AUTH0_ UNSUPPORT	Unsupported security mode
0X500218	FSP_ERR_AT_CMD_ERR_WIFI_ENTAP_ENC0_ UNSUPPORT	Unsupported encrypt mode
0X500219	FSP_ERR_AT_CMD_ERR_WIFI_ENTAP_EAP_PHASE1	Unsupported EAP Phase #1 value

Error No	Error code	Description
0X50021A	FSP_ERR_AT_CMD_ERR_WIFI_ENTAP_EAP_PHASE2	Wrong argument value range: EAP Phase #2
0X50021B	FSP_ERR_AT_CMD_ERR_WIFI_ENTAP_SECU_MODE	Wrong argument value range: Auth
0X50021C	FSP_ERR_AT_CMD_ERR_WIFI_ENTAP_ENC_MODE	Wrong argument value range: Encrypt
0X50021D	FSP_ERR_AT_CMD_ERR_WIFI_ENTAP_EAP_MODE	Wrong argument value range: EAP Phase #1
0X50021E	FSP_ERR_AT_CMD_ERR_WIFI_ENTAP_EAP_ID_NO_VALUE	Login ID information not found in NVRAM
0X50021F	FSP_ERR_AT_CMD_ERR_WIFI_ENTAP_EAP_ID_LEN	Too long ID string
0X500220	FSP_ERR_AT_CMD_ERR_WIFI_ENTAP_EAP_PWD_LEN	Too long PWD string
0X500221	FSP_ERR_AT_CMD_ERR_WIFI_SOFTAP_SSID_NO_VALUE	SSID for Soft AP not found in NVRAM
0X500222	FSP_ERR_AT_CMD_ERR_WIFI_SOFTAP_SECU_MODE	Wrong argument value: Security
0X500223	FSP_ERR_AT_CMD_ERR_WIFI_SOFTAP_ENC_MODE	Wrong argument value range: Encrypt
0X500224	FSP_ERR_AT_CMD_ERR_WIFI_SOFTAP_CH_VALUE_TYPE	Wrong argument type: Channel
0X500225	FSP_ERR_AT_CMD_ERR_WIFI_SOFTAP_CH_VALUE_RANGE	Wrong argument value range: Channel
0X500226	FSP_ERR_AT_CMD_ERR_WIFI_SOFTAP_OPEN_TOO_MANY_ARG	Too many arguments for Open mode
0X500227	FSP_ERR_AT_CMD_ERR_WIFI_SOFTAP_CH_TX_PWR_VALUE	Wrong channel TX-power value
0X500228	FSP_ERR_AT_CMD_ERR_WIFI_SOFTAP_WEP_NOT_SUPPORT	Unsupported security mode on Soft AP
0X500229	FSP_ERR_AT_CMD_ERR_WIFI_SOFTAP_ENC_MODE_TYPE	Wrong argument type: Encrypt
0X50022A	FSP_ERR_AT_CMD_ERR_WIFI_SOFTAP_ENC_MODE_RANGE	Wrong argument value range: Encrypt
0X50022B	FSP_ERR_AT_CMD_ERR_WIFI_SOFTAP_PASSKEY_LEN	Too short/long PSK length
0X5001CC	FSP_ERR_AT_CMD_ERR_WIFI_ALREADY_CONNECTED	Wi-Fi session already connected
0X5001CD	FSP_ERR_AT_CMD_ERR_WIFI_CONCURRENT_NO_PROFILE	Concurrent-mode profile information not found in NVRAM
0X5001CE	FSP_ERR_AT_CMD_ERR_WIFI_PSCAN_DURATION	Duration value out of range
0X5001CF	FSP_ERR_AT_CMD_ERR_WIFI_JAPA_WPA3_PSK_LEN	Too short/long PSK length
0X5001D0	FSP_ERR_AT_CMD_ERR_WIFI_SOFTAP_OWE_TOO_MANY_ARG	Too many arguments for OWE
0X5001D1	FSP_ERR_AT_CMD_ERR_WIFI_SOFTAP_SSID_LEN	Too long SSID string
0X5001D2	FSP_ERR_AT_CMD_ERR_WIFI_SCAN_BAND_TYPE	Wrong argument type: band
0X5001D3	FSP_ERR_AT_CMD_ERR_WIFI_SCAN_BAND_RANGE	Wrong argument value range: band
0X5001D4	FSP_ERR_AT_CMD_ERR_WIFI_ENTAP_WPA_HIDDEN_TYPE	Wrong argument type: Hidden flag
0X5001D5	FSP_ERR_AT_CMD_ERR_WIFI_ENTAP_WPA_HIDDEN_RANGE	Wrong argument value range: Hidden flag
0X5001E1	FSP_ERR_AT_CMD_ERR_WIFI_P2P_CONN_WPS_TYPE	Wrong argument type: wps
0X5001E2	FSP_ERR_AT_CMD_ERR_WIFI_P2P_UNSUPPORT_WPS_TYPE	Unsupported wps value
0X5001E3	FSP_ERR_AT_CMD_ERR_WIFI_P2P_CONN_JOIN_TYPE	Wrong argument type: join

Error No	Error code	Description
0X5001E4	FSP_ERR_AT_CMD_ERR_WIFI_P2P_CONN_JOIN_RANGE	Wrong argument value range: join
0X5001E5	FSP_ERR_AT_CMD_ERR_WIFI_P2P_LISTEN_CH_TYPE	Wrong argument type: ch
0X5001E6	FSP_ERR_AT_CMD_ERR_WIFI_P2P_LISTEN_CH_RANGE	Wrong argument value range: ch
0X5001E7	FSP_ERR_AT_CMD_ERR_WIFI_P2P_OPERATION_CH_ TYPE	Wrong argument type: ch
0X5001E8	FSP_ERR_AT_CMD_ERR_WIFI_P2P_OPERATION_CH_ RANGE	Wrong argument value range: ch
0X5001E9	FSP_ERR_AT_CMD_ERR_WIFI_P2P_GO_INTENT_TYPE	Wrong argument type: intent
0X5001EA	FSP_ERR_AT_CMD_ERR_WIFI_P2P_GO_INTENT_RANGE	Wrong argument value range: intent
0X5001EB	FSP_ERR_AT_CMD_ERR_WIFI_P2P_FIND_TIMEOUT_ TYPE	Wrong argument type: timeout
0X5001EC	FSP_ERR_AT_CMD_ERR_WIFI_P2P_FIND_TIMEOUT_ RANGE	Wrong argument value range: timeout

Table 44. CLI AT command error codes

Error No	Error code	Description
0X5001F4	FSP_ERR_AT_CMD_ERR_WIFI_CLI_STATUS	Failed to run cli status command
0X5001F5	FSP_ERR_AT_CMD_ERR_WIFI_CLI_SET_NETWORK	Failed to run cli set_network 0
0X5001F6	FSP_ERR_AT_CMD_ERR_WIFI_CLI_SET_NETWORK_ HIDDEN	Failed to run cli set_network 0 w/hidden flag
0X5001F7	FSP_ERR_AT_CMD_ERR_WIFI_CLI_SELECT_NETWORK	Failed to run cli select_network 0
0X5001F8	FSP_ERR_AT_CMD_ERR_WIFI_CLI_SAVE_CONF	Failed to run cli save_config
0X5001F9	FSP_ERR_AT_CMD_ERR_WIFI_CLI_SAVE_CONF_HIDDEN	Failed to run cli save_config w/hidden flag
0X5001FA	FSP_ERR_AT_CMD_ERR_WIFI_CLI_DISCONNECT	Failed to run cli disconnect
0X5001FB	FSP_ERR_AT_CMD_ERR_WIFI_CLI_DEAUTHENTICATE	Failed to run cli deauthenticate
0X5001FC	FSP_ERR_AT_CMD_ERR_WIFI_CLI_DISASSOCIATE	Failed to run cli disassociate
0X5001FE	FSP_ERR_AT_CMD_ERR_WIFI_CLI_WPS_PBC_ANY	Failed to run cli wps_pbc any
0X5001FF	FSP_ERR_AT_CMD_ERR_WIFI_CLI_WPS_PIN_GET	Failed to run cli wps_pin get
0X500200	FSP_ERR_AT_CMD_ERR_WIFI_CLI_WPS_PIN_ANY	Failed to run cli wps_pin any
0X500201	FSP_ERR_AT_CMD_ERR_WIFI_CLI_WPS_PIN_NUM	Wrong argument: PIN value
0X500202	FSP_ERR_AT_CMD_ERR_WIFI_CLI_WPS_CANCEL	Failed to run cli wps_cancel
0X500203	FSP_ERR_AT_CMD_ERR_WIFI_CLI_COUNTRY	Failed to run cli country
0X500204	FSP_ERR_AT_CMD_ERR_WIFI_CLI_PSCAN_CH_TL	Failed to run cli passive_scan chan_time_limit
0X500205	FSP_ERR_AT_CMD_ERR_WIFI_CLI_PSCAN_STOP	Failed to run cli passive_scan_stop
0X500206	FSP_ERR_AT_CMD_ERR_WIFI_CLI_PSCAN_CMAX_GET	Failed to run cli passive_scan_condition_max"
0X500207	FSP_ERR_AT_CMD_ERR_WIFI_CLI_PSCAN_CMAX_SET	Failed to run cli passive_scan_condition_max …
0X500208	FSP_ERR_AT_CMD_ERR_WIFI_CLI_PSCAN_CMIN_GET	Failed to run cli passive_scan_condition_min
0X500209	FSP_ERR_AT_CMD_ERR_WIFI_CLI_PSCAN_CMIN_SET	Failed to run cli passive_scan_condition_min …
0X50020A	FSP_ERR_AT_CMD_ERR_WIFI_CLI_SOFTAP_START	Failed to run cli ap start
0X50020B	FSP_ERR_AT_CMD_ERR_WIFI_CLI_SOFTAP_STOP	Failed to run cli ap stop
0X50020C	FSP_ERR_AT_CMD_ERR_WIFI_CLI_SOFTAP_RESTART	Failed to run cli ap restart
0X500212	FSP_ERR_AT_CMD_ERR_WIFI_CLI_P2P_FIND	Failed to run cli p2p_find
0X500213	FSP_ERR_AT_CMD_ERR_WIFI_CLI_P2P_FIND_STOP	Failed to run cli p2p_stop_find

Error No	Error code	Description
0X500214	FSP_ERR_AT_CMD_ERR_WIFI_CLI_P2P_JOIN	Failed to run cli p2p_connect join
0X500215	FSP_ERR_AT_CMD_ERR_WIFI_CLI_P2P_GRP_REMOVE	Failed to run cli p2p_group_remove
0X500216	FSP_ERR_AT_CMD_ERR_WIFI_CLI_P2P_PEER_INFO	Failed to run cli p2p_peers
0X500217	FSP_ERR_AT_CMD_ERR_WIFI_CLI_P2P_LISTEN_CH_TYPE	Wrong argument type: ch
0X500218	FSP_ERR_AT_CMD_ERR_WIFI_CLI_P2P_LISTEN_CH_RANGE	Wrong argument value range: ch

Table 45. Network basic AT command error codes

Error No	Error code	Description
0X500258	FSP_ERR_AT_CMD_ERR_NW_NET_IF_NOT_INITIALIZE	Network interface does not initialize
0X500259	FSP_ERR_AT_CMD_ERR_NW_NET_IF_IS_DOWN	Network interface is DOWN
0X50025A	FSP_ERR_AT_CMD_ERR_NW_IP_IFACE_TYPE	Wrong argument type: interface
0X50025B	FSP_ERR_AT_CMD_ERR_NW_IP_IFACE_RANGE	Wrong argument value range: interface
0X50025C	FSP_ERR_AT_CMD_ERR_NW_IP_ADDR_CLASS	Invalid IP address class
0X50025D	FSP_ERR_AT_CMD_ERR_NW_IP_INVALID_ADDR	Invalid IP address type
0X50025E	FSP_ERR_AT_CMD_ERR_NW_IP_NETMASK	Invalid Netmask address type
0X50025F	FSP_ERR_AT_CMD_ERR_NW_IP_GATEWAY	Invalid Gateway address type
0X500260	FSP_ERR_AT_CMD_ERR_NW_DNS_A_QUERY_FAIL	Failed to get IP address by DNS Query
0X500261	FSP_ERR_AT_CMD_ERR_NW_PING_IFACE_ARG_TYPE	Wrong argument type: Interface
0X500262	FSP_ERR_AT_CMD_ERR_NW_PING_IFACE_ARG_RANGE	Wrong argument value range: Interface
0X500263	FSP_ERR_AT_CMD_ERR_NW_PING_DST_ADDR	Invalid destination IP address
0X500264	FSP_ERR_AT_CMD_ERR_NW_PING_TX_COUNT	Wrong argument: Ping TX count

Table 46. DHCP Client AT command error codes

Error No	Error code	Description
0X500265	FSP_ERR_AT_CMD_ERR_NW_DHCPC_START_FAIL	Failed to start DHCP client
0X500266	FSP_ERR_AT_CMD_ERR_NW_DHCPC_HOSTNAME_LEN	Too long DHCP hostname
0X500267	FSP_ERR_AT_CMD_ERR_NW_DHCPC_HOSTNAME_TYPE	Wrong format for DHCP hostname

Table 47. DHCP Server AT command error codes

Error No	Error code	Description
0X500268	FSP_ERR_AT_CMD_ERR_NW_DHCPS_START_ADDR_NOT_EXIST	IP pool start-address not found in NVRAM
0X500269	FSP_ERR_AT_CMD_ERR_NW_DHCPS_END_ADDR_NOT_EXIST	IP pool end-address not found in NVRAM
0X50026A	FSP_ERR_AT_CMD_ERR_NW_DHCPS_WRONG_START_IP_CLASS	Invalid start IP address class
0X50026B	FSP_ERR_AT_CMD_ERR_NW_DHCPS_WRONG_END_IP_CLASS	Invalid end IP address class
0X50026C	FSP_ERR_AT_CMD_ERR_NW_DHCPS_IPADDR_RANGE_MISMATCH	Mismatch IP address class range
0X50026D	FSP_ERR_AT_CMD_ERR_NW_DHCPS_IPADDR_RANGE_OVERFLOW	Exceed IP address pool count
0X50026E	FSP_ERR_AT_CMD_ERR_NW_DHCPS_NO_CONNECTED_CLIENT	No connected client information to DHCP server
0X50026F	FSP_ERR_AT_CMD_ERR_NW_DHCPS_RUN_FLAG_TYPE	Wrong argument type: dhcpd flag

Error No	Error code	Description
0X500270	FSP_ERR_AT_CMD_ERR_NW_DHCPS_RUN_FLAG_VAL	Wrong argument value range: dhcpd flag
0X500271	FSP_ERR_AT_CMD_ERR_NW_DHCPS_LEASE_TIME_TYPE	Wrong argument type: dhcpd lease_time
0X500272	FSP_ERR_AT_CMD_ERR_NW_DHCPS_LEASE_TIME_RANGE	Wrong argument value range: dhcpd lease_time
0X500273	FSP_ERR_AT_CMD_ERR_NW_DHCPS_DNS_SVR_ADDR_NOT_EXIST	Not exist DNS IP address on DHCP server
0X500274	FSP_ERR_AT_CMD_ERR_NW_DHCPS_DNS_SVR_ADDR_CLASS	Invalid DNS IP address class on DHCP server

Table 48. SNTP Client AT command error codes

Error No	Error code	Description
0X500275	FSP_ERR_AT_CMD_ERR_NW_SNTP_NOT_SUPPORTED	SNTP client does not supported
0X500276	FSP_ERR_AT_CMD_ERR_NW_SNTP_FLAG_TYPE	Wrong argument type: SNTP flag
0X500277	FSP_ERR_AT_CMD_ERR_NW_SNTP_FLAG_VAL	Wrong argument value range: SNTP flag
0X500278	FSP_ERR_AT_CMD_ERR_NW_SNTP_PERIOD_TYPE	Wrong argument type: SNTP period
0X500279	FSP_ERR_AT_CMD_ERR_NW_SNTP_PERIOD_RANGE	Wrong argument value range: SNTP period

Table 49. MQTT Client AT command error codes

Error No	Error code	Description
0X50027A	FSP_ERR_AT_CMD_ERR_NW_MQTT_NOT_CONNECTED	MQTT client is currently not connected
0X50027B	FSP_ERR_AT_CMD_ERR_NW_MQTT_NEED_TO_STOP	Must disconnect the already connected MQTT session
0X50027C	FSP_ERR_AT_CMD_ERR_NW_MQTT_UNKNOWN_OP_ID	Input not supported
0X50027D	FSP_ERR_AT_CMD_ERR_NW_MQTT_CLIENT_TASK_START	MQTT client start failed by unknown reason

Table 50. MQTT Broker AT command error codes

Error No	Error code	Description
0X50027E	FSP_ERR_AT_CMD_ERR_NW_MQTT_BROKER_NAME_NOT_FOUND	MQTT broker name not found
0X50027F	FSP_ERR_AT_CMD_ERR_NW_MQTT_BROKER_PORT_NUM_TYPE	Wrong argument type: MQTT broker port
0X500280	FSP_ERR_AT_CMD_ERR_NW_MQTT_BROKER_PORT_NUM_RANGE	Wrong argument value range: MQTT broker port
0X500281	FSP_ERR_AT_CMD_ERR_NW_MQTT_BROKER_NAME_LEN	Too long MQTT Broker name length

Table 51. MQTT TLS AT command error codes

Error No	Error code	Description
0X500282	FSP_ERR_AT_CMD_ERR_NW_MQTT_TLS_TYPE	Wrong argument value type: tls
0X500283	FSP_ERR_AT_CMD_ERR_NW_MQTT_TLS_RANGE	Wrong argument value range: tls
0X500284	FSP_ERR_AT_CMD_ERR_NW_MQTT_TLS_ALPN_NOT_EXIST	ALPN information not found in NVRAM
0X500285	FSP_ERR_AT_CMD_ERR_NW_MQTT_TLS_ALPN_COUNT_TYPE	Wrong argument type: count
0X500286	FSP_ERR_AT_CMD_ERR_NW_MQTT_TLS_ALPN_COUNT_RANGE	Wrong argument value range: count
0X500287	FSP_ERR_AT_CMD_ERR_NW_MQTT_TLS_ALPN_NAME_LEN	Too long ALPN name length
0X500288	FSP_ERR_AT_CMD_ERR_NW_MQTT_TLS_SNI_NOT_EXIST	SNI information not found in NVRAM
0X500289	FSP_ERR_AT_CMD_ERR_NW_MQTT_TLS_SNI_LEN	Too long SNI string length

Error No	Error code	Description
0X50028A	FSP_ERR_AT_CMD_ERR_NW_MQTT_TLS_CSUITE_NUM_NOT_EXIST	CipherSuite count value not found in NVRAM
0X50028B	FSP_ERR_AT_CMD_ERR_NW_MQTT_TLS_CSUITE_NOT_EXIST	CipherSuite information not found in NVRAM
0X50028C	FSP_ERR_AT_CMD_ERR_NW_MQTT_TLS_CSUITE_NUM_NVRAM_WR	Failed to write Cipher Suit count info to NVRAM
0X50028D	FSP_ERR_AT_CMD_ERR_NW_MQTT_TLS_CSUITE_NVRAM_WR	Failed to write Cipher Suit info to NVRAM

Table 52. MQTT Sub-Topic AT command error codes

Error No	Error code	Description
0X50028E	FSP_ERR_AT_CMD_ERR_NW_MQTT_SUBS_TOPIC_NOT_EXIST	Sub-topic does not exist in NVRAM
0X50028F	FSP_ERR_AT_CMD_ERR_NW_MQTT_SUBS_TOPIC_NUM_TYPE	Wrong argument type: count
0X500290	FSP_ERR_AT_CMD_ERR_NW_MQTT_SUBS_TOPIC_NUM_RANGE	Wrong argument value range: count
0X500291	FSP_ERR_AT_CMD_ERR_NW_MQTT_SUBS_TOPIC_LEN	Too long topic string length
0X500292	FSP_ERR_AT_CMD_ERR_NW_MQTT_SUBS_TOPIC_DUP	Duplicate Sub-topic string
0X500293	FSP_ERR_AT_CMD_ERR_NW_MQTT_SUBS_TOPIC_NUM_NVRAM_WR	Failed to write topic count to NVRAM
0X500294	FSP_ERR_AT_CMD_ERR_NW_MQTT_SUBS_TOPIC_NUM_OVERFLOW	Adding a topic exceeds the max topic count
0X500295	FSP_ERR_AT_CMD_ERR_NW_MQTT_SUBS_TOPIC_ALREADY_EXIST	Subscribe topic already exists

Table 53. MQTT Pub-Topic AT command error codes

Error No	Error code	Description
0X500296	FSP_ERR_AT_CMD_ERR_NW_MQTT_PUB_TOPIC_NOT_EXIST	PUB topic not found in NVRAM
0X500297	FSP_ERR_AT_CMD_ERR_NW_MQTT_PUB_TOPIC_LEN	Too long topic string length

Table 54. MQTT WILL Message AT command error codes

Error No	Error code	Description
0X500298	FSP_ERR_AT_CMD_ERR_NW_MQTT_WILL_TOPIC_NOT_EXIST	WILL topic does not exist in NVRAM
0X500299	FSP_ERR_AT_CMD_ERR_NW_MQTT_WILL_MESSAGE_NOT_EXIST	WILL message not exist in NVRAM
0X50029A	FSP_ERR_AT_CMD_ERR_NW_MQTT_WILL_TOPIC_LEN	Too long WILL topic length
0X50029B	FSP_ERR_AT_CMD_ERR_NW_MQTT_WILL_MESSAGE_LEN	Too long WILL message length
0X50029C	FSP_ERR_AT_CMD_ERR_NW_MQTT_WILL_QOS_TYPE	Wrong argument type: QoS
0X50029D	FSP_ERR_AT_CMD_ERR_NW_MQTT_WILL_QOS_RANGE	Wrong argument value range: QoS

Table 55. MQTT Common AT command error codes

Error No	Error code	Description
0X50029E	FSP_ERR_AT_CMD_ERR_NW_MQTT_PROTOCOL	Network protocol error occurred with Broker
0X50029F	FSP_ERR_AT_CMD_ERR_NW_MQTT_PING_PERIOD_TYPE	Invalid Ping Period value is invalid
0X5002A0	FSP_ERR_AT_CMD_ERR_NW_MQTT_PING_PERIOD_RANGE	Wrong argument value range
0X5002A1	FSP_ERR_AT_CMD_ERR_NW_MQTT_USERNAME_NOT_EXIST	Username does not exist in NVRAM
0X5002A2	FSP_ERR_AT_CMD_ERR_NW_MQTT_USERNAME_LEN	Too long username length
0X5002A3	FSP_ERR_AT_CMD_ERR_NW_MQTT_PASSWORD_LEN	Too long password length
0X5002A4	FSP_ERR_AT_CMD_ERR_NW_MQTT_PUB_MESSAGE_LEN	Too long message length
0X5002A5	FSP_ERR_AT_CMD_ERR_NW_MQTT_PUB_TX_IN_PROGRESS	Previous message TX is still in progress

Table 56. HTTP(s) Server AT command error codes

Error No	Error code	Description
0X5002A8	FSP_ERR_AT_CMD_ERR_NW_HTS_TASK_CREATE_FAIL	Failed to create HTTP server task
0X5002A9	FSP_ERR_AT_CMD_ERR_NW_HTSS_TASK_CREATE_FAIL	Failed to create HTTPs server task

Table 57. HTTP(s) Client AT command error codes

Error No	Error code	Description
0X5002AA	FSP_ERR_AT_CMD_ERR_NW_HTC_TASK_CREATE_FAIL	Failed to create HTTP client task
0X5002AB	FSP_ERR_AT_CMD_ERR_NW_HTC_ALPN_CNT_TYPE	Wrong argument type: alpn_number
0X5002AC	FSP_ERR_AT_CMD_ERR_NW_HTC_ALPN_CNT_RANGE	Wrong argument value range: alpn_number
0X5002AD	FSP_ERR_AT_CMD_ERR_NW_HTC_ALPN1_STR_LEN	Too long ALPN #1 string length
0X5002AE	FSP_ERR_AT_CMD_ERR_NW_HTC_ALPN2_STR_LEN	Too long ALPN #2 string length
0X5002AF	FSP_ERR_AT_CMD_ERR_NW_HTC_ALPN3_STR_LEN	Too long ALPN #3 string length
0X5002B0	FSP_ERR_AT_CMD_ERR_NW_HTC_SNI_LEN	Too long SNI string length

Table 58. Web-Socket Client AT command error codes

Error No	Error code	Description
0X5002B1	FSP_ERR_AT_CMD_ERR_NW_WSC_URL_STR_LEN	Too short URL string length
0X5002B2	FSP_ERR_AT_CMD_ERR_NW_WSC_INVALID_URL	Invalid URL string
0X5002B3	FSP_ERR_AT_CMD_ERR_NW_WSC_TASK_ALREADY_EXIST	WebSocket session already exists
0X5002B4	FSP_ERR_AT_CMD_ERR_NW_WSC_CB_FUNC_DOES_NO_ EXIST	Not registered user Websocket cb-function
0X5002B5	FSP_ERR_AT_CMD_ERR_NW_WSC_INVALID_STATE	No connected session to disconnect
0X5002B6	FSP_ERR_AT_CMD_ERR_NW_WSC_TASK_CREATE_FAIL	Failed to create WebSocket client task
0X5002B7	FSP_ERR_AT_CMD_ERR_NW_WSC_CLOSE_FAIL	Failed to send "Session-Close" frame
0X5002B8	FSP_ERR_AT_CMD_ERR_NW_WSC_SESS_NOT_CONNECTED	No connected session to send message
0X5002B9	FSP_ERR_AT_CMD_ERR_NW_WSC_UNKNOW_CMD	Unknown WebSocket internal error

Table 59. Certificate AT command error codes

Error No	Error code	Description
0X5002D7	FSP_ERR_AT_CMD_ERR_NW_MODULE_NOT_ RESERVED	The specified module is not reserved (enabled) in serial flash space

Table 60. Transport Function (TCP/UDP) AT command error codes

Error No	Error code	Description
0X5002DA	FSP_ERR_AT_CMD_ERR_TCP_SERVER_LOCAL_PORT_TYPE	Wrong argument: local port of TCP server
0X5002DB	FSP_ERR_AT_CMD_ERR_TCP_SERVER_MAX_PEER_TYPE	Wrong argument: max allowed peer
0X5002DC	FSP_ERR_AT_CMD_ERR_TCP_SERVER_TASK_CREATE	Failed to start TCP server
0X5002DE	FSP_ERR_AT_CMD_ERR_TCP_CLIENT_SVR_PORT_TYPE	Wrong argument: TCP server port of TCP client
0X5002DF	FSP_ERR_AT_CMD_ERR_TCP_CLIENT_LOCAL_PORT_TYPE	Wrong argument: local port of TCP client
0X5002E1	FSP_ERR_AT_CMD_ERR_TCP_CLIENT_TASK_CREATE	Failed to start TCP client
0X5002E2	FSP_ERR_AT_CMD_ERR_UDP_SESS_LOCAL_PORT_TYPE	Wrong argument: local port of UDP session
0X5002E3	FSP_ERR_AT_CMD_ERR_UDP_SESS_LOCAL_PORT_RANGE	Invalid range of local port of UDP session
0X5002E4	FSP_ERR_AT_CMD_ERR_UDP_SESS_TASK_CREATE	Failed to create UDP session
0X5002E5	FSP_ERR_AT_CMD_ERR_UDP_CID2_SESS_NOT_EXIST	UDP session, CID 2, does not exist

Error No	Error code	Description
0X5002E6	FSP_ERR_AT_CMD_ERR_UDP_CID2_SESS_ALREADY_EXIST	UDP session, CID 2, already exists
0X5002E7	FSP_ERR_AT_CMD_ERR_UDP_CID2_SESS_INFO	Invalid UDP session, CID 2, information
0X5002E8	FSP_ERR_AT_CMD_ERR_UDP_CID2_REMOTE_PORT_TYPE	Invalid remote port of UDP session, CID 2
0X5002E9	FSP_ERR_AT_CMD_ERR_NO_CONNECTED_SESSION_EXIST	No session information
0X5002EA	FSP_ERR_AT_CMD_ERR_NO_FOUND_REQ_CID_SESSION	No assigned CID to terminate session
0X5002EB	FSP_ERR_AT_CMD_ERR_CONTEXT_CID_TYPE	Wrong argument type: cid
0X5002EC	FSP_ERR_AT_CMD_ERR_CONTEXT_DELETE	Failed to terminate session
0X5002ED	FSP_ERR_AT_CMD_ERR_CONTEXT_TYPE_IS_NOT_TCP_SVR	Wrong CID value: Not TCP server session
0X5002EE	FSP_ERR_AT_CMD_ERR_CONTEXT_INVALID_SESS_TYPE	Invalid session type to save session information
0X5002EF	FSP_ERR_AT_CMD_ERR_TRTRM_CID_TYPE	Wrong argument: CID to terminate session
0X5002F0	FSP_ERR_AT_CMD_ERR_TRTRM_REMOTE_PORT_NUM_TYPE	Wrong argument type: remote_port
0X5002F1	FSP_ERR_AT_CMD_ERR_TRTRM_TCP_SVR_REMOTE_SESS_ DISCON	Failed to disconnect TCP client from TCP server
0X5002F2	FSP_ERR_AT_CMD_ERR_TCP_SERVER_TERMINATE	Failed to terminate TCP server
0X5002F3	FSP_ERR_AT_CMD_ERR_TCP_CLIENT_TERMINATE	Failed to terminate TCP client
0X5002F4	FSP_ERR_AT_CMD_ERR_UDP_SESSION_TERMINATE	Failed to terminate UDP session
0X5002F5	FSP_ERR_AT_CMD_ERR_MULTI_SESSION_CID_TERMINATE	No assigned CID to terminate session
0X5002F6	FSP_ERR_AT_CMD_ERR_NO_SESSION_TO_SAVE_NVRAM	No session information to save
0X5002F7	FSP_ERR_AT_CMD_ERR_UDP_SESS_CONNECT	Failed to start UDP session

Table 61. SSL/TLS AT command error codes

Error No	Error code	Description
0X5002F8	FSP_ERR_AT_CMD_ERR_SSL_ROLE_NOT_SUPPORT	Not supported role of TLS session
0X5002F9	FSP_ERR_AT_CMD_ERR_SSL_CONF_CID_TYPE	Wrong argument: CID of TLS session
0X5002FA	FSP_ERR_AT_CMD_ERR_SSL_CONTEXT_NOT_FOUND	No assigned CID of TLS session
0X5002FB	FSP_ERR_AT_CMD_ERR_SSL_CONTEXT_ALREADY_EXIST	TLS session is already running to configure
0X5002FC	FSP_ERR_AT_CMD_ERR_SSL_CONF_ID_NOT_SUPPORTED	Not supported configuration
0X5002FD	FSP_ERR_AT_CMD_ERR_SSL_SAVE_CLR_ALL_NV	Failed to erase TLS session from NVRAM
0X5002FE	FSP_ERR_AT_CMD_ERR_SSL_SAVE_FAIL_NV	Failed to save TLS session to NVRAM
0X5002FF	FSP_ERR_AT_CMD_ERR_SSL_CONF_ID_TYPE	Wrong argument: configuration ID
0X500300	FSP_ERR_AT_CMD_ERR_SSL_CONF_ID_RANGE	Invalid range of configuration ID
0X500301	FSP_ERR_AT_CMD_ERR_SSL_CONF_CID_CA_CERT	CA certification does not exist for assigned CID
0X500302	FSP_ERR_AT_CMD_ERR_SSL_CONF_CID_CERT	Certification does not exist for assigned CID
0X500303	FSP_ERR_AT_CMD_ERR_SSL_CONF_CID_SNI	Failed to configure SNI of assigned CID
0X500304	FSP_ERR_AT_CMD_ERR_SSL_CONF_CID_SVR_VALID_TYPE	Wrong argument: auth mode of assigned CID
0X500305	FSP_ERR_AT_CMD_ERR_SSL_CONF_CID_SVR_VALID_ RANGE	Invalid range of auth mode of assigned CID
0X500306	FSP_ERR_AT_CMD_ERR_SSL_CONF_CID_RX_BUF_LEN	Wrong argument: RX buffer length of CID
0X500307	FSP_ERR_AT_CMD_ERR_SSL_CONF_CID_TX_BUF_LEN	Wrong argument: TX buffer length of CID
0X500308	FSP_ERR_AT_CMD_ERR_SSL_CONN_CID_TYPE	Wrong argument: CID to configure TLS session
0X500309	FSP_ERR_AT_CMD_ERR_SSL_CONN_ALREADY_	Already TLS session is connected

Error No	Error code	Description
	CONNECTED	
0X50030A	FSP_ERR_AT_CMD_ERR_SSL_CONN_PORT_NUM_TYPE	Wrong argument: peer_port of TLS client
0X50030B	FSP_ERR_AT_CMD_ERR_SSL_CONN_UNKNOWN_ HOSTNAME	Unknown hostname to connect TLS server
0X50030C	FSP_ERR_AT_CMD_ERR_SSL_CONN_CFG_SETUP_FAIL	Failed to setup TLS client
0X50030D	FSP_ERR_AT_CMD_ERR_SSL_CONN_TLS_CLINET_RUN_ FAIL	Failed to connect TLS client

Table 62. SSL Certificate AT command error codes

Error No	Error code	Description
0X50030E	FSP_ERR_AT_CMD_ERR_SSL_CERT_TYPE	Wrong argument: type
0X50030F	FSP_ERR_AT_CMD_ERR_SSL_CERT_RANGE	Invalid range of certificate type
0X500310	FSP_ERR_AT_CMD_ERR_SSL_CERT_STO_SEQ_TYPE	Wrong argument: sequence type
0X500311	FSP_ERR_AT_CMD_ERR_SSL_CERT_STO_SEQ_RANGE	Invalid range of sequence type
0X500312	FSP_ERR_AT_CMD_ERR_SSL_CERT_STO_FORMAT_TYPE	Wrong argument: format type
0X500313	FSP_ERR_AT_CMD_ERR_SSL_CERT_STO_FORMAT_RANGE	Invalid range of format type
0X500314	FSP_ERR_AT_CMD_ERR_SSL_CERT_STO_ALREADY_EXIST	Certificate already exists
0X500315	FSP_ERR_AT_CMD_ERR_SSL_CERT_STO_NO_SPACE	Not enough space to save certificate
0X500316	FSP_ERR_AT_CMD_ERR_SSL_CERT_DEL_LIST_NOT_FOUND	Not found certificate to delete
0X500317	FSP_ERR_AT_CMD_ERR_SSL_CERT_MODULE	Invalid module
0X500318	FSP_ERR_AT_CMD_ERR_SSL_CERT_FORMAT	Invalid format
0X500319	FSP_ERR_AT_CMD_ERR_SSL_CERT_LENGTH	Invalid length
0X50031A	FSP_ERR_AT_CMD_ERR_SSL_CERT_FLASH_ADDR	Invalid address of SFlash memory
0X50031B	FSP_ERR_AT_CMD_ERR_SSL_CERT_EMPTY_CERT	No certificate
0X50031C	FSP_ERR_AT_CMD_ERR_SSL_CERT_INTERNAL	Internal error
0X50031D	FSP_ERR_AT_CMD_ERR_SSL_SESS_TASK_CREATE	Failed to create SSL task
0X5003E7	FSP_ERR_AT_CMD_ERR_UNKNOWN	Undefined Error

Appendix G RA6W1 vs DA16200 AT Command Response

Table 63. The differences in AT Command Response between RA6W1 and DA16200

AT Command	Difference in response	Comments
AT	No change	-
AT+	No change	-
ATZ	No change	-
ATF	No change	-
ATE	No change	-
ATQ	No change	-
AT+RESTART	No change	-
AT+CHIPNAME	Yes	The response is changed to: AT+CHIPNAME+CHIPNAME:RA6W1-RRQ61001
AT+VER	No change	-
AT+SDKVER	No change	-
AT+TIME	No change	-
AT+RLT	No change	-
AT+DEFAP	No change	-
AT+DEFCCRNT	Yes	For RA6W1, to enable concurrent mode the value should be 4 instead of 2.
AT+WFMODE	No change	-
AT+WFMAC	No change	-
AT+WFSPF	No change	-
AT+WFSTAT	Yes	Format is different. RA6W1 uses FSP format
AT+WFSTA	No change	-
AT+WFPBC	No change	-
AT+WFPIN	No change	-
AT+WFCWPS	No change	-
AT+WFCC	No change	-
AT+WFSCAN	Yes	For DA16200, the AT scan command returns access point lines separated by \n, while the overall AT response uses \r\n as the delimiter. For example: `\r\nap0\nap1\nap2\n\r\nOK\r\n`. For RA6W1, the AT scan command returns access point lines separated by \r\n, and the entire AT response also uses \r\n as the delimiter. For example: `\r\nap0\r\nap1\r\nap2\r\n\r\nOK\r\n`.
AT+WFRSSI	No change	-
AT+WFJAP	No change	-
AT+WFJAPA	No change	-
AT+WFJAPA3	No change	-
AT+WFCAP	No change	Even though the AT command response is same, but error code for both RA6W1 and DA16200 are different
AT+WFQAP	Yes	DEAUTH message response not present in DA16200.
AT+WFDIS	No change	-
AT+WFENTAP	No change	-
AT+WFENTLI	No change	-
AT+WFSAP	No change	-

AT Command	Difference in response	Comments
AT+WFOAP	No change	-
AT+WFTAP	No change	-
AT+WFRAP	No change	-
AT+WFLCST	No change	-
AT+WFAPWM	No change	-
AT+WFAPCH	No change	-
AT+WFAPBI	No change	-
AT+WFAPUI	No change	-
AT+WFAPRT	No change	-
AT+WFAPDE	No change	-
AT+WFAPDI	No change	-
AT+WFWMM	No change	-
AT+WFWMP	No change	-
AT+WFSMSAVE	No change The command is added to RA6W1	-
AT+WFMODESWTCH	No change The command is added to RA6W1	-
AT+HOSRA6W1ITDONE	No change	-
AT+NWIP	No change	-
AT+NWDNS	No change	-
AT+NWDNS2	No change	-
AT+NWHOST	No change	-
AT+NWPING	No change	-
AT+NWDHC	No change	-
AT+NWDHCHN	No change	Even though the AT command response is same, but error code for both RA6W1 and DA16200 are different
AT+NWDHCHNDEL	No change	-
AT+NWDHR	No change	-
AT+NWDHLT	No change	
AT+NWDHS	No change	
AT+NWDHIP	No change	Even though the AT command response is same, but error code for both RA6W1 and DA16200 are different
AT+NWSNS	No change	-
AT+NWSNS1	No change	-
AT+NWSNS2	No change	-
AT+NWSNUP	No change	-
AT+NWSNTP	No change	-

AT Command	Difference in response	Comments
AT+NWSNTP1	No change	-
AT+NWSNTP2	No change	-
AT+NWCCRT	Yes	The way certificates are handled was changed for RA6W1
AT+NWDCRT	Yes	The way certificates are handled was changed for RA6W1
AT+NWMQBR	No change	-
AT+NWMQQOS	No change	-
AT+NWMQTLS	No change	-
AT+NWMQALPN	No change	Even though the AT command response is same, but error code for both RA6W1 and DA16200 are different
AT+NWMQSNI	No change	Even though the AT command response is same, but error code for both RA6W1 and DA16200 are different
AT+NWMQCSUIT	No change	Even though the AT command response is same, but error code for both RA6W1 and DA16200 are different
AT+NWMQTS	No change	Even though the AT command response is same, but error code for both RA6W1 and DA16200 are different
AT+NWMQATS	No change	-
AT+NWMQDTS	No change	-
AT+NWMQUTS	No change	-
AT+NWMQTP	No change	Even though the AT command response is same, but error code for both RA6W1 and DA16200 are different
AT+NWMQPING	No change	-
AT+NWMQV311	No change	-
AT+NWMQCID	No change	-
AT+NWMQLI	No change	Even though the AT command response is same, but error code for both RA6W1 and DA16200 are different
AT+NWMQWILL	No change	Even though the AT command response is same, but error code for both RA6W1 and DA16200 are different
AT+NWMQDEL	No change	
AT+NWMQCL	Yes	In both RA6W1 and DA16200 `+NWMQCL:1 msg` is present. But DA16200 was not updated with `msg +NWMQCL:1`. The response `+NWMQCL:0,IN_RETRY` is added for RA6W1 indicating MQTT_client is in retrial state.
AT+NWMQMSG	No change	-
AT+NWMQTT	No change	-
AT+NWMQAUTO	No change	-
AT+NWMQCS	No change	-
AT+TRTS	No change	-
AT+TRTC	No change	-
AT+TRUSE	Yes	`IP_TYPE 0/1(IPv4/Ipv6)` is not mentioned in DA16200
AT+TRUR	No change	-
AT+TRPRT	No change	-
AT+TRPALL	No change	-
AT+TRTRM	No change	-

AT Command	Difference in response	Comments
AT+TRTALL	No change	-
AT+TRSAVE	No change	-
AT+TCPDATAMODE	No change	-
AT+TRSSLINIT	No change	-
AT+TRSSLCFG	No change	-
AT+TRSSLCO	No change	-
AT+TRSSLCL	No change	-
AT+TRSSLCERTLIST	No change	-
AT+TRSSLCERTDELETE	No change	-
AT+TRSSLSAVE	No change	-
AT+TRSSLDELETE	No change	-
AT+NWWSC	No change	-
AT+NWHTC	Yes	RA6W1 doc updated based on JIRA TVR-3953
AT+NWHTCSNI	No change	-
AT+NWHTCSNIDEL	No change	-
AT+NWHTCALPN	No change	-
AT+NWHTCALPNDEL	No change	-
AT+NWHTCTLSAUTH	No change	-
AT+NWHTS	No change	-
AT+TMLMACINIT	No change	-
AT+RFTX	No change	-
AT+RFTXSTOP	No change	-
AT+RFCWTEST	Yes	Additional power `setRA6W1g config` is provided in DA16200. In RA6W1 only center frequency is provided without any power `setRA6W1g config`.
AT+RFCWSTOP	Yes	Additional power `setRA6W1g config` is provided in DA16200. In RA6W1 only center frequency is provided without any power `setRA6W1g config`.
AT+RFCONTSTART	No change	-
AT+RFCONTSTOP	No change	-
AT+RFCHANNEL	Yes	RA6W1 uses channel and Band, while DA16200 uses carrier frequency. DA16200 supports only 2.4 G and RA6W1 supports both 2.4 G and 5 G.
AT+NWOTADWSTART	No change	-
AT+NWOTADWSTOP	No change	-
AT+NWOTADWPROG	No change	-
AT+NWOTARENEW	No change	-
AT+NWOTASETADDR	No change	-
AT+NWOTAGETADDR	No change	-
AT+NWOTAREADFLASH	No change	-
AT+NWOTAERASEFLASH	No change	-
AT+NWOTATLSAUTH	No change	-
AT+NWOTAFWNAME	No change	-

AT Command	Difference in response	Comments
AT+NWOTAFWSIZE	No change	-
AT+NWOTAFWCRC	No change	-
AT+NWOTAREADFW	No change	-
AT+NWOTATRANSFW	No change	-
AT+NWOTAERASEFW	No change	-
AT+NWOTABYMCU	No change	-
AT+TZONE	No change	-
AT+GETFASTCONN	Yes	RA6W1 AT Commands do not support fast connection configuration.
AT+SETFASTCONN	Yes	RA6W1 AT Commands do not support fast connection configuration.
Power saving Mechanism	Yes	Entire commands was changed. In DA16200 it is DPM and in RA6W11 it is PMGR.

Appendix H Wi-Fi RF Parameters

Table 64. TX rate and TX power descriptions for Wi-Fi

Supported protocol	TX rate and TX power parameter	Description
11b	b1, <txPower> b2,<txPower> b5.5,<txPower> b11,<txPower>	Example: TX frequency 2412, number of frames 100, frame length 1000, TX rate 11b 1M and power value 0 AT+RFTX=2412,0,100,1000,b1,0
11g	g12, <txPower> g18,<txPower> g24,<txPower> g36,<txPower> g48,<txPower> g54,<txPower>	Example: TX frequency 2412, number of frames 100, frame length 1000, TX rate 11g 18 M and power value 0 AT+RFTX=2412,0,100,1000,g18,0
11n	n<MCS Index>,<txPower>	Example: TX frequency 2412, number of frames 100, frame length 1000, TX rate 11n MCS7 and power value 0 AT+RFTX=2412,0,100,1000,n7,0
11ac	ac;<GI>;<MCS Index>, <txPower>	<GI> is guard interval value. 0: 0.8 µs 1: 1.6 µs 2: 3.2 µs Example: TX frequency 2412, number of frames 100, frame length 1000, TX rate 11ac MCS4, Guard interval 0.8 µs and power value 0 AT+RFTX=2412,0,100,1000,ac;0;4,0
11ax-su	ax-su;<GI>; <MCS Index>p; <LTFtype>;<txPower>	<GI> is guard interval value. 0: 0.8 µs 1: 1.6 µs 2: 3.2 µs <LTFtype> is LTF type value. 0: 3.2 µs 1: 6.4 µs 2: 12.8 µs Example: TX frequency 2412, number of frames 100, frame length 1000, TX rate 11ax-su MCS3, Guard interval 0.8 µs LTF 3.2 µs and power value 0 AT+RFTX=2412,0,100,1000,ax-su;0;3,p;0;0
11ax-er	ax-er;<GI>;<MCS Index>p;<LTFtype>; <txPower>	<GI> is guard interval value. 0: 0.8 µs 1: 1.6 µs 2: 3.2 µs <LTFtype> is LTF type value. 0: 3.2 µs 1: 6.4 µs 2: 12.8 µs Example: TX frequency 2412, number of frames 100, frame length 1000, TX rate 11ax-er MCS3, Guard interval 0.8 µs LTF 3.2 µs and power value 0 AT+RFTX=2412,0,100,1000,ax-er;0;3,p;0;0

NOTE

Supported LTF type value at the specific guard interval:
- GI 0 (0.8 µs): Support LTF 0 (3.2 µs) ,1 (6.4 µs) , and 2 (12.8 µs)
- GI 1 (1.6 µs): Only support LTF 1 (6.4 µs)
- GI 2 (3.2 µs): Only support LTF 2 (12.8 µs)

Appendix I Special Characters Support in SSID or PSK

The SSID or PSK parameters have special characters that include delimiters (commas, single quotes, and backslash), extended ASCII, and UTF-8 characters. To enter these special characters, follow these rules:

- If the SSID/PSK contains delimiters(comma or single quote), the SSID/PSK must be enclosed in single quotes.
  For example:
  SSID = MY,SSID'CS
  sec = 3
  idx = 2
  PSK = N12,345’678
  Is encoded as:

```
AT+WFJAP='MY,SSID'CS',3,2,’N12,345’678'
OK
```

- If the SSID/PSK contains delimiters(backslash), it must be entered as double backslash and enclosed in single quotes.
  For example:
  SSID = MYSSID\CS
  sec = 3
  idx = 2
  PSK = N12345\678
  Is encoded as:

```
AT+WFJAP='MYSSID\\CS',3,2,’N12345\\678'
OK
```

- If the SSID/PSK contains a single quote followed by a comma, it must be entered as a hexadecimal value.
  For example:
  SSID = MY',SSID -> \x4D\x59\x27\x2C\x53\x53\x49\x44
  sec = 3
  idx = 2
  PSK = N123',45 -> \x4E\x31\x32\x33\x27\x2C\x34\x35
  Is encoded as:

```
AT+WFJAP=\x4D\x59\x27\x2C\x53\x53\x49\x44,3,2,\x4E\x31\x32\x33\x27\x2C\x34\x35
OK
```

- If the SSID/PSK contains extended ASCII or UTF-8 characters, the SSID/PSK must be entered by hexadecimal value.
  For example:
  SSID = SSID_!@#$ -> \x53\x53\x49\x44\x5F\x21\x40\x23\x24
  sec = 3
  idx = 2
  PSK = N123_!@#$ -> \x4E\x31\x32\x33\x5F\x21\x40\x23\x24
  Is encoded as:

```
AT+WFJAP=\x53\x53\x49\x44\x5F\x21\x40\x23\x24,3,2,\x4E\x31\x32\x33\x5F\x21\x40\x23\x24
OK
```

4. Revision History

Revision	Date	Description
1.07	Sep 21, 2026	Updated ATB command <persistence> description. Added channel details in Wi-Fi Connection Commands. Updated AT+TRSSLCFG command description. Added new OTA RESUME AT COMMAND.
1.06	July 21, 2026	Added the Support Special Characters in SSID or PSK appendix. Added the AT+WFJAPMK command - Connect to AP using Pre-computed Raw PMK. Updated the publish length of MQTT and the topic length in the description of the AT+NWMQMSG command. Added <duration> range for the AT+PMGRFORCE command. Modified AT+IEBNDE valid index value. Updated MQTT retain behavior for AT+NWMQMSG and AT+NWMQWILL.
1.05	May 26, 2026	Added the Wi-Fi RF Parameters Appendix. Updated section about RF Test Function Commands. Renamed the HTTP Return Values appendix to HTTP Client Result Codes.
1.04	Dec 22, 2025	Added section about LittleFS commands. Added appendix about RA6W1 vs DA16200 AT Command Response Differences.
1.03	Aug 31,2025	Updated section on Matter commands.
1.02	May 30,2025	Updated section about Bluetooth® LE Commands Changed the chip name from RRQ61000/RRQ61400 to RA6W1/RA6W2. Updated section about RF Test Function Commands.
1.01	Mar 13, 2025	Updated section about Power Manager Commands.
1.00	Dec 11, 2024	First release.